POLITECHNIKA GDAŃSKA

Imię i nazwisko autora rozprawy: Jan Piesik
Dyscyplina naukowa: Automatyka, Elektronika i Elektrotechnika

ROZPRAWA DOKTORSKA

Tytuł rozprawy w języku polskim: Narzędzia i metody zarządzania produktywnością i bezpieczeństwem w skomputeryzowanych procesach przemysłowych.

Tytuł rozprawy w języku angielskim: Methods and Tools for Productivity and Safety Management in Computerized Industrial Processes.

Promotor *podpis*
prof. dr hab. inż. Kazimierz T. Kosmowski

Gdańsk, rok 2022

GDAŃSK UNIVERSITY
OF TECHNOLOGY

The author of the doctoral dissertation: Jan Piesik
Scientific discipline: Automation, Electronic and Electrical Engineering

DOCTORAL DISSERTATION

Title of doctoral dissertation: Methods and Tools for Productivity and Safety Management in Computerized Industrial Processes.

Title of doctoral dissertation (in Polish): Narzędzia i metody zarządzania produktywnością i bezpieczeństwem w skomputeryzowanych procesach przemysłowych.

Supervisor *signature*
Prof. Kazimierz T. Kosmowski, PhD, DSc

Gdańsk, year 2022

Załącznik nr 2/1
do Zarządzenia Rektora PG nr /2022 z kwietnia 2022 r.

POLITECHNIKA
GDAŃSKA

OŚWIADCZENIE

Autor rozprawy doktorskiej: Jan Piesik

Ja, niżej podpisany, oświadczam, iż jestem świadomy, że zgodnie z przepisem art. 27 ust. 1 i 2 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2021 poz. 1062), uczelnia może korzystać z mojej rozprawy doktorskiej zatytułowanej:
,,Narzędzia i metody zarządzania produktywnością i bezpieczeństwem w skomputeryzowanych procesach przemysłowych”
do prowadzenia badań naukowych lub w celach dydaktycznych.[1]

Świadomy odpowiedzialności karnej z tytułu naruszenia przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych i konsekwencji dyscyplinarnych określonych w ustawie Prawo o szkolnictwie wyższym i nauce (Dz.U.2021.478 t.j.), a także odpowiedzialności cywilnoprawnej oświadczam, że przedkładana rozprawa doktorska została napisana przeze mnie samodzielnie.
Oświadczam, że treść rozprawy opracowana została na podstawie wyników badań prowadzonych pod kierunkiem i w ścisłej współpracy z promotorem prof. dr hab. inż. Kazimierzem Kosmowskim.
Niniejsza rozprawa doktorska nie była wcześniej podstawą żadnej innej urzędowej procedury związanej z nadaniem stopnia doktora.
Wszystkie informacje umieszczone w ww. rozprawie uzyskane ze źródeł pisanych i elektronicznych, zostały udokumentowane w wykazie literatury odpowiednimi odnośnikami, zgodnie z przepisem art. 34 ustawy o prawie autorskim i prawach pokrewnych.
Potwierdzam zgodność niniejszej wersji pracy doktorskiej z załączoną wersją elektroniczną.

Gdańsk, dnia ....

podpis doktoranta

Ja, niżej podpisany, nie wyrażam zgody na umieszczenie ww. rozprawy doktorskiej w wersji elektronicznej w otwartym, cyfrowym repozytorium instytucjonalnym Politechniki Gdańskiej.

Gdańsk, dnia ....

podpis doktoranta

[1] Art. 27. 1. Instytucje oświatowe oraz podmioty, o których mowa w art. 7 ust. 1 pkt 1, 2 i 4–8 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, mogą na potrzeby zilustrowania treści przekazywanych w celach dydaktycznych lub w celu prowadzenia działalności naukowej korzystać z rozpowszechnionych utworów w oryginale i w tłumaczeniu oraz zwielokrotniać w tym celu rozpowszechnione drobne utwory lub fragmenty większych utworów.
2. W przypadku publicznego udostępniania utworów w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i czasie przez siebie wybranym korzystanie, o którym mowa w ust. 1, jest dozwolone wyłącznie dla ograniczonego kręgu osób uczących się, nauczających lub prowadzących badania naukowe, zidentyfikowanych przez podmioty wymienione w ust. 1.

POLITECHNIKA
GDAŃSKA

STATEMENT

The author of the doctoral dissertation: Jan Piesik

I, the undersigned, declare that I am aware that in accordance with the provisions of Art. 27 (1) and (2) of the Act of 4th February 1994 on Copyright and Related Rights (Journal of Laws of 2021, item 1062), the university may use my doctoral dissertation entitled:

Methods and Tools for Productivity and Safety Management in Computerized Industrial Processes for scientific or didactic purposes.[1]

Gdańsk,...................................... ....

signature of the PhD student

Aware of criminal liability for violations of the Act of 4th February 1994 on Copyright and Related Rights and disciplinary actions set out in the Law on Higher Education and Science (Journal of Laws 2021, item 478), as well as civil liability, I declare, that the submitted doctoral dissertation is my own work.

I declare, that the submitted doctoral dissertation is my own work performed under and in cooperation with the supervision of prof. Kazimierz Kosmowski.

This submitted doctoral dissertation has never before been the basis of an official procedure associated with the awarding of a PhD degree.

All the information contained in the above thesis which is derived from written and electronic sources is documented in a list of relevant literature in accordance with Art. 34 of the Copyright and Related Rights Act.

I confirm that this doctoral dissertation is identical to the attached electronic version.

Gdańsk,...................................... ....

signature of the PhD student

I, the undersigned, do not agree to include an electronic version of the above doctoral dissertation in the open, institutional, digital repository of Gdańsk University of Technology.

Gdańsk,...................................... ....

signature of the PhD student

[1] Art 27. 1. Educational institutions and entities referred to in art. 7 sec. 1 points 1, 2 and 4–8 of the Act of 20 July 2018 – Law on Higher Education and Science, may use the disseminated works in the original and in translation for the purposes of illustrating the content provided for didactic purposes or in order to conduct research activities, and to reproduce for this purpose disseminated minor works or fragments of larger works.

2. If the works are made available to the public in such a way that everyone can have access to them at the place and time selected by them, as referred to in para. 1, is allowed only for a limited group of people learning, teaching or conducting research, identified by the entities listed in paragraph 1.

POLITECHNIKA GDAŃSKA

OPIS ROZPRAWY DOKTORSKIEJ

Autor rozprawy doktorskiej: Jan Piesik
Tytuł rozprawy doktorskiej w języku polskim: Narzędzia i metody zarządzania produktywnością i bezpieczeństwem w skomputeryzowanych procesach przemysłowych.
Tytuł rozprawy w języku angielskim: Methods and Tools for Productivity and Safety Management in Computerized Industrial Processes.
Język rozprawy doktorskiej: angielski
Promotor rozprawy doktorskiej: prof. dr hab. inż. Kazimierz Kosmowski
Data obrony:
Słowa kluczowe rozprawy doktorskiej w języku polskim: predykcja uszkodzeń, bezpieczeństwo funkcjonalne, produktywność, utrzymanie ruchu, maszyny
Słowa kluczowe rozprawy doktorskiej w języku angielskim: failure prediction, functional safety, productivity, maintenance, machinery

Streszczenie rozprawy w języku polskim: Przedmiotem niniejszej rozprawy jest problem skutecznego zastosowania w zakładach przemysłowych zintegrowanego systemu wspomagającego podejmowanie decyzji dla utrzymania ruchu, opartego na analizie danych zgromadzonych na różnych poziomach sterowania i przetwarzającego je z wykorzystaniem metod predykcyjnych oraz koncepcji systemu ekspertowego, zapewnianego zwiększenie niezawodności i dostępności maszyn oraz spełnienia wymagań bezpieczeństwa funkcjonalnego. W rozprawie analizowane jest również potrzeba zastosowania metody wyznaczania interwałów testów funkcjonalnych w oparciu o dane niezawodnościowe oraz wdrożenie podejścia uwzględniającego dodatkowe czynniki środowiska pracy przy jednoczesnym ograniczeniu strat wynikających z przestojów maszyn. Na początku rozprawy zaprezentowany jest przegląd literatury dotyczącej najnowszych rozwiązań i wymagań dla nowoczesnego przemysłu zgodnego z ideą Przemysłu 4.0, w tym zarządzania jakością, ryzykiem, bezpieczeństwem funkcjonalnym i cyberbezpieczeństwem oraz dostępnych metod i narzędzi predykcyjnych. Następnie zaprezentowano opracowanie narzędzia predykcyjnego do poprawy produktywności, niezawodności i bezpieczeństwa funkcjonalnego. Kolejny fragment rozprawy prezentuje opracowanie metody umożliwiającej łatwe i efektywne zarządzanie testami funkcjonalnymi dla funkcji bezpieczeństwa maszyn.

Streszczenie rozprawy w języku angielskim: The subject of this dissertation is the problem of effective application of an integrated system in industrial plants to support decision-making for maintenance, based on an analysis of data collected at various levels of control and processing them using predictive methods and the concept of an expert system, ensuring increased reliability and availability of machines and meeting the requirements of functional safety. The dissertation also analyses the need to apply a method for determining functional test intervals based on reliability data and to implement an approach taking into account additional factors of the operating environment while reducing losses resulting from machine downtime. At the beginning of the dissertation, a literature review is presented on the latest solutions and requirements for modern industry compliant with the idea of Industry 4.0, including quality, risk, functional safety and cyber security management, as well as available methods and predictive tools. Then, the development of a predictive tool for improving productivity, reliability and functional safety is presented. The next section of the dissertation presents the development of a method to easily and efficiently manage functional tests for machine safety functions.

GDAŃSK UNIVERSITY OF TECHNOLOGY
Faculty of Electrical and Control Engineering

DESCRIPTION OF DOCTORAL DISSERTATION

The Author of the doctoral dissertation: Jan Piesik
Title of doctoral dissertation: Methods and Tools for Productivity and Safety Management in Computerized Industrial Processes.
Title of doctoral dissertation in Polish: Narzędzia i metody zarządzania produktywnością i bezpieczeństwem w skomputeryzowanych procesach przemysłowych.
Language of doctoral dissertation: English
Supervisor: Prof. Kazimierz Kosmowski, PhD, DSc
Date of doctoral defense:

Keywords of doctoral dissertation in Polish: predykcja uszkodzeń, bezpieczeństwo funkcjonalne, produktywność, utrzymanie ruchu, maszyny
Keywords of doctoral dissertation in English: failure prediction, functional safety, productivity, maintenance, machinery

Summary of doctoral dissertation in Polish: Przedmiotem niniejszej rozprawy jest problem skutecznego zastosowania w zakładach przemysłowych zintegrowanego systemu wspomagającego podejmowanie decyzji dla utrzymania ruchu, opartego na analizie danych zgromadzonych na różnych poziomach sterowania i przetwarzającego je z wykorzystaniem metod predykcyjnych oraz koncepcji systemu ekspertowego, zapewnianego zwiększenie niezawodności i dostępności maszyn oraz spełnienia wymagań bezpieczeństwa funkcjonalnego. W rozprawie analizowane jest również potrzeba zastosowania metody wyznaczania interwałów testów funkcjonalnych w oparciu o dane niezawodnościowe oraz wdrożenie podejścia uwzględniającego dodatkowe czynniki środowiska pracy przy jednoczesnym ograniczeniu strat wynikających z przestojów maszyn. Na początku rozprawy zaprezentowany jest przegląd literatury dotyczącej najnowszych rozwiązań i wymagań dla nowoczesnego przemysłu zgodnego z ideą Przemysłu 4.0, w tym zarządzania jakością, ryzykiem, bezpieczeństwem funkcjonalnym i cyberbezpieczeństwem oraz dostępnych metod i narzędzi predykcyjnych. Następnie zaprezentowano opracowanie narzędzia predykcyjnego do poprawy produktywności, niezawodności i bezpieczeństwa funkcjonalnego. Kolejny fragment rozprawy prezentuje opracowanie metody umożliwiającej łatwe i efektywne zarządzanie testami funkcjonalnymi dla funkcji bezpieczeństwa maszyn.
Summary of doctoral dissertation in English: The subject of this dissertation is the problem of effective application of an integrated system in industrial plants to support decision-making for maintenance, based on an analysis of data collected at various levels of control and processing them using predictive methods and the concept of an expert system, ensuring increased reliability and availability of machines and meeting the requirements of functional safety. The dissertation also analyses the need to apply a method for determining functional test intervals based on reliability data and to implement an approach taking into account additional factors of the operating environment while reducing losses resulting from machine downtime. At the beginning of the dissertation, a literature review is presented on the latest solutions and requirements for modern industry compliant with the idea of Industry 4.0, including quality, risk, functional safety and cyber security management, as well as available methods and predictive tools. Then, the development of a predictive tool for improving productivity, reliability and functional safety is presented. The next section of the dissertation presents the development of a method to easily and efficiently manage functional tests for machine safety functions.

Contents

LIST OF SYMBOLS AND ACRONYMS

Symbols

β - susceptibility factor to common cause failures (according to [57])

β_{10D} - the number of cycles at which 10% of components have failed dangerously

C - is the duty cycle or mean operation, per hour

conf() - confidence of a rule in Apriori algorithm

d_{op} - is the mean operation, in days per year

h_{op} - is the mean operation, in hours per day

λ - failure rate, h^{-1}

λ_{D} - danger failure rate, h^{-1}

λ_{DD} - danger detected failure rate, h^{-1}

λ_{DU} - danger undetected failure rate, h^{-1}

λ_{S} - safe failure rate, h^{-1}

λ_{SD} - safe detected failure rate, h^{-1}

λ_{SU} - safe undetected failure rate, h^{-1}

lift() - lift of a rule in Apriori algorithm

MTTR - mean time to restoration, h

Pf - planning factor

PFH - probability of dangerous failure per hour (ISO 13849-1:2015), average frequency of dangerous failure of an SCS to perform a specified safety function over a given period of time (IEC 62061:2021), h^{-1}

$\mathrm{PFH}_{\mathrm{SYS}}$ - average frequency of dangerous failure of a safety function for the E/E/PE safety-related function (IEC 61508-6), h^{-1}

S_{FF} - safe failure fraction

supp() - support of a rule in Apriori algorithm

T - period (time interval) assumed for calculating the average probability PFH, h

T - random variable representing time to failure of a component or a system

T_1 - proof test interval or lifetime whichever is the smaller, h

T_2 - is the diagnostic test interval, h

t_{CE} - channel equivalent mean downtime, h

t_{cycle} - is the mean time between the beginning of two successive cycles of the component, s

Acronyms

AI	- artificial intelligence
ALARP	- as low as reasonably applicable
BCM	- business continuity management
BSC	- balanced scorecard
BPCS	- basic process control system
CAST-P	- computer-aided statistical tool with prediction of potential defects and failures
CBA	- cost benefit analysis
CMMS	- computerized maintenance management system
CT	- cloud technology
DC	- diagnostic coverage
DCS	- distributed control system
DMZ	- demilitarized zone, screened subnet
DNN	- deep neural networks
DSS	- decision support system
EC	- European Community
E/E/PE	- electrical/electronic/programmable electronic
E/E/PES	- electrical/electronic/programmable electronic system
EN	- European Norms
EU	- European Union
EUC	- equipment under control
FMEA	- failure mode and effect analysis
GPU	- graphics processing unit
HAZOP	- hazard and operability study
HFT	- hardware fault tolerance
HMI	- human machine interface
HSE	- Health and Safety Executive (UK)
HTML	- hyper text markup language
IACS	- industrial automation and control system
IEC	- International Electrotechnical Commission
IEE	- Institution of Electrical Engineers (UK)

IEEE	- Institute of Electrical and Electronics Engineers (USA)
IoT	- internet of things
IIoT	- industrial internet of things
ISO	- International Organization for Standardization
IT	- information technology
k-NN	- k-nearest neighbour
KooN	- K out of N configuration
KPI	- key performance indicator
ML	- machine learning
MTBF	- mean time between failures
MTTF	- mean time to failure
MUDA	- Japanese word (無駄) used in TPM meaning - waste, looses
NN	- neural network
OEE	- overall equipment effectiveness
OT	- operational technology
PDCA	- plan→ do→ check→ act (Deming cycle)
PL	- performance level
PLC	- programmable logic controller
PM	- planned / preventive maintenance
PST	- partial stroke testing
QoS	- quality of service
RBI	- risk based inspection
RCM	- reliability centred maintenance
ROI	- return of investment
SAL	- security assurance level
SCADA	- supervisory control and data acquisition
SCS	- safety-related control system [57]
SIL	- safety integrity level
SQL	- structured query language
SRP/CS	- safety-related parts of controls systems
SRS	- safety requirements specification
SVM	- support vector machines

TPM	- total productive maintenance
TQM	- total quality management
WAN	- wide area network

Chapter 1

INTRODUCTION

In this chapter, the background of the research area will be described. In addition, a problem discussion, the aim, the research questions, and the structure of the thesis are presented.

1.1. Background

In recent years, the approaches to manufacturing have changed enormously. The changes are due to the digital revolution [42], the multitude of digital tools both supporting the production process itself as well as other processes, logistics, accounting, and so on. Nowadays, many plants are supported and even maintained remotely when it is justified by specialists from another country [103]. Also, new techniques and changing approaches influence the organisation and responsibility [109], [132]. Companies are also responding to changing external conditions and expectations. These include a rapidly growing awareness of the extent to which equipment failure affects safety [63], reliability [116], [126] and the environment. A growing knowledge of the connection between maintenance and product quality [79] and increasing expectations force to achieve a high plant availability and to limit costs [8]. Thus, it requires improved management, as well as technical skills [85], [91] and its core objective is to ensure that the entire production and supporting system of a company remains reliable, productive, efficient and effective [93], [94]. Simultaneously, some limitations of maintenance systems are becoming increasingly apparent, no matter how computerised they are [27], [167].

The approach to company management has also changed rapidly in recent years. It can be observed that after the implementation of the quality management, which appears according to the standard family ISO 9000 [138], many companies have also been implementing the environmental management system ISO 14001 [64]. Nowadays, the certification of these two standards becomes the basis for business management these are recently complemented by a third family of ISO 45000 [72] standards improving employee safety, reducing workplace risks and creating better, safer working conditions. However, it still doesn't cover the full scope of activities required in industrial practice. For that reason, such standards as ISO

31000 [71], ISO 31010 [75] and ISO 22301 [68] have also been created that cover the risk management and business continuity management issues. The reason for this is that the management process becomes more complex than at the end of the twentieth century and new hazards and threats potentially affecting industrial companies have been identified. As a response, the new policy has to be implemented and the approach used till now has to be modified and/or adapted to current conditions. In those changes, almost all departments of a company, especially the maintenance department, are involved.

At the operation and maintenance stage of the production line life cycle, numerous issues can also be found. Many manufacturing facilities are based on mature management systems that have been derived from or are based on a Toyota production system [128]. It results in very high productivity ratios. However, a further increase in efficiency indicators is assumed in the coming years. Year after year it becomes increasingly difficult, as the tools that guarantee this growth begin to exhaust the current formula [98]. As a result, a new approach of Industry 4.0 has been presented [111] proposing a revolutionary change in the manufacturing system by integrating the information technology (IT) and operational technology (OT) tools [155]. At present, IT and OT systems intertwine in the aspects of machine control system, safety related control system and cyber security, among others. Which reflected in the origin of the IEC 62243 family of standards [59] and the IEC 62061 [57] standard update.

In the wake of emerging opportunities, new tools are created that will further increase productivity [135]. Unfortunately, these tools often use partial data or a narrow spectrum of maintenance approach. New methods are being developed and introduced into industrial practice for the predictive analysis regarding more and more parameters to eliminate failures using, for example, the vibroacoustic analysis or thermography. These methods use, in most cases, a narrow passage of all available information and usually do not seek connections between them. Even modern maintenance departments still suffer from a lack of integrated methods for predictive analysis. Most popular tools answer only for the marginal percentage of equipment issues [7] [187]. In the industry, in addition to necessary compliance with the law, standards, and workplace requirements, increasingly important interactions between them and other business-related issues and risks (e.g., brand receipt by customers) are becoming important [102].

For these reasons it is necessary to change the current approach to productivity, from that limited only to machinery, costs or organisational aspects, to manage modern integrated IT and OT systems proposing a superior goal to increase the productivity regarding the entire spectrum of the risk management issues [88]. Thus, achieving productivity goals should be effectively managed in the life cycle regarding the risks to be mitigated in relation to the criteria defined.

1.2. Thesis of the dissertation

Delineation of the research problems are:

1. The application of an integrated system in industrial plants to support decision making, based on the analysis of data collected at relevant hierarchy levels and processing them using predictive methods and the expert system concept ensures an increase of the reliability and availability of machines that indirectly affect productivity, the quality of products and fulfilling the functional safety requirements (regarding the cyber security aspects).
2. Applying a proposed method for determining the functional test intervals based on trustworthy-reliability data and deployment of an approach that takes into account additional factors influencing the operation of safety-related systems will ensure the required level of safety integrity while reducing losses due to the machinery downtimes.

1.3. Purpose of the study

The main objectives of the dissertation are as follows:

1. To develop methods based on modern technologies to detect potential failure in advance, which will result in the improvement of the machine availability and maintain functional safety of industrial control system (ICS). The first research hypothesis made by the author is that in modern machinery with already implemented techniques for productivity improvement, by the implementation of the computerised predictive tool with expert-based system, an increase of the overall equipment effectiveness (OEE) indicator can be achieved at minimum 0,5%. The second research hypothesis of the author is the possibility of safety-related anomalies detection, especially those due to modifications and upgrades of software and firmware of the control and safety-related elements. This will contribute to the appropriate functional safety level. The author proposes a new approach for the productivity improvement by developing an integrated strategy of maintenance oriented on productivity increase regarding the functional safety aspects.

2. To propose a method that allows to maintain the safety integrity level resulting from additionally identified risks and minimizing the negative impact on machine availability. The author proposes a customer-oriented approach for selecting appropriate tools considering relevant organisational aspects and legal requirements.
3. Development of a method that will allow to easily determine the proof test frequency of the safety functions. The author proposes a user-friendly method for selecting the frequency of functional tests considering international standards and relevant legal requirements.

Collateral objectives:

- Make a case study of the proposed method on the example of tire production line;
- Define adequate key performance indicators (KPI) for measuring profits achieved;
- Verification after a certain time in the life cycle of the obtained improvements using established key performance indicators;
- Research carried out in operation, maintenance and repair life cycle, according to the IEC 61508 and IEC 62061 standards.

1.4. Scope of the study

The scope of the dissertation covers the following areas:

- A review of scientific literature, research reports, standards, and laws (national, European, and international) concerning the latest solutions and requirements for a modern industry compliant with Industry 4.0, including risk management and functional safety (including cyber security management related to functional safety).
- Review of available industry-related prediction methods and tools for the domains of interest.
- Development of a prediction tool for productivity and reliability increase and maintaining functional safety. Development of methods and techniques for data analysis to identify specific problems that potentially can impact productivity and/or safety.

- Development of a method enabling easy and efficient managing the proof tests for the safety-related system of machinery. This includes the frequency or intervals of performing proof tests and the identification and selection of additional proof tests considering their impact on the machinery availability.

The scope of the doctoral dissertation includes issues related to the process of maintaining the machinery, its safety-related control system and auxiliary equipment. The study concerns the machinery-based production lines on the example of a tire production line. The proposed method should be considered as an important step towards improving the efficiency and safety of computerised manufacturing systems and processes.

1.5. Structure of the thesis

The dissertation consists of five chapters. The thesis has been structured into three main parts (see Fig. 1.1):

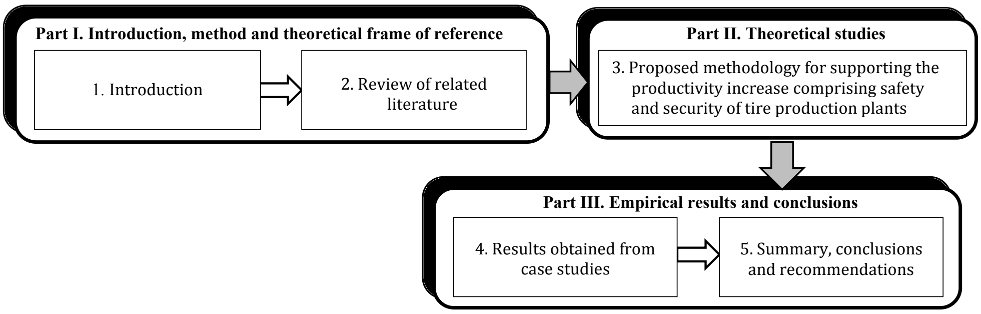

Part I. Introduction, method and theoretical frame of reference
1. Introduction
2. Review of related literature
Part II. Theoretical studies
3. Proposed methodology for supporting the productivity increase comprising safety and security of tire production plants
Part III. Empirical results and conclusions
4. Results obtained from case studies
5. Summary, conclusions and recommendations

Figure 1.1 The structure of the thesis

Part I: This part of the thesis comprises the introduction, and the theoretical frame of reference issues on the reliability techniques, the maintenance management approaches, prediction methods, functional safety, security related to functional safety issues. A review of the literature and developed solutions are shortly presented concerning the reliability and safety management in the context of Industry 4.0 concept.

The first chapter is an introduction to the definition of objectives, statement of the problem and scope of this work. The second chapter is devoted to a review of the literature with consideration of selected issues of modern production lines.

Part II: This part of the thesis comprises the theoretical studies. The proposal of the method for increasing productivity that comprises the safety and reliability needs including specificity of the production line is given. The third chapter presents the method of advanced reliability management with failure prediction that can influence the availability, safety and security of the production line. The next presented elements are the functional test interval optimisation method and the proof test interval evaluation methods for the safety integrity level (SIL) determined based on the risk assessment results.

Part III: This part of the thesis comprises the models developed during a research project, and a case study of implementing a proposed new approach in the tires production plant, and in the final part, the general discussion, conclusions and recommendations. The fourth chapter presents the implementation of the proposed method to the real manufacturing process as a case study in relation to a real industrial manufacturing plant. The fifth chapter consists of conclusions summarising the report and recommendations for further studies.

Chapter 2

REVIEW OF RELATED LITERATURE

This chapter conducts a literature review in terms of the challenges and threats facing today's industry by category. First, an overview of the idea of Industry 4.0 is presented, followed by an elaboration of the challenges faced by the industry today in adapting to the new technological revolution. It starts with management techniques focused on risk analysis, vision and strategy, keeping in mind - productivity and ensuring functional safety. In addition, prediction methods are presented along with a presentation of the latest commercial solutions. This is followed by a presentation of safety aspects with a focus on functional tests.

2.1. Industry 4.0

At the moment, the industry is deeply involved in the idea of Industry 4.0 or, in other words, the fourth industrial revolution which already accompanies us in the form of numerous smart sensors, extensive communications and cloud computing. To explain what the term „ Industry 4.0" means, meaning the fourth industrial revolution, it's necessary to explain the history of the industrial revolutions.

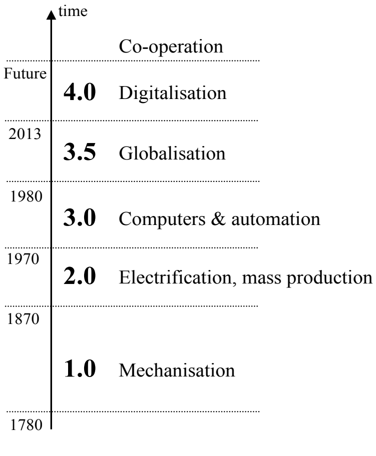


Figure 2.1. History of industrial revolutions (based on [111])

The first revolution in the industry (Industry 1.0) came with machines powered by steam, which reduced or eliminated manual labour in industry and significantly reduced the share of working animals in the industry (Fig. 2.1). The next revolution came with electricity, the assembly line and the birth of mass production (Industry 2.0). The third industrial revolution came about with the advent of computers and the beginning of automation processes. This results in replacing human workers with robots and machines on the assembly lines. The third and a half era began with globalisation and moving of the factories to low-cost countries. „Industrie 4.0" is a German term of an initiative which was first presented and discussed in 2011 on Hannover Messe and later adopted in 2013. Close to "Industrie 4.0" are the Chinese idea known as the China Manufacturing 2025, and the United States' "Industrial Internet" initiatives in an international context. The Industry 4.0 technology connects machines to a network where production processes and speeds are automatically adjusted to minimise losses and costs. The heart of the Industry 4.0 idea is intelligent manufacturing, i.e. applying the tools of information technology (AI, cyber-physical systems, as well as the cloud and cognitive computing) to production, using the internet of things (IoT) to connect small and medium-sized companies more efficiently in global production and innovation networks so that they can not only engage more efficiently in mass production but just as easily and efficiently customize products [111].

Built on the improvements brought to manufacturing by computers, Industry 4.0 will streamline production with the industrial internet of things (IIoT) and other cutting-edge technologies. In the past, information technology (IT) and operations technology (OT) operated independently of each other in manufacturing organizations. IT was mainly used to support management, administration, and accounting while OT, encompassing all the equipment and resources involved in manufacturing, controlled the machines and equipment on the shop floor without access to information from the rest of the organization. Today, the tools that makeup Industry 4.0, such as IoT, have led to a convergence of IT and OT systems that open up entirely new opportunities for smarter manufacturing and unified business management. The convergence of IT-OT systems in the era of Industry 4.0 is enabling many of the new capabilities expected of a smart factory.

Digital transformation creates the following challenges for manufacturers in the transition to the Industry 4.0 era [186]:

- **Modern business strategy and processes**: critical tasks that have the highest impact on production will increasingly rely on automated data collection and analysis. As a result, factories will be able to minimize errors and become more flexible, cost-effective and competitive.
- **Changed organizational processes**: during the transition phase to Industry 4.0, consideration must be given on how to make long-term changes to business strategy

and organizational processes. It may be necessary to modify the supply chain, change the way a company interact with customers, and hire new employees with skills in managing complex digital networks.

- **Operational disruption**: many devices in a smart factory must work together. Disruptions to process stability caused by outdated resources and the inability to communicate between systems can negatively impact the bottom line if not addressed on time. Operational disruptions can be prevented by removing any instabilities and implementing continuous monitoring for signs of potential problems in the network.
- **Safety hazards and security threats**: the high degree of communication in Industry 4.0, requires an extensive network of interconnected devices that enable data collection. These devices introduce new safety and security risks because each sensor is a specific entry point into the system. To meet this challenge, it is necessary to choose devices and software with advanced security features. Additionally, it is necessary for a company to implement an overall safety and security strategy that includes resources and employees.

The subsequent literature review is presented, according to the above categorization of the challenges currently faced by the industry.

2.2. Modern business strategy and processes

2.2.1. Corporate strategy

To operate efficiently, an enterprise must be managed, the quality of this management depends on its effectiveness in each domain. The world has been focusing on quality management for several decades, resulting in the creation of ISO 9000 series standards [38]. At present, every major company operates according to its intentions and is audited to verify its compliance. Environmental management is also becoming more and more common [90] [6] due to the increasingly stringent requirements of EU law; most manufacturing companies have also complied with these standards [52]. Businesses operating in some space and environment are obliged to comply with local and international law [117]. Many international companies also have internally developed standards and requirements that apply independently of local needs [158].

The main principle in management is presented in Fig. 2.2. It is based on the Deming cycle [145]. Most of today's companies try to make progress using the PDCA (Plan-Do-Check-Act) approach supporting it with the creation or use of well-known standards.

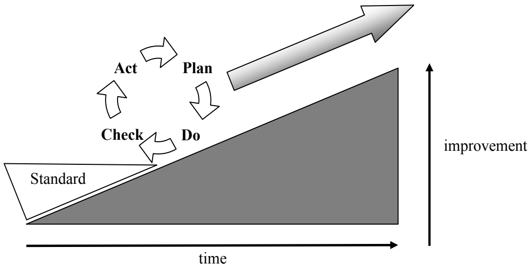


Figure 2.2. Traditional iterative four-step management model (Deming cycle) (based on [145])

To present the whole horizon and all aspects of the enterprise and common relations, the author chose the solution of presentation used in a balanced scorecard (BSC) method. BSC is a popular strategic management system proposed by Kaplan and Norton [80], and documented in their books and articles on the subject. BSC assesses the vision, mission, and business strategies of the company and aligns them to specific objectives, metrics, and indicators. The development of this system is also well presented in the literature, one of such development was proposed by Gram [43]. According to him, each of four components can be divided into sub classes or modified on the basis of company focus, needs or criticality analysis. Internal Process Perspective can be divided into material perspective, machine perspective, energy perspective, labour perspective.

The author used the BSC approach, which presents the company divided into four perspectives of performance (Fig. 2.3). All four perspectives are connected with a mutual alignment with the company's vision and strategy. In order to monitor the company's performance in each of the presented perspectives, the process of collecting, analysing and/or reporting information regarding the performance of an individual, group, organization, system, or component is needed. KPIs were specified for selecting important/critical performance measures in an organisational context. Below is a brief explanation of each of the perspectives, its relations and dependencies, and the impact on other elements of the company. This introduction is also intended to represent the range of different factors that influence and are taken into account in the normal operation of different departments within a plant, for instance maintenance.

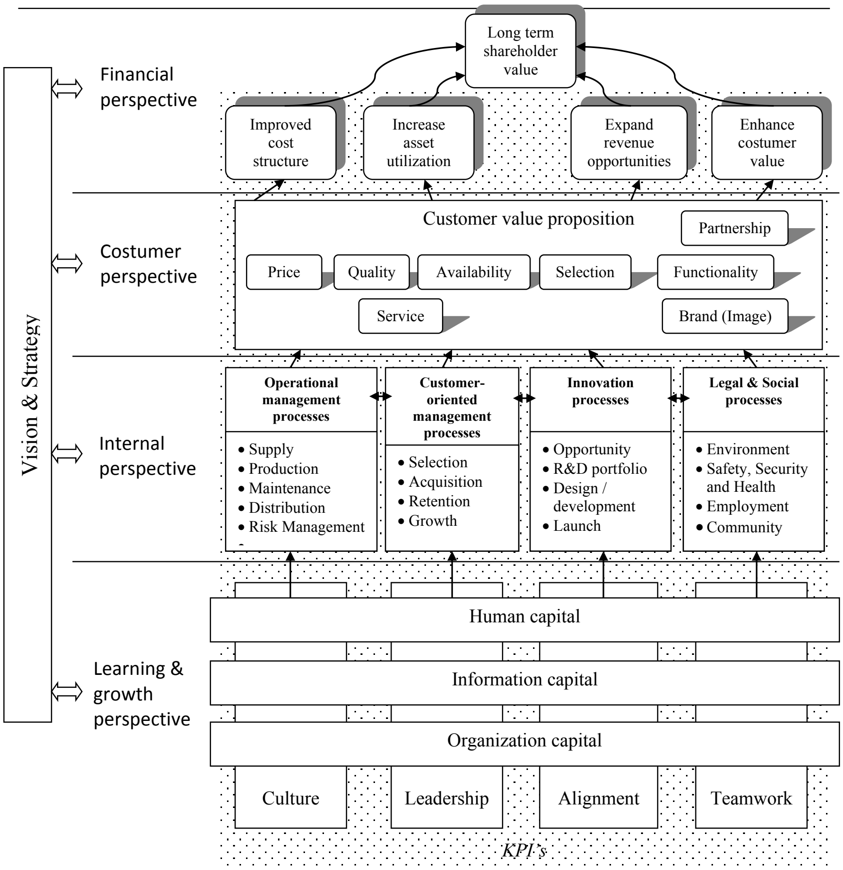


Figure 2.3. Corporate strategy and interaction map (based on [80] [122])

2.2.2. Vision and strategy

One of the most important elements presented in Fig. 2.3 is vision and strategy. These elements interact with the other four perspectives. The company's vision is how it perceives its products, markets, customers, and itself. The vision answers the simple question "Why are we here?" Vision is the goal. On the other hand, a business strategy informs how a company intends to achieve (or maintain) its vision. Strategy is a plan, tactics determine how the plan is to be implemented, and vision is the end result [80].

2.2.3. Learning and growth perspectives

The perspective of employee learning and growth are the foundation upon which the three others are built. Throughout its operations, the company discovers certain gaps between the current organizational infrastructure of employee skills (human capital), IT systems (information capital), and the environment required to maintain success (organizational capital). The objectives and measures identified in this perspective help the company to fill this gap and ensure sustainable productivity in the future [122].

2.2.4. Internal perspective

In the perspective of the internal issues, key processes are identified in which the company must stand out to be able to continue to add value to customers and ultimately to shareholders. Each of the above-mentioned customer disciplines entails the efficient operation of specific internal processes in order to service the customer and meet value proposition. The company's task is to identify relevant processes and develop the best possible goals and means by which it will be able to track progress.

Consequently, to be competitive, companies are working to improve management efficiency that will increase revenue and hence profits. The analysed aspect of the management must represent all the emerging opportunities and threats to be effective. That was already noticed by Zawiła-Niedzwiedźcki [179] and proposed as a division of risk management levels. Also, the quality management standard ISO 9001 in the version from 2015 obliges companies to consider and manage identified risks. There are many definitions of risk and risk management. The definition in ISO Guide 73 [73] is that risk is "the effect of uncertainty on objectives". Risks can affect the organization in the short, medium, and long term. These risks are related to operations, tactics, and strategy, respectively [88].

Due to the changing approach, new identified internal risks, modifications to the management model and additional elements of external risks, there was a need to add all of the hazards in the area of business management. As an answer to these needs, there are new additions to the current management approach - risk management and BCM. Both are now integrated in international standards series ISO 31000 and ISO 27000. Those standards enriched the existing model of PDCA by the part of continual improvement of the business continuity management system [68]. The second modified part of the management model is the mutual dependence between the different internal and external contexts within the company including all interested parties [71]. Enterprise management has also begun to realise that management only through indicators does not guarantee success because everything depends on their proper selection and careful analysis of the results. Commitment is another management tool that is a development of the tools for lean management [84], [16], [15] and total productive maintenance (TPM) [87], [93].

Lean manufacturing solutions is a development of Toyota's good industrial practices [84]. Their success in the international arena has led to the popularisation of this strategy [15]. Lean manufacturing is based on the philosophy of saving resources by the elimination of losses (in Japanese: MUDA). The three basic pillars of lean manufacturing are: a) continuous elimination of wastes; b) resource saving, c) and continuous improvement. In practice, this translates into reduced production lead time, increased product quality, and reduced manufacturing costs. In typical production management solutions, the machine is used in 35-60% of available time. The majority of these losses result from inefficient organisation management [67].

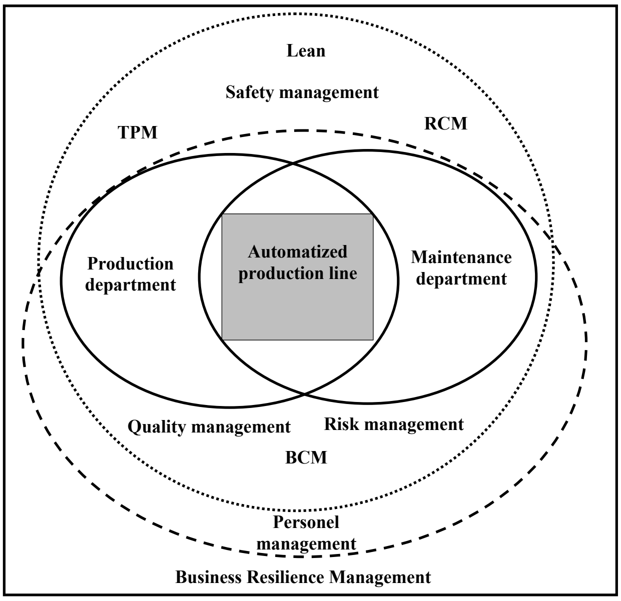


Figure 2.4. Diagram of interaction between methodologies and management scopes regarded in the thesis (based on own studies)

TPM takes into account human capabilities and limitations (human errors cause about 80% of all breakdowns [87]) and is suitable for the actions assigned to operators and maintenance staff. Subject of human factors influence is widely described by Dunn [34], Noroozi [123], Shappell [151], Bell [11], Kosmowski [87], [95], and in AICE report [26]. TPM actions are not as sophisticated as in the reliability centered maintenance (RCM) approach [116] [140], [165]. Therefore, this method is presented as a separate element in Fig. 2.4.

Two aspects leadership and commitment are the further important change in the modern management approach. Leadership and commitment were included in recent versions of standards of quality management [61] and risk management [71]. Fig. 2.4 presents a diagram of selected dependencies that affect the results of the production line. As it is widely described in the literature by Juran [79], Suzuki [158] Kletz [83], Downarowicz [32] and Zawiła-Niedźwiecki [179], the main and principal issue in the industry is proper company management. That is the foundation on which other strategies might be built and developed. In the authors' professional experience, it become clear that many technical problems were caused not by lying-in technique but rather in improper management.

2.2.5. Customer perspective

This domain includes the elements relevant from the client's point of view, which are affected by the internal perspective. Therefore, elements such as price, quality, availability of products, choice, service, partnership, functionality and brand strength are presented here. These are so universal parameters that it is not necessary to describe them further for the purposes of work [122].

2.2.6. Financial perspective

Financial resources are a key element, especially in a profit-oriented world. Objectives and measures in this perspective inform the company whether the implementation of the strategy - which is described in detail in objectives and measures selected in other perspectives - leads to an improvement in financial results. From the financial perspective, classic indicators can be observed. The methods chosen here include profitability, revenue growth and asset utilisation [149].

2.2.7. Key performance indicators

The efficiency of the production plant can be evaluated through KPIs. This method is widely utilized in many companies. Recently. the definition of KPIs was defined by international standards, e.g., ISO 22400 [10]. KPIs in manufacturing facilities are ranked according to many categories. Indicators are reflected in the objectives of the plant. They play the role of a performance measure of plant operations. Typically, they are different at different levels of business management. Their right choice often determines the success of the company. KPIs can be implemented in all types of industries, including machinery, continuous and batch processes. Proper selection of indicators allows for quick identification of losses. The key maintenance indicators, set out in standard ISO 22301, enable maintenance operations to be more efficient.

Based on the quality process approach, to qualify if the process is well managed, there is a need to define the indicators. The indicators can be divided into qualitative and quantitative. The best practice in enterprises is to use measurable indicators in the first place. If it is impossible to find indicators measurable to present or monitor a given value, qualitative indicators are proposed.

Key performance indicators is a group that describes the level of organization and functioning of companies in a model for including the organizational and technical aspects. The most known key performance indicator in maintenance is OEE [105]. It was provided with the development of the TPM concept launched in the 1980s [158]. It is a quantitative measure for expressing the productivity of manufacturing equipment. This coefficient includes three most important aspects of manufacturing: availability (A), performance (P) and quality (Q), presented in Fig. 2.5. The OEE indicator is a multiplication of those three components presented in equation 2.1 and it is expressed in percentage values. Determining this OEE supports the improvement of equipment effectiveness and equipment productivity.

$$OEE=A\times P\times Q \tag{2.1}$$

Table 2.1 shows top-level OEE and total productivity values from different types of industries. Total productivity of production unit is the result of multiplication OEE result with the planning factor (Pf) - includes planned maintenance activities and planned gaps in the production schedule [104]. Based on the analysis made in different companies it can be stated that an average production line stops more than 20 000 times per year. The majority of those stops are minor stops. The minor stop index is a measurement of the number of stops lasting ten minutes or less each hour. Continuing minor stops at average production line caused at about 6.7 hours per day. Even the best in class companies noted 3.19 hours per day because of minor downtimes [148].

Table 2.1. Overall equipment effectiveness values in different types of industries [161]

Industry	OEE top-level	Total productivity (OEE · Pf)
Manufacturing	85%	60%
Process	>90%	>68%
Metallurgy	75%	55%
Paper	95%	>70%
Cement	>80%	60%

Another example comes from packaging lines where best in class companies performed availability at level of 82.8%. Compared to mentioned above minor stoppages, middle in the class packaging lines experienced minor stoppages 8.6 times per hour, so at average line stops every seven minutes. Best in class companies have an index of minor stoppages at a level of 2.2 [143].

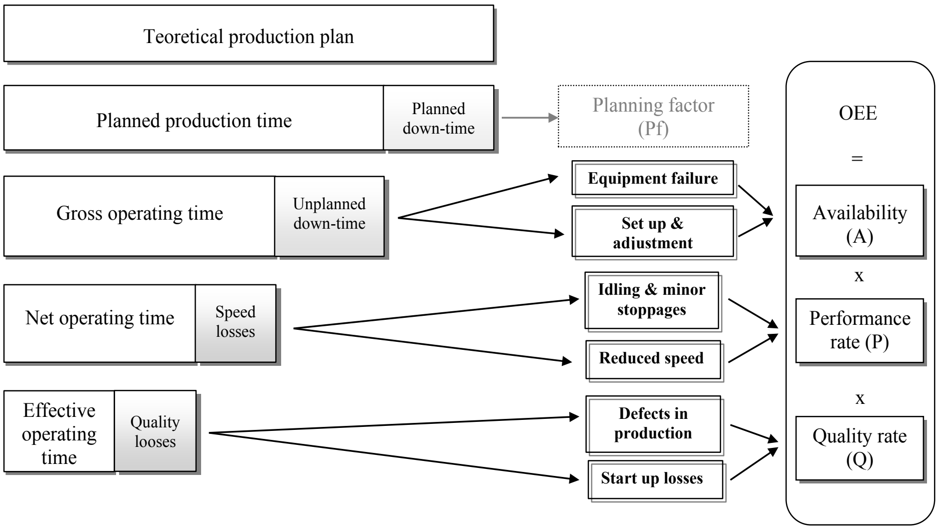


Figure 2.5. Overall equipment effectiveness KPI presentation (based on [161])

It is wide spreading around the globe and is very popular as a quantitative tool to measure equipment performance in the industry [161]. Through the years the amount of KPI's increased enormously. International standards describing indicators such as EN 15431 [20] and ISO 22400-1 [69] have also emerged. With this increase, many approaches to classify those indicators can be found in literature, example of the division is presented in Fig. 2.6. Cambell in a publication [22] has classified maintenance performance into three categories. Equipment performance as a first group with measuring availability and reliability. Measures of cost performance as a second group with maintenance, labour and spare parts costs and measures of process performance as a third category [96]. Chosen indicators are presented in Appendix 3.

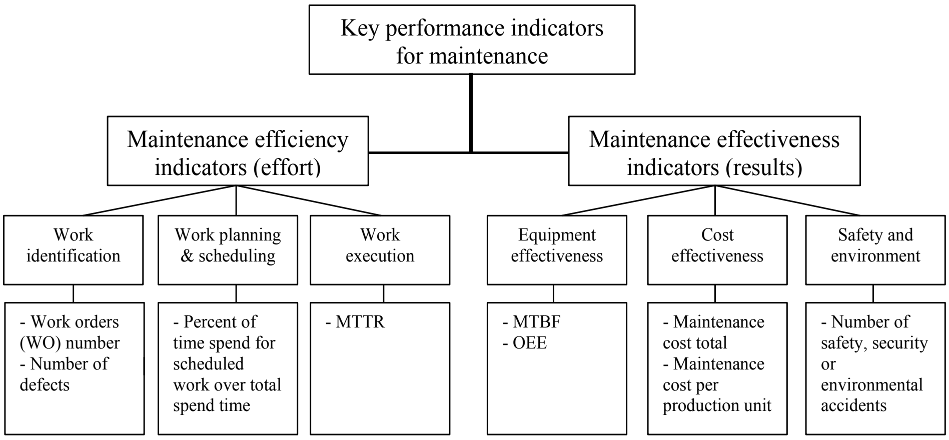

Key performance indicators for maintenance
Maintenance efficiency indicators (effort)
Maintenance effectiveness indicators (results)
Work identification
Work planning & scheduling
Work execution
Equipment effectiveness
Cost effectiveness
Safety and environment
- Work orders (WO) number
- Number of defects
- Percent of time spend for scheduled work over total spend time
- MTTR
- MTBF
- OEE
- Maintenance cost total
- Maintenance cost per production unit
- Number of safety, security or environmental accidents

Figure 2.6. Key performance indicators division (based on [33], [96], [106])

Key performance indicators are used further in the dissertation to present the past and present situation and to show the progress achieved through the implementation of the tool proposed by the author.

2.3. Changed organizational processes

In 2015, the government of the Federal Republic of Germany adopted essential elements of the Industry 4.0 model as the creation of the relevant specifications [42] of five main domains. One of them is RAMI 4.0 (Reference Architecture Model Industry 4.0) of the Industry 4.0 platform (Fig. 2.7). The architecture model requires a three-dimensional presentation.

The three axes of RAMI 4.0 describe the hierarchy levels of the internet-connected production equipment, the life cycle of the equipment and products and the IT presentation of the components of Industry4.0.

The first axis described is the hierarchy level axis. These levels basically correspond to the automation pyramid levels. They are in line with IEC 62264/IEC 61512 (Fig. 2.8) standards and can be divided into several subsystems and levels of control [144]:

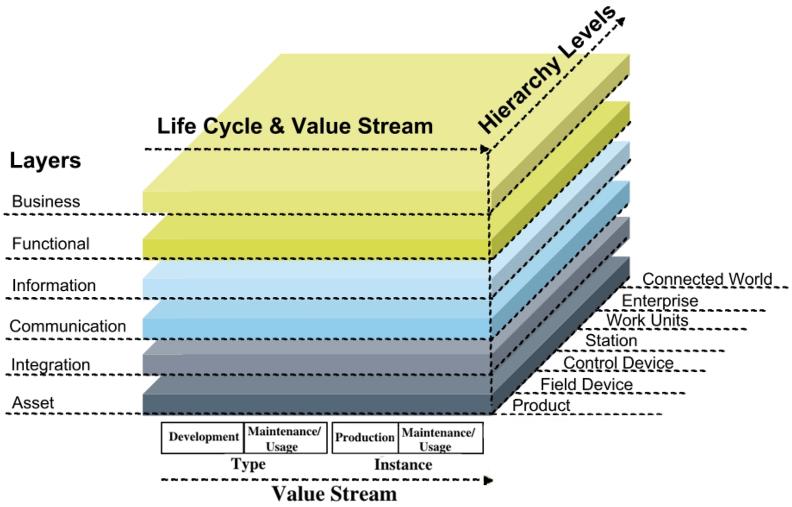


Figure 2.7. The architecture of the RAMI 4.0 model for industry 4.0 concept (based on [31])

Level 0 - Hardware level - The inputs of the system, collecting information elements, such as sensors and system of outputs with valves, relays.

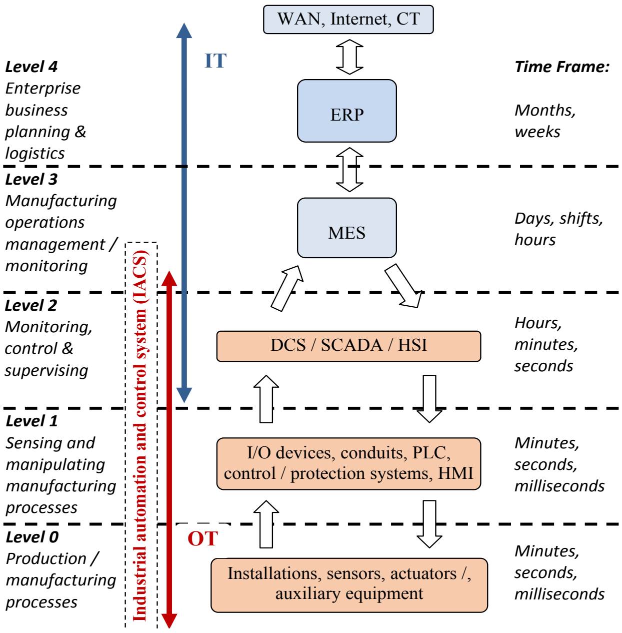

WAN, Internet, CT
IT
Level 4
Enterprise business planning & logistics
ERP
Time Frame:
Months, weeks
Level 3
Manufacturing operations management / monitoring
MES
Days, shifts, hours
Level 2
Monitoring, control & supervising
DCS / SCADA / HSI
Hours, minutes, seconds
Level 1
Sensing and manipulating manufacturing processes
I/O devices, conduits, PLC, control / protection systems, HMI
Minutes, seconds, milliseconds
Level 0
Production / manufacturing processes
OT
Installations, sensors, actuators /, auxiliary equipment
Minutes, seconds, milliseconds
Industrial automation and control system (IACS)

Figure 2.8. ISA-95/IEC 62264 functional hierarchy model division (based on [88], [4], [58])

Level 1 - The control system – Is a system that checks, manages, commands, directs or regulate the hardware level elements. In the majority of cases in the industry, programmable controllers are used for this purpose [3].

Level 2 - Process Management Level, batch control, continuous or discrete control. It is a system that supervises Level 1 – Monitoring, supervisory control an automated control of the production process [10].

Level 3 – Manufacturing Operations Management, Work flow / recipe control to produce the desired end products. Maintaining records and optimising the production process.

Level 4. - Business Planning & Logistics, Plant Product Scheduling, Operational Management. Establishing the basic plant schedule, production, material use, delivery and shipping. Determining inventory levels [177].

Note that the IEC 62243 standard is based upon ANSI/ISA-95 [4] (Fig. 2.9). To represent the Industry 4.0 environment, these functionalities have been expanded to include workpieces, labelled "Product" and the connection to the Internet of Things and services, labelled "Connected World".

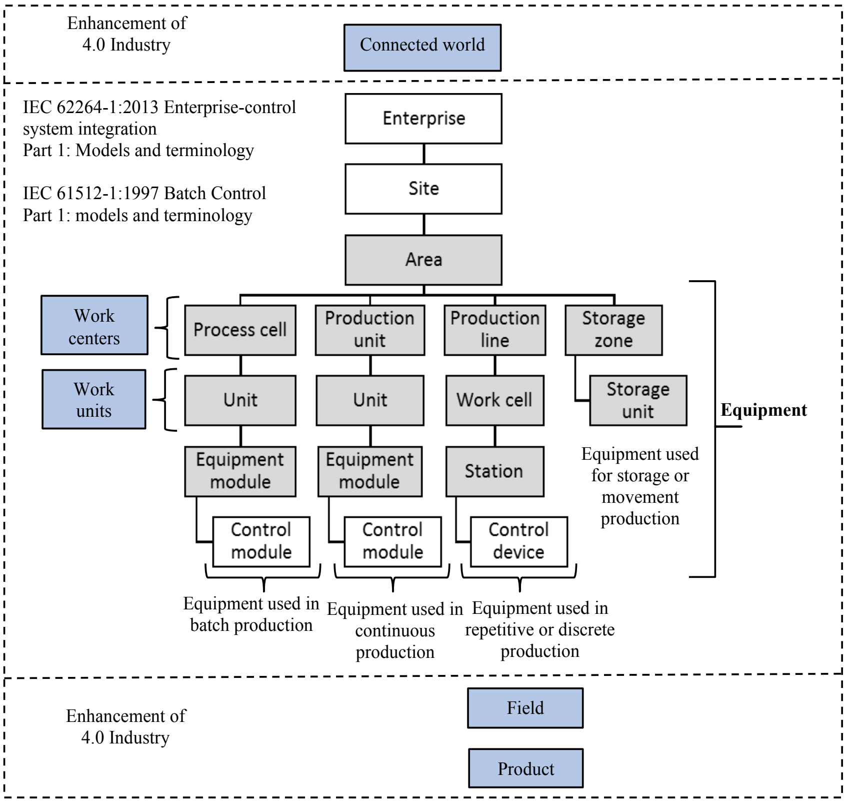

Enhancement of 4.0 Industry
Connected world
IEC 62264-1:2013 Enterprise-control system integration Part 1: Models and terminology
IEC 61512-1:1997 Batch Control Part 1: models and terminology
Enterprise
Site
Area
Work centers
Work units
Process cell
Production unit
Production line
Storage zone
Unit
Unit
Work cell
Storage unit
Equipment
Equipment module
Equipment module
Station
Equipment used for storage or movement production
Control module
Control module
Control device
Equipment used in batch production
Equipment used in continuous production
Equipment used in repetitive or discrete production
Enhancement of 4.0 Industry
Field
Product

Figure 2.9. The organisation of control system according to Industry 4.0 [180]

The second axis - process axis (value stream) includethe various stages within the life of an asset and the value creation process based on IEC 62890;

The third axis shown on a vertical axis with six layers overlapping and described as layers is the IT presentation of the components of Industry 4.0. The layers explain how business processes are viewed, functional descriptions, data mapping, how to communicate with quality of service (QoS) and how assets are linked through an integration layer. In addition to physical components such as components, machines, devices or cables, the asset layer also includes data from the planning process.

The RAMI 4.0 approach presented allows for the convergence of IT and OT systems mentioned at the beginning of this chapter and rejects analysing them as separate systems but as elements of a common system. It will be utilized in the next chapter in the methods proposed by the author.

2.4. Operational disruption

2.4.1. Reliability basics

The biggest challenge for the industry of the future for operational disruption is facing the maintenance department and the implementation of new tool and a significant change in the approach to failure management.

Failure and failure mode are important concepts in reliability analysis that needs to be explained. Based on definition from International Electrotechnical Vocabulary (IEV 192-03-01) [184] failure is defined as the termination of the ability of an item to perform its required function. It is therefore treated as an event that takes place when a required function is terminated. After the failure the item will be in a failed state so it can be named that it has a fault. The concept of failure and fault is illustrated on Fig. 2.10. A failure mode is a description of a fault by reporting how the object's inability to perform the required function according to the functional requirements can be observed [141].

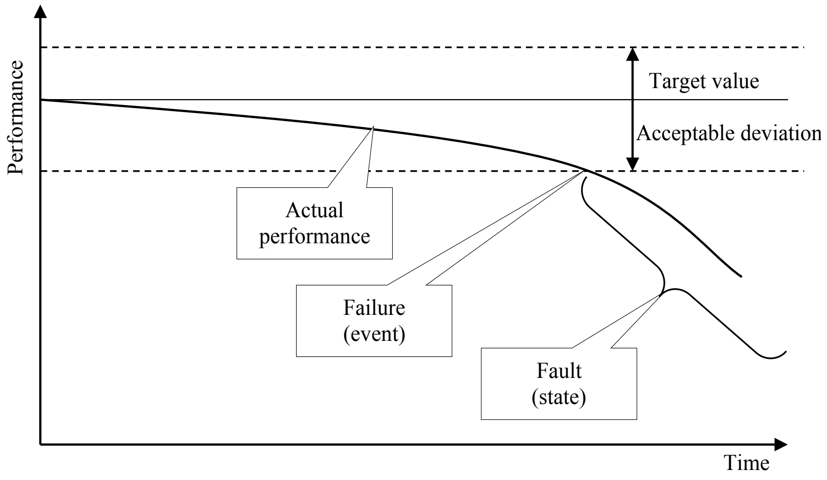


Figure 2.10. The concept of fault and failure (based on Rausand [141])

Let *T* be a random variable representing time to failure of a component or a system. Reliability is the probability that the system will perform its expected function under specified conditions of environment over a specified period of time. Mathematically, reliability is expressed as the probability that the unit does not fail in the time interval (0, *t*] [170]:

$$R(t) = P(T \geq t) \tag{2.2}$$

As the reliability denotes failure – free operation, it can be termed success probability. Conversely, the probability that failure occurs before the time *t* is called failure probability or unreliability. Failure probability can be mathematically expressed as the probability that time to failure occurs before a specific period of time *t*:

$$F(t) = P(T < t) \tag{2.3}$$

Substituting equations (2.2) and (2.3), we have:

$$F(t) + R(t) = 1 \tag{2.4}$$

The basic measure used for failure is the failure rate, *λ(t)*, which plays an important role in the reliability analysis. To explain it, it's necessary to analyze the conditional probability of a failure in the time interval from *t* to *(t+*Δ*t)* given that the unit has survived to time *t* is equal:

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{P(t < T \leq t + \Delta t \mid T \geq t)}{\Delta t} \Rightarrow \lambda(t) = \frac{f(t)}{R(t)} \tag{2.5}$$

after transformation the equations at above we come to the formula of reliability function shown below:

$$R(t) = \exp[-\int_{0}^{t} \lambda(\tau) d\tau] \tag{2.6}$$

The mean time to failure (*MTTF*) of an object is the expected value of the random variable of lifetime T, written as E(T), gives the following equation:

$$\mathrm{E(T)} = \int_{0}^{\infty} tf(t)\mathrm{d}t = \int_{0}^{\infty} R(t)\mathrm{d}t = MTTF \tag{2.7}$$

The failure rate $\lambda(t)$ defines thus completely the reliability function $R(t)$ of a nonrepairable item. In many practical applications, $\lambda(t) = \lambda$ can be assumed [17], [142]. This follows from the middle section of the bathtub curve and assumptions of an exponential distribution of the random variable for which the failure rate function $\lambda(t) = \lambda$=const. Regarding formulas (2.6) and (2.7) it can be easily shown that in such case *MTTF* is a reciprocal of the failure rate λ:

$$\int_{0}^{\infty} R(t)\mathrm{d}t = \int_{0}^{\infty} e^{-\lambda t}\mathrm{d}t = \frac{1}{\lambda} \Rightarrow MTTF = \frac{1}{\lambda} \tag{2.8}$$

In reliability evaluations of the safety related control systems taking into account the dangerous failure of the unit is often of interest. In such cases the mean time to dangerous failure ($MTTF_{\mathrm{D}}$) for known dangerous failure rate λ_{D} of the unit or channel is calculated as follows:

$$MTTF_{\mathrm{D}} = \frac{1}{\lambda_{\mathrm{D}}} \Rightarrow \lambda_{\mathrm{D}} = \frac{1}{MTTF_{\mathrm{D}}} \tag{2.9}$$

For reliability calculations to be meaningful it is necessary to be, not only concerned with the failure rate of the system, but also how a system may fail, e.g. the failure mode. Identification of all the potential failures is extremely challenging because of the fact that there are many types of failure modes. Therefore, there are various ways to classify failures based on different causes.

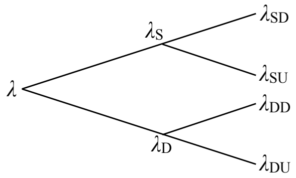


Figure 2.11. Failure classification based on the causes of failures (based on [86])

Most common failure classification proposed in IEC 61508 standard is presented on Fig. 2.11 [56]. Failure modes can be classified as safe or dangerous. Dangerous failure of an element and/or subsystem and/or system in a safety function prevents that function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the equipment under control (EUC) is put into a hazardous or potentially hazardous state (e.g. valve does not close on demand) or decreases the probability that safety function operates correctly when required. The dangerous failure rate is denoted by the symbol - $\lambda_{D.}$ A dangerous failure may result in loss of functional safety. A safe failure (λ_S) is a failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that results in the spurious operation of the safety function to put the EUC (or part) into a safe state or maintain a safe state; or increases the probability of the spurious operation of the safety function to put EUC (or part) into a safe state or maintain a safe state. A safe state can result in loss of production or service, but not the loss of a functional safety. Additionally, failures are distinguishing between detected and undetected failures. The ISO TR 12489 [76] identifies them as:

a) detected - failure which is immediately evident to operation and maintenance personnel as soon as it occurs (e.g. faults reported as diagnostic faults or alarms).

b) undetected - failure which is not immediately evident to operations and maintenance personnel (e.g. failure that is hidden until the component is asked to carry out its function).

In order to calculate the functional safety, the reliability data of the components in machinery are generally based on the data of the component manufacturer or on data from international reliability databases (e.g. SINTEF OREDA, EXIDA). There are significantly more terms and concepts in reliability theory, but due to the scope of the work and the comprehensive literature they are not discussed here.

Having already briefly described the process of failure, I would like to describe the process within companies that ensures the correct level of equipment reliability over time. The maintenance is a process that supports the manufacturing. The maintenance process as supporting the production is intended to ensure the reliability and functional safety. Ensuring reliability is reflected in the cost-effectiveness of the company as well as the stability of the quality of manufactured products in the long term and improving it [93].

2.4.2. Types of maintenance strategies

Maintenance management of equipment is carried out to increase the reliability, availability and maintain functional safety, so that equipment will continue to operate satisfactorily for the entire life cycle with required cost-effectiveness [94]. Maintenance is the corporate effort directed toward the effectiveness of plant equipment and facilities. Maintenance is a vital issue in assets management.

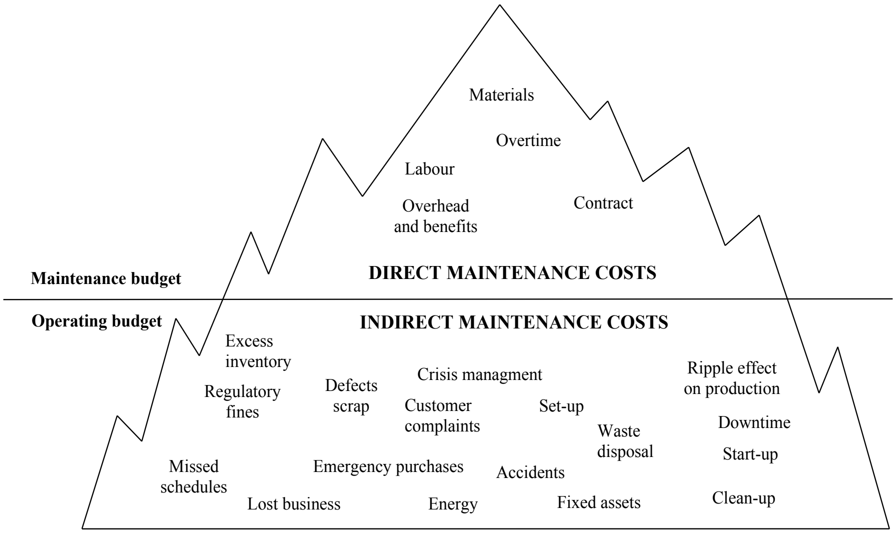


Figure 2.12. Maintenance Iceberg (based on [127])

Maintenance is often wrongly considered to be not productive and cost generating function [133]. Many managers often do not discover possibilities that are hidden in proper maintenance management and don't see the opportunity for possible inverse threats of a maintenance iceberg presented in Fig. 2.12 into business effectiveness.

Research initiated by Nowlan and Heap [126] has changed many of the most basic beliefs about the correlation between ageing and failure rate ('infant mortality' ; 'bathtub' curve). In particular, it is apparent that in each decade there is less and less connection between the operating age of most assets and the likelihood they are to fail. However, research has revealed that not one or two but six failure patterns occur in practice. Finally, some results of recent research have shown that the current equipment has entirely different types of wear than the first published in the 1978 by Nowlan and Heap. At present, the device is characterised by three types of failure patterns not related to the time of use [166], [54] but, which could be caused by variable stress or complexity in equipment [108].

Different maintenance strategies focused on the various aspects are proposed in the literature. Few of them are strategies suggested by Tu [164], Bertolini [13] Bevilacqua [14], Bris [19], Fernandez [40], Hipkina [51], Ohno [128]. Summarising there are four main categories of maintenance strategies: reactive, planned, proactive and strategic. Each of them is used nowadays depending on the industry profile, budget requirements, and safety-related criteria. Frequently, all four types are used simultaneously in the same facility. Each of these management types has some pros and cons. Depending on the company scale (number of employees), profile (chemical, automotive, fast-moving consumer goods), the range of activities (local, national, global), a different approach to organisation and sensitivity for human aspects can be found. The main categories of maintenance strategies are presented in Fig. 2.13.

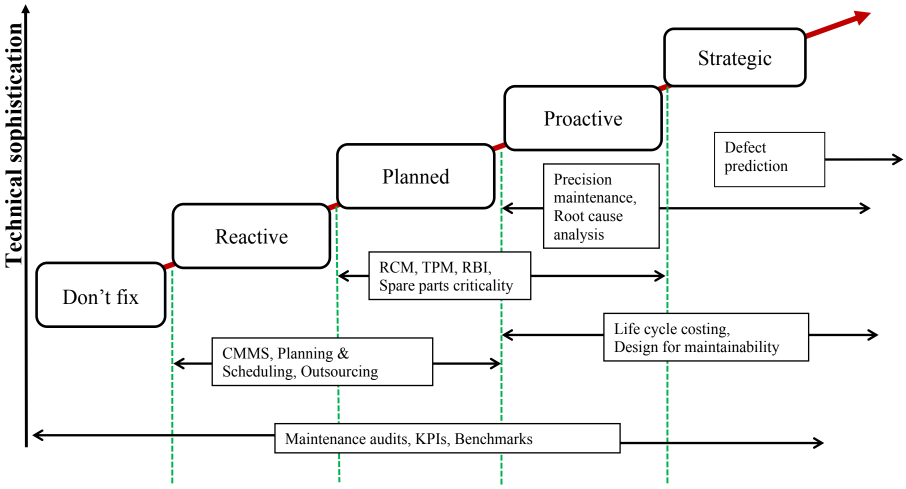

Technical sophistication
Strategic
Proactive
Planned
Reactive
Don't fix
Defect prediction
Precision maintenance, Root cause analysis
RCM, TPM, RBI, Spare parts criticality
Life cycle costing, Design for maintainability
CMMS, Planning & Scheduling, Outsourcing
Maintenance audits, KPIs, Benchmarks

Figure 2.13. Categories of maintenance strategies (based on [173])

The major challenge facing maintenance departments nowadays is to decide which maintenance strategy are worthy and which are not, in their own organizations. This issue is well described in the literature, in guides [5], for different types of industries (petro-chemical [178], electricity [154], nuclear plants [78], railway [131], automotive [128], aerospace [120], military [112], [113], metal processing [29] municipal systems [159]) and some developed methodologies [168] as well as in numerous articles [175], [176], [171]. It is possible to improve asset performance and at the same time contain and even reduce the cost of maintenance. It concerns mainly equipment -the OT system.

Currently, the greatest attention in maintenance is placed on increasing the predictive activities, which is related both to the idea of Industry 4.0 and the huge potential of advanced solutions what will be described in the next subsection.

2.4.3. Classification of prediction methods

Artificial intelligence (AI) research area can be considered to have begun during World War II with the works of Von Neuman [119]. In the beginning, these were simple algorithms.

With progress in computer techniques and increase of the calculation speed, from the beginning of ’80s, a second stage of artificial intelligence development – machine learning has been observed. The last decade brings more sophisticated tools with special processors dedicated for deep neural network (DNN) algorithms, the evolution of this approach is shown in Fig. 2.14.

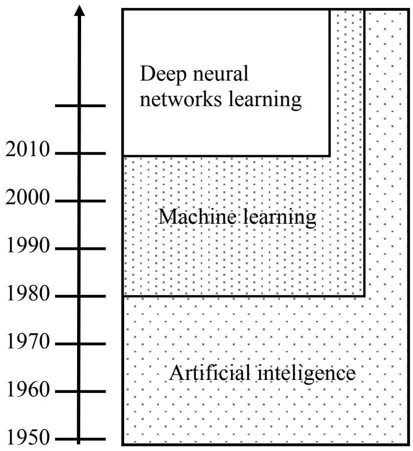


Figure 2.14. The development of artificial intelligence over the last several decades (based on own study)

Machine learning - its essence is the use of algorithms to analyse data, infer from it and then determine or predict things that were requested. Therefore, instead of hand-coding software with a specific set of instructions to perform a particular task, the machine is "trained" using a large amount of data and algorithms that allow it to learn, for instance, how to perform a task. The algorithmic approach over the years included decision tree learning, reinforcement learning, Bayesian learning and other methods. For predictive analysis the most commonly seen algorithms are:

- The k-nearest neighbours (k-NN) is a non-parametric method used also classification and regression [7].
- Support vector machines (SVMs) supervised learning models with associated learning algorithms that analyse data used for classification and regression analysis.
- Apriori used for frequent item set mining and association rule learning over transactional databases. It is utilised by the author in this thesis.
- Cox regression (or proportional hazards regression) is a method for investigating the effect of several variables upon time elapsed before a specific event occurs. In the context of an outcome such as death, this is known as Cox regression for survival analysis [47].

- Decision trees is a classification and regression algorithm for use in predictive modelling of both discrete and continuous attributes [156].
- Ada boost created by Freund and Schapire [10] was the first practical boosting algorithm. Boosting is an approach to machine learning based on the idea of creating a highly accurate prediction rule by combining many relatively weak and inaccurate rules.

Deep Learning – the base for this type of approach has stated artificial neural networks known for the last few decades. The idea of neural networks was inspired by understanding the biology of the human brain especially interconnections between neurons [156]. The difference between the biological brain and the neural networks approach is that in nature each neuron can be connected to another neuron, unlike the artificial neural networks that have discrete layers, connections, and directions of data propagation [147]. Several commercial solutions have attempted to apply deep learning in their solutions what is also discussed in the following pages. Machine learning in particular association analysis was applied in the dissertation.

2.4.4. Association analysis

Association analysis together with the construction of association rules is a method included in data mining, which is understood as statistical methods and artificial intelligence methods that enable the discovery of unknown relationships between data in accumulated data sets [12], [101]. These are methods that allow to create knowledge from data, i.e. find relationships, patterns and trends "hidden" in data. Discovering associations and building association rules is used to search and find relationships between objects or groups of objects described by many quantitative or qualitative characteristics [100]. It is an unsupervised machine learning algorithm. It can be used to generate association rules from a given data set. A priori algorithm can use boolean, quantitative, categorical types of item values. Association rule is named as single-dimensional (intradimension) since it contains a single distinct predicate with multiple occurrences. Association rules represent, in the most general terms, knowledge about the fact that some values of relevant attributes are combined with other values of other attributes in a significant frequency.

Association rules have the form of implications: if [*predecessor*] then [*successor*], which can be written down: if A then B, where A stands for predecessor and B for the successor and symbolically mark $A \rightarrow B$ [100]. From logical implications, association rules differ in that if event A occurs, then event B does not have to occur with certainty, but only with some probability (e.g. 90%). Examples of association rules are statements: "in 90% of transactions where bread and butter were bought, milk was also bought" [2]. Searching for association rules is one of the basic methods of discovering knowledge. Association rules have found application in many different areas, e.g. basket analysis (discovering patterns of customers' behaviour, which allows for better/effective placement of goods in the store, designing product catalogues, encouraging customers to buy additional articles), diagnosing failures in communication networks, conducting marketing actions, insurance activity, banking etc [12], [101], [99].

In the presented terminology explanations, the determinations commonly used in the descriptions of association analysis methods have been taken up (e.g. [101]). Let $I = \{i_1, i_2, ..., i_m\}$ denote a set consisting of m elements. In the basket analysis, it is a set of goods that can be bought in a supermarket. Each subset of T_j set I $(T_j \subset I)$ is called a transaction. In a basket analysis, a T_j transaction is a set of goods purchased by j -th customer (the so-called basket). The transaction database is a set of character pairs (id_j, T_j), where id_j is the transaction identifier, T_j is a transaction, e.g. a set of goods purchased by a customer with identifier id_j. In this case, an association rule can be formally saved as an $A \rightarrow B$ implication, where $A \subset I$, $B \subset I$ and $A \cap B = \emptyset$, this means that A and B are transactions with no common elements. The quality of an association rule can be measured on the basis of data contained in a specific transaction database. There are three indicators to be defined [101]:

support of itemset (supp)

$$\text{supp}(A) = \frac{n(A)}{N} = P(A) \tag{2.10}$$

$$\text{supp}(A \rightarrow B) = \frac{n(A \cup B)}{N} = P(A \cup B) \tag{2.11}$$

where: N - number of all transactions,

$\text{n}(A)$ - number of transactions containing elements of transaction A,

$\text{n}(A \cup B)$ - number of transactions containing simultaneously elements of transaction A and transaction B,

$\text{P}(A)$ - probability that transaction contains A,

$\text{P}(A \cup B)$ - probability that transaction contains simultaneously A and B.

If the transaction fits the rule, the conditions of the predecessor and successor are met, we say that the rule contains a specific transaction (the transaction supports a specific association rule).

a) confidence of rule (conf)

$$\mathrm{conf}(A \rightarrow B) = \frac{n(A \cup B)}{n(A)} = \mathrm{P}(B/A) \tag{2.12}$$

To consider a rule, it’s necessary to impose a minimum support, indicating a reasonable amount of data about the rule. The confidence measures how good a predictor the rule is:

b) lift

$$\mathrm{lift}(A \rightarrow B) = \frac{\mathrm{conf}(A \rightarrow B)}{\mathrm{P}(A) \cdot \mathrm{P}(B)} = \frac{\mathrm{P}(B / A)}{\mathrm{P}(A) \cdot \mathrm{P}(B)} \tag{2.13}$$

Lift is the factor by which, the co-occurrence of *A* and *B* exceeds the expected probability of *A* and *B* co-occurring, had they been independent. So, the higher the lift, the higher the chance of *A* and *B* occurring together. An example of Apriori algorithm use is presented in Appendix D.1.2.

Interesting are the rules in which both support and confidence take on relatively high values. Note that an association rule is strong if its support and confidence are greater than certain fixed minimum values:

$$\mathrm{supp}(A \rightarrow B) > \mathrm{minSupp} \tag{2.14}$$

$$\mathrm{conf}(A \rightarrow B) > \mathrm{minConf} \tag{2.15}$$

where the minSupp and minConf parameters are set by the computer program, user or an expert in the field, depending on the problem.

An important concept is the frequency of the transactions collection. In a given transaction database, the occurrence of a set of *A* transactions is the number of transactions containing a given set: n(*A*). Set *A* is defined as frequent when it occurs in transactions at least a certain fixed minimum number of times *Φ* (e.g. when we adopt Φ = 8, it means that a given set of elements from set I occur in at least eight transactions).

Frequent item set can be defined as for set value minSupp > *0,* it is said that *A* is a frequent item set then and only then if:

$$\mathrm{supp}(A) \geq \mathrm{minSupp} \tag{2.16}$$

Let it be assumed that the elements of the collection *I* are ordered. Thus, there is

$$i_1 < i_2 < \cdots < i_m \tag{2.17}$$

This order is transferred to the subset of collection I, e.g. transactions. The next stage in the presentation of association methods are algorithms for generating association rules. The number of possible association rules to be created even for a small set of I sets is very large. Therefore, it is not easy to computationally generate all association rules first and then choose the most optimal ones. Association analysis was used in this dissertation as a method for failure prediction. Which will be discussed in chapter 3.

2.4.5. Integrated prediction tool focused on reliability

As it was mentioned above, the nowadays failure types are rarely age-related and with the technical progress, the lifetime of machines has been significantly increased. At the same time, economic aspects caused that factories increase usage of their own equipment by increasing productivity and usage of machines availability. This causes that the minute of machine stops cost each year more. For those reasons, in the industry works, many companies deliver proactive diagnostics (ultrasonic, vibration analysis, oil analysis, thermography). Also, one of the goals of the Industry 4.0 revolution is to increase the availability of machines. In modern production lines equipped with all computer-based control levels, many data are gathered but used only in small percentages. Those systems rarely make use of all gathered information for learning about up to now observed failures and use this knowledge to prevent them in the future. In the past, some prognostic methods were proposed by Barringer [9], Popescu [139], Zhao [181], Carnero [25] and military standards [114], [112]. Since the year 2016, different solutions for predictive maintenance appear on the market. Those solutions can be divided into two main groups shown in Fig. 2.15. The first are based mainly on condition-based maintenance. Mainly on vibration and temperature sensors analysis. The second group are solutions that use artificial intelligence algorithms to predict failures or breakdowns.

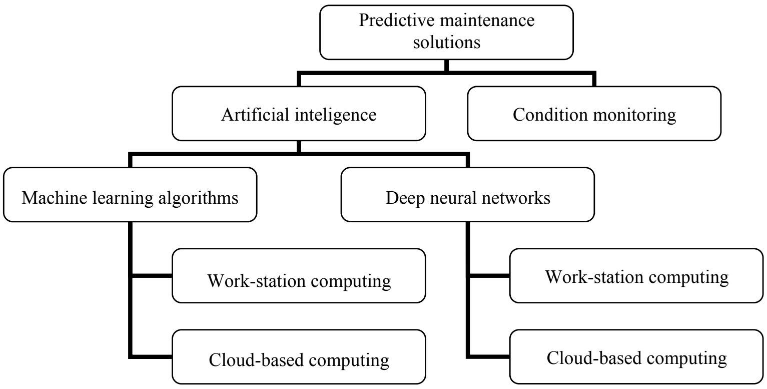


Figure 2.15. Categories of predictive maintenance solutions (based on own studies)

This category can be divided into tools based on machine learning algorithms, mainly survival algorithms and association rules algorithms. The data are computed based on powerful local servers or cloud-based solutions discussed further in the next group. The second group in this category is based on DNN. This group can be divided into two categories depending on the approach to data collection. First work-station computing is based on local high-powered servers or graphic processing units (GPU) computers. In this group, data does not leave the plant where they were collected. The second group is supported by the cloud computing which means that the collected data are sent to the cloud and analysed by distributed high powered servers outside the plant from where the data came and after analysis, results are transferred back to the user. The benefits for local data computing are the security of data as it doesn't leave the company. The cons are that data to be analysed as close as possible to real-time needs powerful servers. The second con is that there is no possibility to share the data which improves the effectiveness of the algorithms (the more data for testing the better efficiency of the algorithms). For cloud computing, the situation is inverse. The data are sent and stored in the cloud which can provoke data security problems. In pros, the data from many similar installations can be shared what leads to finding many new undiscovered relation and rules. There is no need to buy and maintain server architecture but high-speed data network is necessary.

One of the recent examples of cloud computing predictive tools can be presented based on Google Cloud IoT shown in Fig. 2.16. The tool can be divided into five modules. The first is Data capturing into the cloud (ingest). The second stage (process) is preparation of the data to be able to store and later use the data.

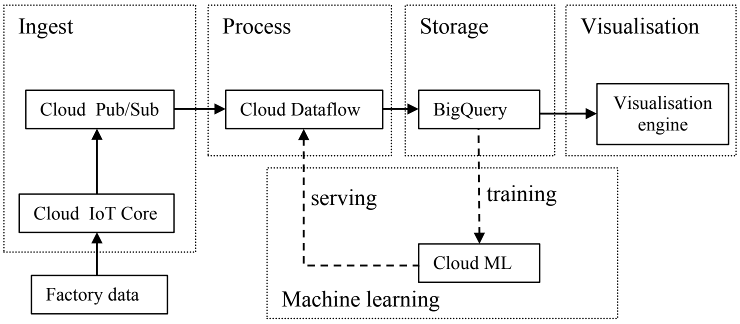


Figure 2.16. Google solution for predictive maintenance (based on [187])

The third stage of the tool is data storage in the cloud. The fourth stage is machine learning which uses the historical data to train the algorithm and after that to serve the Cloud DataFlow with founded rules. The last stage is feedback to the user with the visualisation of the received data [187].

2.5. Current safety and cyber-security related issues

2.5.1. Functional safety principles

Modern machines and installations are commonly equipped with electrical, electronic and programmable electronic control systems. That reduces the cost of machines, adds many new functions, and reduces people engagement in the direct production process. On the other hand, it creates some previously unknown safety threats [155]. This problem was noticed by specialists and international regulatory organisations which affect the founding of international standards (e.g. IEC 61508 [56], IEC 62061 [57], ISO 13849 [63]). It is important to emphasize that despite the existing wealth of knowledge, standards of machine safety and machine protection, there are still accidents at work, which was presented by Dźwiarek [35]. Looking through the perspective of Industry 4.0 and the idea of lean manufacturing, an important element is an appropriate safety level. In addition, the operation of devices in the network, frequent modification of software, remote access, information exchange at various levels of the control and management make that the entire infrastructure is vulnerable to cyber threats [81]especially SCS. As shown by quite frequent cases of cyber-attacks, the problem is no longer just a matter of thought, but has become real and can result in significant losses. Risk determination and risk management are included in life cycle of functional safety management. Below, a system-oriented life-cycle model is outlined, from initial development through to decommissioning. The diagram shown below in Fig. 2.17 is extracted from the IEC 61508 standard. The safety life cycle of a safety-related system is defined in a task flow graph. The task graph associates 16 steps within the safety life cycle. The safety life cycle is that part of the life cycle of a system during which activities related to assuring the safety of the system take place. Other tasks also appear if they are prerequisites for tasks associated with assuring the functional safety of the system [97].

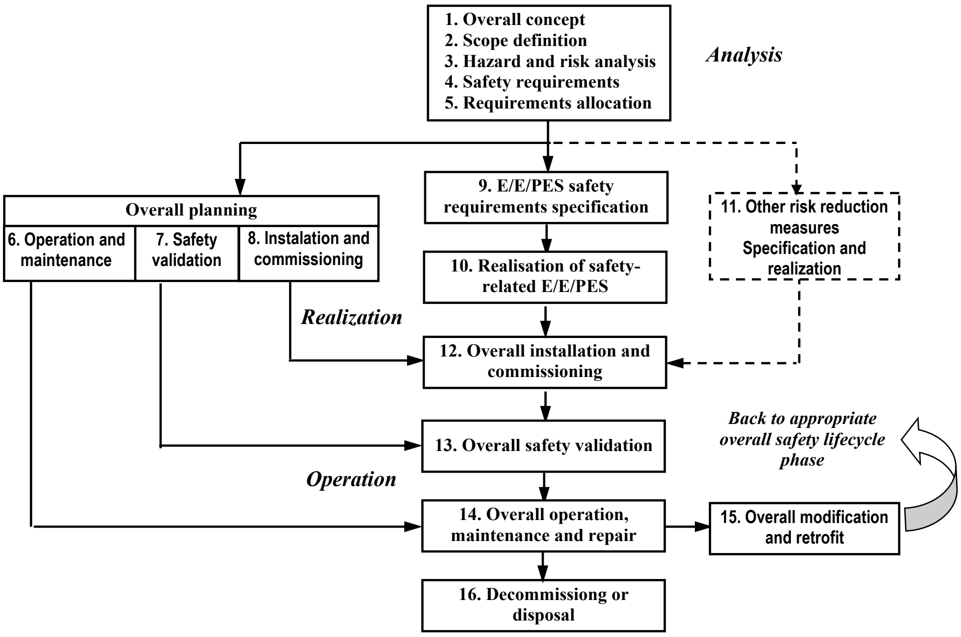

1. Overall concept
2. Scope definition
3. Hazard and risk analysis
4. Safety requirements
5. Requirements allocation
Analysis
Overall planning
6. Operation and maintenance
7. Safety validation
8. Instalation and commissioning
9. E/E/PES safety requirements specification
10. Realisation of safety-related E/E/PES
11. Other risk reduction measures Specification and realization
Realization
12. Overall installation and commissioning
13. Overall safety validation
Back to appropriate overall safety lifecycle phase
Operation
14. Overall operation, maintenance and repair
15. Overall modification and retrofit
16. Decommissiong or disposal

Figure 2.17. The total life cycle in functional safety management (based on IEC 61508 [56] [86])

This dissertation mainly focuses on stage 14, which is general operation, maintenance, and repair. It is worth noting that the diagram shows that only stage 15 is followed by the selection and re-analysis stage. It does not take into account potentially changing conditions during stage 14 and the need to perform repeated risk analyses occurring without modification (stage 15). In the following pages, on the basis of three widely used [36] machine standards ISO 12100, ISO 13849-1 and IEC 62061 risk assessment process is briefly described.

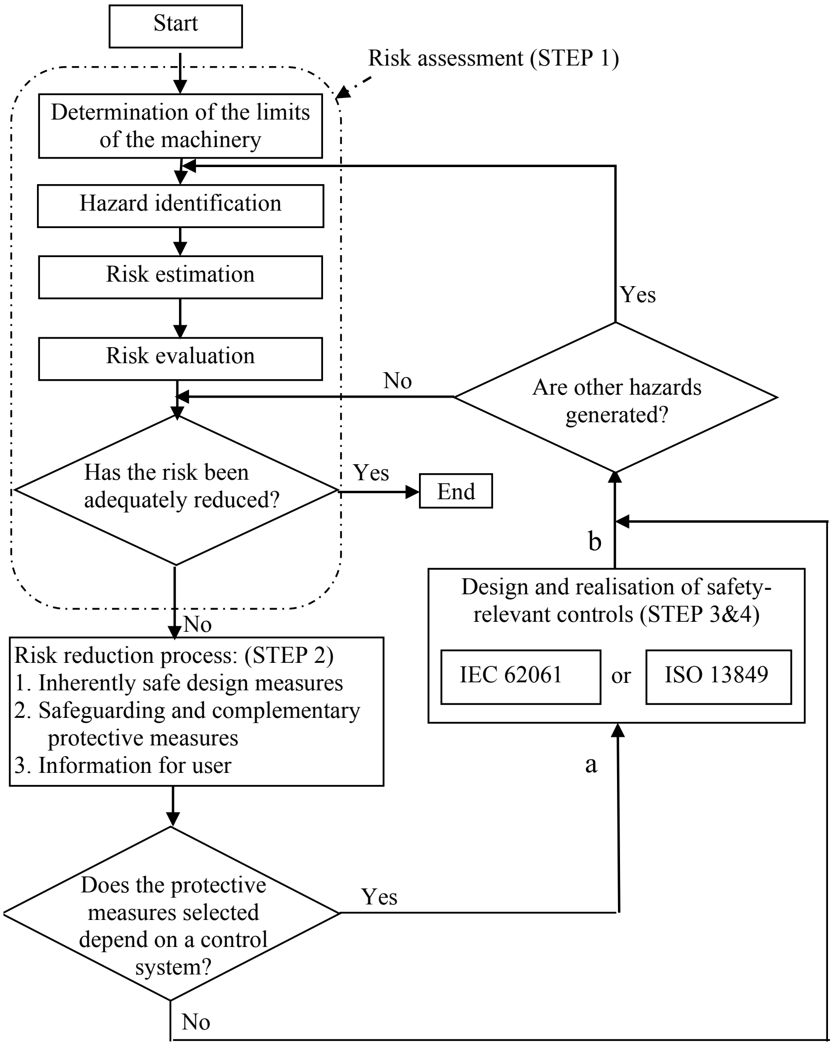

Start
Risk assessment (STEP 1)
Determination of the limits of the machinery
Hazard identification
Risk estimation
Risk evaluation
Yes
No
Are other hazards generated?
Has the risk been adequately reduced?
Yes
End
b
Design and realisation of safety-relevant controls (STEP 3&4)
IEC 62061
or
ISO 13849
No
Risk reduction process: (STEP 2)
1. Inherently safe design measures
2. Safeguarding and complementary protective measures
3. Information for user
a
Does the protective measures selected depend on a control system?
Yes
No

Figure 2.18. Risk assessment process of IEC 12000, IEC 62061and ISO 13849 (based on [62])

The objective of functional safety is freedom from unacceptable risk of physical injury or damage to the health of people either directly or indirectly (through damage to property or to the environment) by the proper implementation of one or more automatic protection functions (called safety functions). The entire step-by-step procedure for achieving safety is presented on Fig. 2.18 and described below:

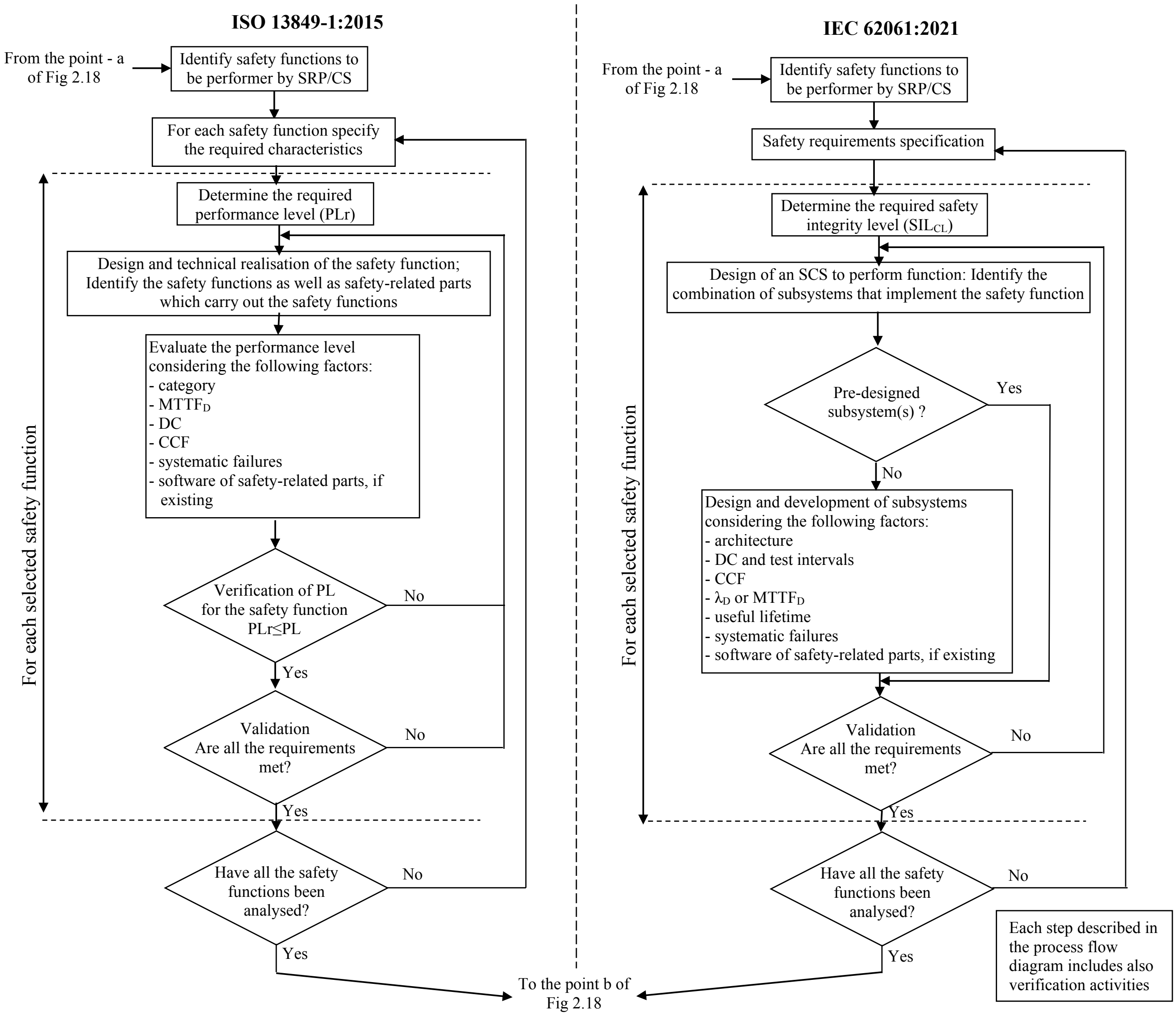

ISO 13849-1:2015
From the point - a of Fig 2.18
Identify safety functions to be performer by SRP/CS
For each safety function specify the required characteristics
Determine the required performance level (PLr)
Design and technical realisation of the safety function; Identify the safety functions as well as safety-related parts which carry out the safety functions
Evaluate the performance level considering the following factors:
- category
- $MTTF_D$
- DC
- CCF
- systematic failures
- software of safety-related parts, if existing
Verification of PL for the safety function PLr≤PL
No
Yes
Validation Are all the requirements met?
No
Yes
Have all the safety functions been analysed?
No
Yes
For each selected safety function
IEC 62061:2021
From the point - a of Fig 2.18
Identify safety functions to be performer by SRP/CS
Safety requirements specification
Determine the required safety integrity level (SIL_{CL})
Design of an SCS to perform function: Identify the combination of subsystems that implement the safety function
Pre-designed subsystem(s) ?
Yes
No
Design and development of subsystems considering the following factors:
- architecture
- DC and test intervals
- CCF
- λ_D or $MTTF_D$
- useful lifetime
- systematic failures
- software of safety-related parts, if existing
Validation Are all the requirements met?
No
Yes
Have all the safety functions been analysed?
No
Yes
For each selected safety function
Each step described in the process flow diagram includes also verification activities
To the point b of Fig 2.18

Figure 2.19. Iterative design process outline for design of safety-related control system according to IEC 62061:2021 and ISO 13849-1:2015 (based on [63], [57])

a) Step 1 – Risk assessment in accordance with ISO 12100.

A safety-related control system (SCS) consists of one or more safety functions. Safety functions and SCS are specified as a result of the risk assessment of the whole machine according to ISO 12100 [62]. Risk management (comprise risk assessment) is a series of logical steps to enable, in a systematic way, the analysis and evaluation of the risks associated with machinery (Fig. 2.20). It involves the systematic application of principles, processes, procedures and practices relating to communication and consultation activities in an appropriate context, as well as the monitoring and recording of results that may be useful in the assessment of KPIs relevant to the risk evaluation and treatment [88].

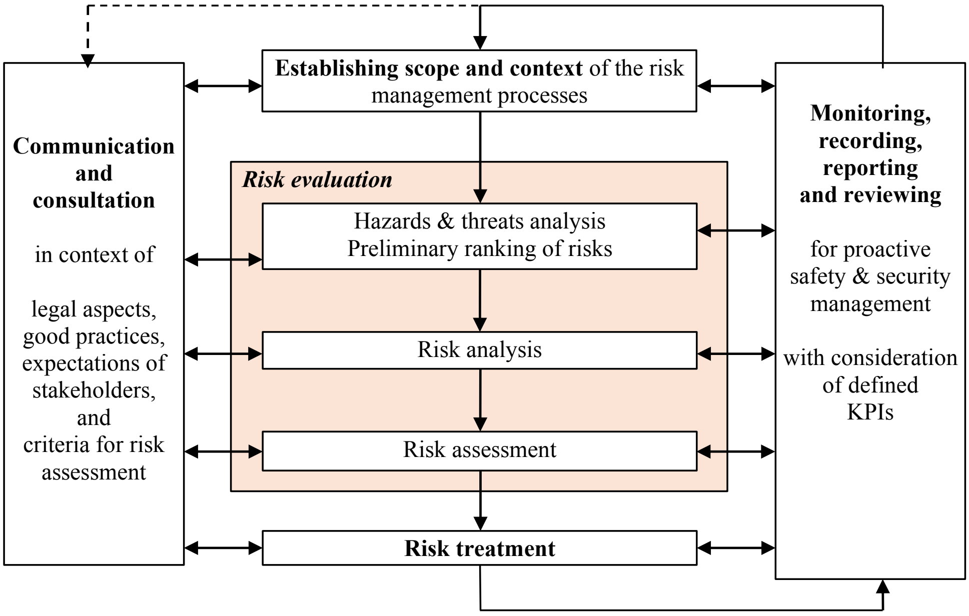

Establishing scope and context of the risk management processes
Communication and consultation
in context of
legal aspects, good practices, expectations of stakeholders, and criteria for risk assessment
Risk evaluation
Hazards & threats analysis
Preliminary ranking of risks
Risk analysis
Risk assessment
Risk treatment
Monitoring, recording, reporting and reviewing
for proactive safety & security management
with consideration of defined KPIs

Figure 2.20. Risk management process (based on [71] [89])

The ALARP (as low as reasonably practicable) principle is to be used in practice to evaluate and reduce a risk measure of interest to the level which involves balancing the risk reduction against the time available, technical problems and related cost, e.g. applying the cost-benefit analysis (CBA) [86]. Below this level, the cost of further risk reduction could become too high, unreasonably disproportionate to the benefit obtained in terms of decreased risk. Typical individual risk thresholds and lines are presented in Fig. 2.21 for workers and other persons being exposed to danger. As it is shown, the individual risk thresholds values proposed for workers/employees are an order of magnitude higher than for other persons (e.g. visitors) [92]. Three individual risk ranges are indicated in this figure: intolerable range - I, conditionally tolerable range - II and tolerable range - III, respectively for workers (w) and other persons (o).

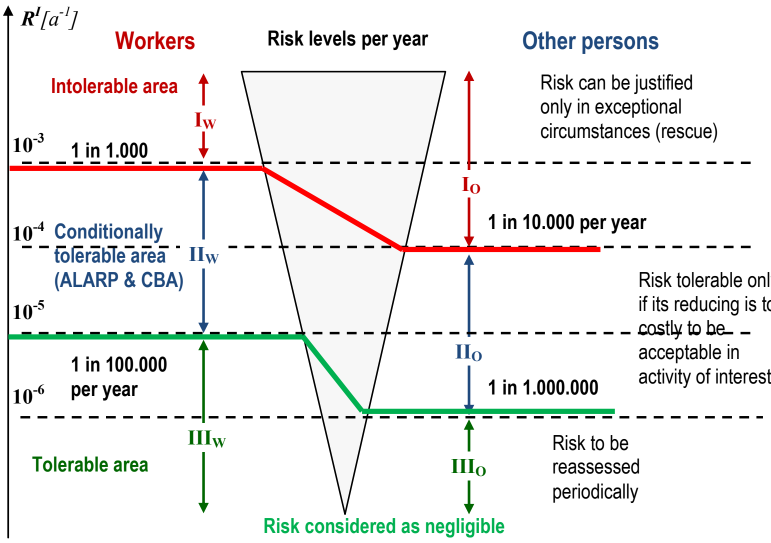

R^I[a^-1]
Workers
Risk levels per year
Other persons
Intolerable area
I_W
10^-3
1 in 1.000
Risk can be justified only in exceptional circumstances (rescue)
I_O
1 in 10.000 per year
10^-4
Conditionally tolerable area (ALARP & CBA)
II_W
10^-5
Risk tolerable only if its reducing is too costly to be acceptable in activity of interest
II_O
1 in 100.000 per year
10^-6
1 in 1.000.000
III_W
Tolerable area
III_O
Risk to be reassessed periodically
Risk considered as negligible

Figure 2.21. Individual risk criteria in the context of ALARP principle (based on [88] [92])

The individual risk R^I can be roughly defined as a function of the occurrence rate of a hazardous event per year and probability of a dangerous failure of the SCS; in which a specific safety function is implemented [88].

The main objectives of risk analysis are:

- Establish the limits and the intended use of the machinery
- Identify the hazards and any associated hazardous situations
- Evaluate the risk and decide on the need for risk reduction
- Estimate the risk for each identified hazard and hazardous situation

b) Step 2 – Define the measures required to reduce the calculated risks

The objective of this stage is to reduce risk as much as possible, taking into account various factors. This process is iterative and it may be necessary to repeat it several times in order to reduce the risk. The hazard analysis and risk reduction process require hazards to be eliminated or reduced using the following hierarchy:

1) Hazard elimination or risk reduction through design
2) Risk reduction through technical protective devices and potential additional protective measures.
3) Risk reduction through the availability of user information about the residual risk.

c) Step 3 – Risk reduction through control measures

In order to achieve the necessary risk reduction, safety control parts are used and this defines that the design of those control parts has to be an integral part of the overall design procedure of the machine.

d) Step 4 – Implementation of control measures

The implementation of control measures using standards ISO 13849 and IEC 62061 is presented below (Fig. 2.19):

1. Determination of the required performance.

The probability of dangerous failure per hour (PFH) related interval criteria proposed for designing the safety-related control system (SCS) that implements defined safety functions are specified in functional safety standards for high demand or continuous mode of operation [56]. Fig. 2.22 illustrates these interval PFH criteria for determining the safety integrity level claimed (SIL CL) given in IEC 62061 [57] and the required performance level (PL$_r$) according to ISO 13849-1 [63] standard. It corresponds with required individual risk reduction after implementation defined safety function in designing the SCS of architecture proposed, characterised e.g. by the hardware fault tolerance (HFT), i.e. hardware (HW) without redundancy (HFT = 0) or with single redundancy (HFT = 1), and requirements concerning the quality, including the reliability, of safety-related software (SW).

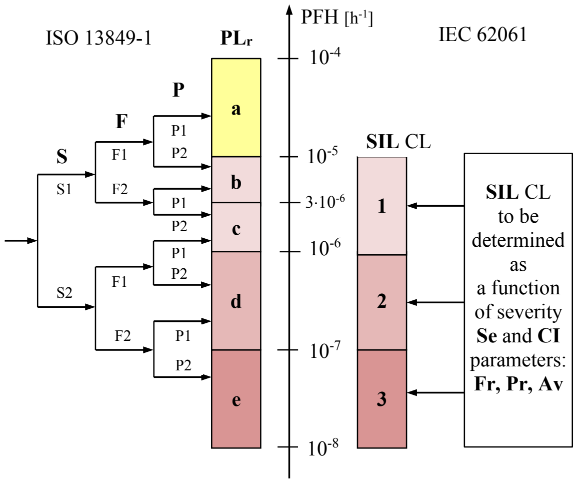


Figure 2.22. Risk graphs for determining required performance level PL$_r$ or safety integrity level claimed SL CL (based on standards [57] [63])

The risk related to the safety of machinery for a hazard considered is a function of severity of harm that could result from that hazard and probability of occurrence of that harm. It was assumed in ISO 12100 that this probability is influenced by three factors:

- the exposure of person(s) to the hazard,
- the occurrence of a hazardous event, and
- the possibility to avoid or limit the harm.

As it is shown in Fig. 2.22, the risk evaluation method proposed in IEC 62061 aimed at determining SIL CL for the safety function are considered for reducing individual risk.

The SIL CL for a safety function is determined according to Table 2.2 for the severity level (Se) selected and the class index (CI) evaluated. The CI is a sum of integer numbers for three parameters presented in Table 2.3. For instance, if Fr = 5, Pr = 4, Av = 3, then CI = 12 and for the severity selected Se = 3 from Table 2.2 the SIL CL = 2 is determined for the safety function considered. For some cases, the determination of SIL CL is not required if other safety measures (OM) are available.

Table 2.2. Determining SIL CL (or PL$_r$) of a safety function for severity level Se of consequence and class index CI [57]

Consequences	Severity **(Se)**	Class Index (**CI = Fr + Pr + Av**)								
		3	4	5 - 7	8	9 - 10	11	12 - 13	14	15
Death, losing an eye or arm	4	SIL 1		SIL 2	SIL 2		SIL 3		SIL 3	
		PL$_r$b	PL$_r$c	PL$_r$d	PL$_r$d		PL$_r$e		PL$_r$e	
Permanent, losing fingers	3	No SIL (or PL) required		(OM)	SIL 1		SIL 2		SIL 3	
				PL$_r$a	PL$_r$b	PL$_r$c	PL$_r$d		PL$_r$e	
Reversible, medical attention	2				(OM)		SIL 1		SIL 2	
					PL$_r$a		PL$_r$b	PL$_r$c	PL$_r$d	
Reversible, first aid	1						(OM)		SIL 1	
							PL$_r$a		PL$_r$b	PL$_r$c

Table 2.3. Parameters for determining class index CI [57]

Frequency and duration, **Fr**			Probability index of a hazardous event, **Pr**		Avoidance, **Av**	
	Duration of exposure ≥10min	Duration of exposure <10min				
≤ 1 hour	5	5	Very high	5		
> 1 hour ≤ day	5	4	Likely	4		
> 1 day ≤ 2 weeks	4	3	Possible	3	Impossible	5
> 2 weeks ≤ 1 year	3	2	Rarely	2	Possible	3
> 1 year	2	1	Negligible	1	Likely	1

The performance level required (PLr) for a safety function can be determined according to left side of the graph presented on Fig. 2.22 considering parameters presented in Table 2.4

according standard ISO 13849 [63] or considering Table 2.2 and 2.3 according to standard IEC 62061 [57].

Table 2.4. Parameters for determining required performance level PL_r [63]

Severity of injury, **S**		Frequency and/or exposure to hazard, **F**		Possibility of avoiding hazard or limiting harm, **P**	
Slight (reversible injury)	S1	Seldom, exposure time is short	F1	Possible under specific conditions	P1
Serious (irreversible injury or death	S2	Frequent to continuous	F2	Scarcely possible	P2

2. Specification preparation

Specification of the functional requirements shall describe each safety function that is to be performed. A safety function that is implemented using control measures generally comprises sensor, logic unit, and actuator. Such a chain can include, on the one hand, discrete elements such as guard interlocking devices or valves and complex safety controllers. As a rule, it is therefore necessary to decompose a safety function to a structure of sub-function(s). The decomposition process shall lead to a structure of sub-functions that fully describes the functional and integrity requirements of safety-related control system. Furthermore, the requires SIL or PL must be defined [172].

3. Design of control architecture

Part of the risk reduction process involves the definition of the machine's safety functions. This includes the safety functions of the control system. Why defining the safety functions, it is always important to consider that a machine has different operating states (e.g. automatic, setup mode) and that the protective measures in these different modes may be totally different. A safety function may be implemented via one or more safety-relevant control parts and several safety functions may be divided over one or more safety- relevant control parts [172].

4. Determination of the achieved performance

The process of PL/SIL determination is only outlined in Figure 2.19. Both standards use calculation methods based on simplified methods, while IEC 62061 standard additionally presents the possibility to calculate PL/SIL by formulas. The calculation results from both standards lead to similar results. There are many descriptions of these calculations in the literature and therefore the author does not include a detailed description here.

5. Verification

Approach based on ISO 13849 standard is that for any single safety function, the PL of the corresponding safety-related parts of controls systems (SRP/CS) must be equal to the required performance level. When multiple SRP/CS are part of a safety function, their PLs shall be equal to or greater than the required performance level for that function.

However, according to the IEC 62061 standard for known SIL CL, the relevant level has to be verified whether it is achieved by designed SCS of architecture considered for implementing the safety function of interest using relevant probabilistic models to meet interval criteria for PFH.

Verification of the safety system design means confirmation by examination (e.g. tests, analysis) that SCS, its subsystems or subsystem elements meet the requirements set by the relevant specification [57]. In order to verify that a target SIL or PL has been achieved we need to consider a number of things, these include the hardware architectures of the safety related controls (e.g. single channel or dual channel), the reliability of the components used, the amount of diagnostic coverage (DC), and the susceptibility to common cause failures (CCF). These are considered to be the quantifiable aspects.

One of the elements described above is the hardware architecture, which requires a brief presentation. Standard EN 62061 defines a number of basic subsystem architectures to help with the estimation of the probability of random hardware failures, these are subsystems architectures A, B, C, and D. The safety related control function might be achieved by a number of different subsystem architectures in a series alignment. Subsystem architecture A is a single channel architecture without diagnostics, the sum of the failure rates of the individual elements is the probability of failure of the subsystem. Subsystem architecture B this is a single fault tolerant (redundant) subsystem without a diagnostic function. Subsystem architecture C is zero fault tolerant with a diagnostic function. Subsystem architecture D - is single fault tolerant with diagnostic functions, the overall probability of dangerous failures of this subsystem is influenced by the design of the subsystem elements.

6. Validation

The design of a safety-related control system requires validation. The appropriateness of the safety-related control function is examined for the application. Validation can be done through analysis or testing. The verifying procedure is to be carried out for each safety function defined together with validation of additional specific requirements for the implementation site considered. Details are given in the standard [57] and publications [88], [90]. Each standard provides a unique definition of validation. Next, completing the validation of safety function step means confirmation by examination (e.g. tests, analysis) that the SCS meets the functional safety requirements of specific application [57]. Validation takes place at both the machine builder's facility, and the end-user's facility to make sure the safety-related control system operates correctly at every stage of commissioning, from installation, through start-up, to machine set-up.

2.5.2. Contemporary requirements for functional safety

The measures of the reliability of the components used and DC mentioned above in the verification phase are influenced by the functional testing parameter. It's element of the fourteen-stage total file cycle of functional safety management. Functional test's objective is to detect hidden failures which collection could prevent the execution of operating SCS in the correct manner with implemented safety requirements. Those tests should be made in conditions as close as possible to normal operating conditions of SCS. Well prepared tests include all elements of SCS from the sensor by communication devices up to logic controllers. The functional test should be created as an integral test, which means all safety-related elements of a channel should be tested at the same time. In situations where it is impossible because of lack of possibility to stop the entire line those tests should be done in sub-systems. However, also with rare frequency, entire tests have to be done.

The following tests and fault detection help to detect and remove hidden faults in the safety system. There are three possibilities for failure detection [153]:

- failure detection by automatic (diagnostic) self-tests (including operator observation),
- failure detection by functional test (manual test), e.g. proof test,
- failure detection during process requests and shutdowns.

In case of safety-related systems, three general types of testing methods exist [53] named shutdown testing, bypass testing and partial stroke testing. In machinery, the most common type of testing is shutdown testing.

At start-up, the operation of the safety function is validated but the safety function must be maintained by periodic proof testing. The definition of proof test given is a ''periodic test performed to detect failures in safety-related systems so that the system can be restored to as a new condition or as close as practical to this condition'' [125]. The full proof test performing a safety function is treated as the undesired stopping of the production process, which reduces production effectiveness. According to standard ISO 12100:2010 [62], the product manufacturer should provide information for end-user about the nature and frequency of inspections for safety functions [62]. Unfortunately, frequently no information can be found in safety manuals about proof test frequency or there is a statement that proof test is recommended to be performed at least once per year. The frequently encountered rule is also that proof test interval should not be more than 50% of the demand rate [45]. The standards assume that the useful lifetime of the machinery is twenty years [57]. It is based on the assumption of difficulty in the prediction of valid reliability data above this period [57].

The fact which cannot be neglected is a crucial role of maintenance in sustaining safety at the appropriate level in operation [182] considering maintenance and repair stage of overall safety lifecycle [56]. After machine commissioning the maintenance department takes care of safety-related aspects [82] as well as the cost criteria what has to be done choosing the correct maintenance strategy [107]. Optimisation of preventive stops is widely described in the literature. Their optimisation is analysed in terms of incurred costs [169], in short term cost optimisation and long term cost optimisation [44] and time-dependent inspection frequency models [110]. Most of the current articles focus on a narrow range of individual cost optimisations. In industry, in addition the first step, however, is to comply with legal and standard requirements, followed by optimisation in terms of productivity and costs.

Following the standard PN-EN ISO 14119 [39] covering interlocks, one can find direct values of test proof interval. For applications using interlocking devices with automatic monitoring, it is stated that for PL e with Category 3 or Category 4 or SIL 3 with HFT equal, one functional test should be performed every month. Moreover, for PL d with category 3 or SIL 2 with HFT=1, a functional test should be carried out at least every twelve months [39]. In the newest version of IEC 62061 standard [57] also appears a recommendation of redundant systems with non-electronic technology with infrequent operation to make functional tests at least every month for SIL 3 and at least every 12 months for SIL 2 [57]. In safety manuals of safety equipment, it can often be found that the producer advises or recommends to make a proof test of the device at least once per year. IEC/EN 62061 states that a proof test interval of twenty years is preferred (but not mandatory) [69]. Recently, in many safety manuals, manufacturers write that the maximum proof test interval in a high demand mode of operation is twenty years.

2.5.3. Security aspects related to functional safety

The last ten years provide a huge change in the aspect of security in the industry. With the growth of infrastructure development, more and more data are sent to the company's data centre servers around the world. The tele maintenance is becoming common not only for huge enterprises but also for small companies. The services included in cloud services are becoming increasingly popular. With all benefits provided by those innovations, the risk re-

lated to security is rapidly increasing. Cyber-attacks resulting in the physical damage on industrial plants become frequent. To help enterprises manage this new risk, new methods and security standards have been created (e.g. IEC 62243[59], IEC TR 63074 [60], ISO 27000 [70]). The issues of cyber threats in this dissertation are concerned with the impact on the functional safety of safety- related control systems.
The IEC 62443 series of standards [59] now comprises in principle 14 parts, but some of them are still under development or proposed. The aim is to cover the industrial automation and control (IACS) safety topics in a comprehensive and independent manner. It is suggested to use this series of standards to add security-related topics to IEC 61508 [56]. So far, however, IEC 61508 and IEC 62443 have been only loosely linked [88]. The IEC 62443 standard includes the concept of security assurance levels (SAL). The security assurance level framework helps group cybersecurity requirements to make them easier to implement [41]. These threats are a direct result of the increase in IT solutions used from programmable logic controllers to smart sensors and programmable actuators often connected to the internet via various communication protocols including often Ethernet. These threats have been recognised by the standards authors and therefore a technical report IEC TR 63074 [60] was published in year 2019, describing both security risk assessment but also security countermeasures.

At present, in the literature is a wealth of descriptions of proposals for strategies and countermeasures to prevent cyber-attacks, while systems can never be one hundred percent safeguarded, author quotes one of the more known general four practices that should be deployed to effectively manage cyber risk [111]:

- Prioritize protection around key assets according to the risk level identified.
- Integrate cybersecurity into core processes also as part of the enterprise wide risk management process, focusing on short reaction times.
- Engage management and employees focusing that senior management act as role models for vigilance against cyber risk.
- Safeguard the technology by automating defence as far as possible to enable cybersecurity professionals to focus on safeguarding the technology against new threats [111], this point is particularly relevant for systems with determined PLe / SIL3.

In the following chapter author take into consideration elements of security aspects in terms of protection of functional safety functions against cyber-attacks.

2.6. Chapter summary

This chapter presents an overview of the factors identified by the author that have an adverse impact on productivity and safety. Business management models are changing, encompassing an ever-growing range of phenomena that affect an enterprise. Reliability management techniques have been improved and adopted in various industries for several decades now. The analysis of the increasingly wider group and the scope of potential risks makes the company more and more secure to the impact of various negative external factors. For this purpose, business continuity management [68] and risk management [71] methods had been created and then formulated in the form of standards. In the era of digitalisation, leadership is needed at many levels of business management activities. Companies need to make many decisions quickly at many levels, often at the same time. To achieve this, it is required to have adequate methods and tools. For decades, extensive research, analysis and implementation of new models have been conducted to increase productivity, such as Juran [79], TQM or Toyota manufacturing way with TPM [64], [63], [162], [152]. USAF's reliability studies [130], [30] have given rise to further developments. Another very broadly described literature in the field of human factors research is widely covered in military standards [115], [123], [151] and by practitioners like Kletz [83] and their potential impact on all areas of the business activity.

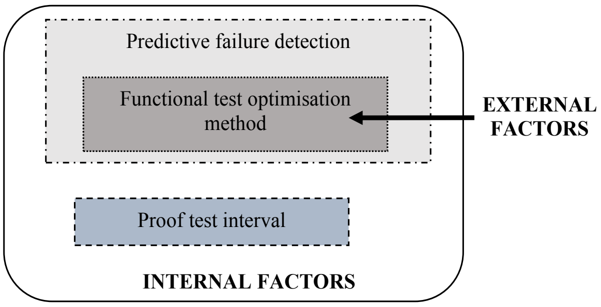

Predictive failure detection
Functional test optimisation method
EXTERNAL FACTORS
Proof test interval
INTERNAL FACTORS

Figure 2.23. Areas of interest to the author in this dissertation.

Following increasing market conditioned needs of productivity, cost reduction and safety requirements declared by families of international standards ISO 9000, ISO 14000, IEC 61508, ISO 13849 and IEC 62061 standard, computerised industries are faced with finding the optimum between economic aspects of business and risk assessment. Modern production lines, designed according to the latest requirements of international standards (especially Industry 4.0) and optimised including the economic aspects, as well as the older production lines, face the problems to ensure adequate reliability as a function of costs while ensuring the required safety integrity level [135]. A factory equipped with computerised processes and enhanced diagnostic tools often does not use a lot of information that have been collected from the hardware operation. Many possible failures to be detected and prevented still do not have the root cause found in given operational conditions. To ensure an adequate level of reliability and safety, it is required to periodically inspect safety-related features.

The first observation that the author noticed is the multitude of approaches that describe solutions to current problems in industry in a pointwise manner. The tools are not interconnected, there is a lack of synergy, especially in predictive systems. Fig. 2.23 shows several of the author's areas of interest, amid some internal and external types of factors. Failure detection as a research problem is the subject of many methodologies, which becomes very important today. However, there are no comprehensive solutions covering this topic.

The second author observation is that standards, publications and methods of functional safety are often focused on the process industry where the risk of accident and failure on a large scale is much higher than in other industries. The author focuses the research on machinery where two standards EN 13849 and EN 62061 are considered. Further analysis in this dissertation will focus on just these two areas.

Chapter 3

METHODS PROPOSED FOR SUPPORTING THE PRODUCTIVITY INCREASE AND SAFETY ASSURANCE OF PRODUCTION PLANTS

This chapter will present the methods and tool proposed by the author to improve productivity by predicting failures and ensuring the appropriate level of functional safety with test interval optimisation. Finally, the tool for the choice of proof test interval is presented.

3.1. Proposed new methods and tool

In this dissertation, the author presents tool and different methods that affect different aspects of a company (Fig. 3.1).

The first proposed method and tool aims at predicting events that can be detected by linking relationships of the predecessor/antecedent and a consequent /successor which improves availability and indirectly affects productivity, maintain functional safety (also by reducing the risk of cyber-attacks) and indirectly goods quality of the analysed object. The proposed model, in other words, is based on anticipating events through the earlier occurrence of a symptom.

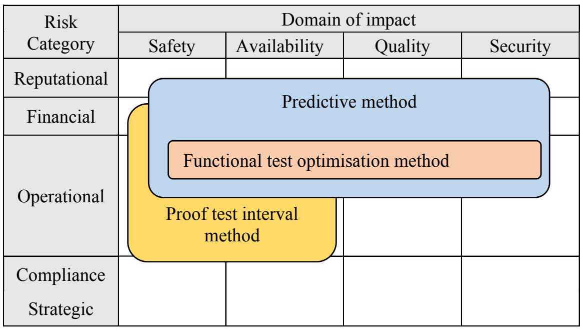


Figure 3.1. Impact matrix of the methods and tool proposed by the author by risk type and impact domain (based on [179])

The second essential point shown by the author is functional test interval optimization. This method can be provided with information from the first method presented. It is therefore a complement to the first method with elements of functional safety assurance. It is a method that was created as a result of the author's observations and the need to ensure an adequate level of functional safety while providing an adequate level of machine availability. This method affects the functional safety and availability of machines.

The last method developed by the author is the proof test interval selection tool. This tool affects operational risk and functional safety and availability of machines.

In the following pages, each of these methods and tool will be discussed in turn.

3.2. Outline of the proposed prediction method

3.2.1. General principles

The author's professional practice shows that at present, with significant development of reliability analysis and diagnostics methods, events classified as failures occur rarely without previous symptoms. Data collected by the authors' observations, made on modern production line shows that over 43% of events can be detected before the occurrence. Looking through the perspective of maintenance, the data show that product-related influences defects are the most difficult to predict. This is largely due to the variability of the quality of raw materials over time, the sensitivity of recipes and machines to this variability and fewer sensors installed for measuring these parameters on the analysed line. For all the reasons mentioned above, the sequence if the predecessor than a successor, is justified in the machinery-based industry.

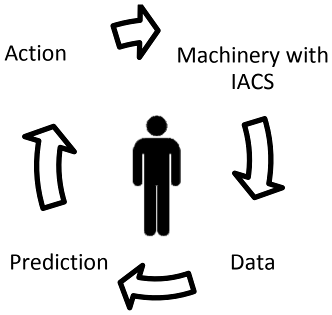


Figure 3.2. Human-centered concept of the method (based on own study)

The realization of this approach requires working in four areas (Fig. 3.2), taking into account the main role of man as a client. The first element of the cycle is the object which is the machinery with IACS. It is the source of information and the subject of corrective actions at the end of the cycle. It is also the main element of interaction with the human being. The next stage of the cycle is data. The data is obtained from the machinery at different levels of control. The data is processed here and adapted for the next stage of the process. In the next stage - prediction, the process of identifying potential future events takes place. The last stage is action where obtained predictive data is transmitted and actions are taken to eliminate safety hazards and potential failures. A significant difference in the presented approach to market solutions is the human-centred approach. The solutions described in the literature and the available market solutions are comprehensively focused on the preparation of the data for their processing and the display of the results obtained. Additionally, the methods occurring during this process are a black box for the user. Such a solution works very well when there is no need for the user's intervention to obtain the finished product and their knowledge of the process does not add value to the user (an example is artificial intelligence in camera image processing). However, systems in the industry are not currently able to collect data from machines, process this data, make predictions, issue results and take corrective action on their own. At the moment, it is a strongly interconnected and human-dependent system.

As mentioned above, predictive solutions products (failure predictive solutions) exists on the market, but they are not widely used due to a number of disadvantages. The author presents an improved prediction process with eleven groups of key changes. The course of the prediction process together with the proposed changes is presented in Fig. 3.3. The presented model comprises the basis of implemented organizational systems (TPM, RCM) and analysed object - machine, its proper preparation for predictive approach, the next stage is preparation and selection of data (data cleaning, data integration, data selection, data transformation). The model proposed by the author consists of two distinct processes. The first is data mining. This is a process of finding patterns and trends (the rule search module) useful in large data sets. The second process is predictive analytics. This is the process of extracting information from large sets of data to make forecasts and estimates of future results [115]. Both processes are co-relevant and predictive analytics is the second process. The last but equally important stage is the management of the results held, their presentation, the selection of recipients, the division of the obtained knowledge into recipients and the establishment of a model of action according to the defined criteria. After the completion of these activities as a cyclical process, all activities are performed again.

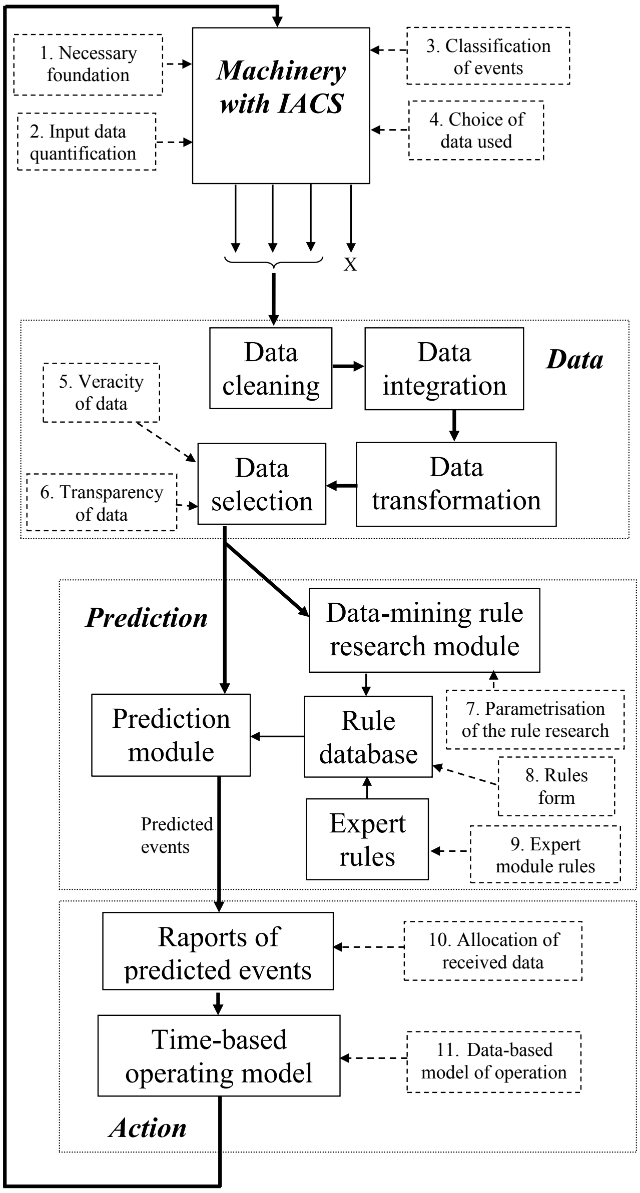


Figure 3.3. Complex predictive process with eleven enhancements proposed by the author CAST-P model (based on own study)

Main assumptions and innovative elements introduced to the author's method:

- use the prediction process to improve functional safety,
- possible applications in cyber security, quality deviations cause detection, energy efficiency optimisation and analysis of operator' behaviour.

- managing the whole process from the machinery itself to the return of human action on the object where other solutions take into consideration only data and prediction stages,
- human-centred process (taking into account the human as a client) at every stage of the process,
- approach from the user's perspective (operator, maintenance), not purely mathematical and IT, the process is not a black box for the user.

In the following subsections, each of the four stages will be approximated in detail.

3.2.2. Machinery with control system - process stage

The first stage of the process is machinery with control system. It includes the entire production line with all levels of control, safety systems, human-system interfaces. At this stage, the author proposes four groups of modifications to improve the process (Fig. 3.4). The author takes into account devices whose age does not exceed twenty years. This is the age that is currently defined by most of the manufacturers as the lifetime of the device and it is the maximum value for which operation is planned and an appropriate level of reliability [57].

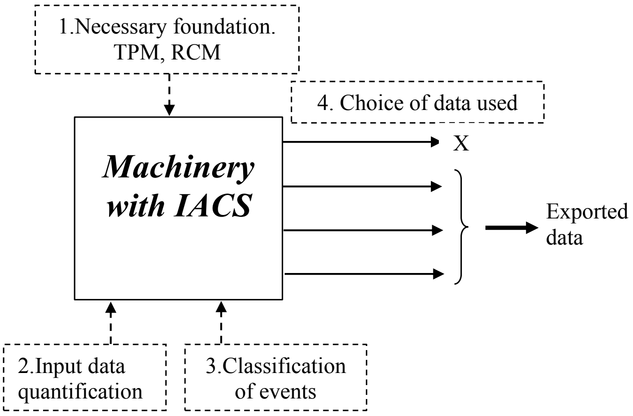


Figure 3.4. Inputs and outputs of the different levels of control system (based on own study)

Four of the changes proposed by the author concern, in the first case, the necessary organisational requirements, in the second and third case, the preparation of the data, while the fourth concerns the selection of the data.

3.2.2.1. The necessary foundations

As previously presented in chapter 2, due to the high impact of maintenance services on the company's economic performance, in particular, costs related to the purchase of spare parts and the percentage of unplanned and planned shutdowns reducing production line efficiency and the same fixed maintenance costs (wages, tools, subcontractors) many methodologies and tools to improve the efficiency of this department were developed. These methodologies address the production system (TPM), for analysis of the costs associated with preventive spare parts replacement policy (RCM). TPM as a methodology covers a wide range as it also refers to behaviours, working methods as well as cost reduction. A lot of space in the literature is also devoted to the management of maintenance competencies. In relation to other departments, they are usually much wider and require specialist knowledge.

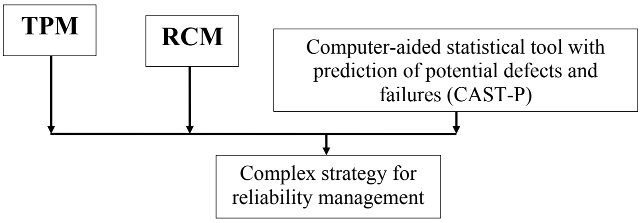

TPM
RCM
Computer-aided statistical tool with prediction of potential defects and failures (CAST-P)
Complex strategy for reliability management

Figure 3.5. Integrated maintenance concept [132]

The proposed integrated solution is very multidisciplinary as it proposes a data mining solution. Each technique requires human servicing and maintenance, the more technically advanced it is, the more skill is required to handle and maintain traffic, but the human behaviour remains the same for both cases, resulting in the need to implement organisational techniques such as TPM and cost optimisation approach as RCM (Fig. 3.5). Having both of these methods implemented at some point ends up ways for further progress in conjunction with the implementation of a computer-aided statistical tool with prediction of potential defects and failures (CAST-P) as it was presented by the author in [132]. It is a good foundation for a complex strategy of reliability management. The implementation of these tool guarantees the best-known standards of action plan piloting and problem-solving at the moment. This brings the following benefits:

- the required level of training for operators and maintenance
- a professional approach to machine repairs
- planned maintenance at a high level,
- proper management of the predictive results obtained
- to carry out a cause analysis with the detection of the real root causes

This also results in the lack of false or noisy information received at the subsequent stages of the prediction process. It is assumed that the RCM and TPM methods have to be already implemented in the analysed production lines, and besides the short description, those management techniques and methods will not be the subject of this work.

3.2.2.2. Input data quantification

There is a wealth of data in manufacturing companies. This data comes from sensors, smart sensors, converters, control systems, human-system interfaces, supervisory control and data acquisition (SCADA) systems, and several other sources (Fig. 3.6). The number of data sources is increasing from year to year thanks to the progressive digitalisation of production and ancillary processes and the digitalisation of all operations that have been recorded so far in paper form.

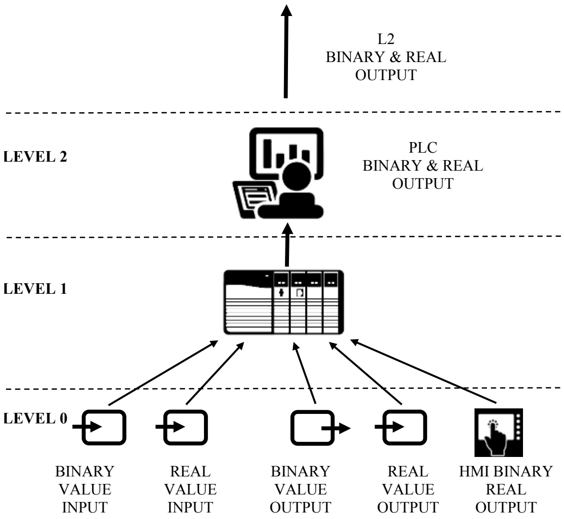


Figure 3.6. Inputs and Outputs of the different levels of control system
(based on RAMI 4.0 and ISA 95)

The important element of the model is the form in which data is obtained for further analysis. As already mentioned above, data can be obtained in various value and data formats. Several types of data can be distinguished here:

- binary data (boolean)
- real-value (real number)

Data in binary form Eq 3.1 - such a choice causes a dramatic decrease in the amount of valuable information and results in a significant decrease in the number of rules that may arise from this data. On the other hand, it is the simplest and most comprehensible way to do analyse without requiring much computing power.

$$DB = \{x_1, \cdots, x_i\} \text{ where } x_i = 0 \vee 1; i = 1,2,...,n \tag{3.1}$$

Data in real value Eq 3.2- this selection results in the largest, from all data types, the possible number of rules to be found, but they can often be untrue, and it takes a lot of human resources and expertise to pre-treat the data and then to lay down and select the resulting rules. Considerable hardware requirements also arise.

$$\text{DR} = \{y_1, ..., y_j\} \text{ where } y_j \in R, j = 1,2,...,n \tag{3.2}$$

The authors' proposal is to use two data types in further calculations: binary data and simplify other data types into quantified data (Fig. 3.7.) Eq.3.3. Data quantification is an intermediate solution using smart metering and smart sensor concepts. It entails the quantification of input data as close as possible to its origin, e.g. through smart metering systems that process analogue values into several thresholds and send them further to control systems.

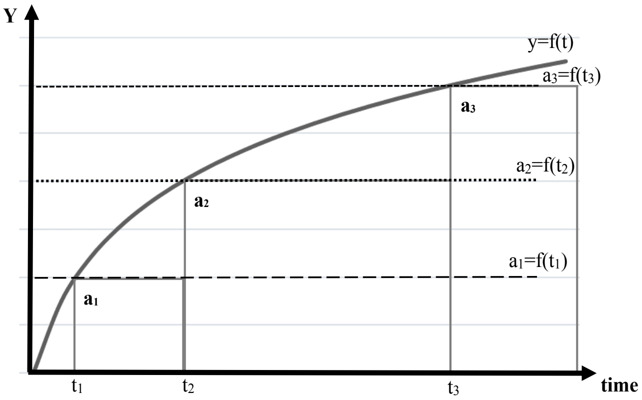


Figure 3.7. Example of data quantification into three quantified value levels (based on own study)

$$DQ = \begin{cases} a_1, < t_1, t_2) \\ a_2, < t_2, t_3) \\ a_3, < t_3, t_N) \end{cases} \tag{3.3}$$

The value added from the data quantification results in the possibility of building multiple levels of values, which can be used depending on symptom and effect, e.g. if two oil temperature sensors outputs are programmed (warning level, alarm level), the occurrence of the first sensor output can be considered as a symptom for the occurrence of an alarm input (oil overheating → alarm temperature level → machine stop). The solution proposed by the author consists of the verification of installed digital sensors for the use of quantification of output levels and set switching values. In the case of analogue sensors, verification of the controller's or transmitter's logic in order to determine appropriate switching levels and messages issued. Optionally, during the preparation process, adding new sensors with several switching levels.

3.2.2.3. Classification of events

All events can be divided into many categories depending on the division key. These divisions are used for many purposes (e.g.: division of information displayed on the operator's dashboards of a given operator station) defined by plant and machine designers and control engineers. Events classification (Eq. 3.4) is a division of all recorded events into categories.

$$Events = (EVT_1,\ EVT_2,\ ...,\ EVT_N) \qquad (3.4)$$

Categories can serve many indirect purposes and the primary purpose of dividing all events into two categories: symptoms and failures. This action allows to reduce the number of computer calculations and eliminates the creation of trivial and misleading rules. Examples of categories are

a) operator actions - all events performed by the operator;
b) HMI - all activities of an operator's interaction via operator panels;
c) machine stoppages - failures resulting in machine stoppage;
d) section stops - failures that result in machine section stops;
e) system events - information on events generated by the SCADA, machine control system or other systems;
f) recipe change - information about the change of the current recipe on the machine.

3.2.2.4. Choice of data used

Each control level has a different range, size and variety of data formats. This means that collecting data from only one level may not be sufficient for analysis and prediction purposes. On the other hand, data collected from all levels may place a heavy workload on the IT infrastructure (capacity, computing power) (Table 3.3) and may duplicate information already obtained in another format (which may create unnecessary trivial rules). Therefore, the author considered it reasonable to create a data selection matrix depending on the purpose of the analysis (Table 3.2).

Table 3.2. The data selection matrix depending on the purpose of the analysis.

Data mining or prediction module	Level 0 (L0)	Level 1 (L1)	Level 2 (L2)	Comments
Failures prediction	x	x	x	$L0\ or\ L1\ or\ L2$
Safety deviation prediction		x	x	$L1\ or\ L2$
Cyber-attack detection	x	x		$L0\ or\ L1$
Quality deviation detection	x	x	x	$(L0\ or\ L1)\ and\ L2$
Energy efficiency optimisation	x	x	x	$(L0\ or\ L1)\ and\ L2$
Operator's behaviour analysis			x	$L2$

For example, in the case of failure prediction, machine data are of interest. These data can be found at each level of control - of course in a different form and scope. However, analysis of the data of any of the levels will allow results to be obtained. Therefore, it can be written that the user can select one of three control levels as the data source ($L0$ or $L1$ or $L2$). The situation changes in the case of quality deviation detection where knowledge from two levels is needed to correctly predict events. It results from the fact that only level 2 contains all events informing about quality parameters. The information about machine state can be collected from level 0 or level 1. Therefore, here the user must use data from L0 or L1 and L2 (($L0$ or $L1$) and $L2$).

The proposed selection table has a general purpose and can be modified depending on the specifics of the plant and control systems. However, it gives the foundation to select the necessary data to achieve assumed goals.

Table 3.3. A comparison of advantages and disadvantages of collecting data from different control levels.

Level 0	Level 1	Level 2
+ the largest amount of raw data to allow for the most complex analyses	+ pre-processed and assigned data	+ processed and assigned data, - loss of certain information
- large data size, - no attribution of data details, - tedious data pre-processing required,	- large data size but smaller than level 0, - tedious data pre-processing required,	+ moderate data size, - processed data

- data in the form of different formats,	- data in the form of different formats,	+ data in a single form of format,
- very powerful computers or cloud computing and a very efficient internet connection are required,	- very powerful computers or cloud computing and a very efficient internet connection are required,	+ no need for very powerful computers or cloud computing and no need of a very efficient internet connection,
- lack of information on the interaction of operators with the control system.	- partial information on the interaction of operators with the control system,	+ practically complete information on the interaction of operators with the control system.

3.2.3. Data - process stage

The second stage of the analysis - Data, this is the process of processing and preparing data. Here, as standard, the data mining process is divided into four stages (Fig. 3.8.):

1. Data cleaning (to remove noise and inconsistent data)

2. Data integration (where multiple data sources may be combined)

3. Data selection (where data relevant to the analysis task are retrieved from the database)

4. Data transformation (where data are transformed or consolidated into forms appropriate for mining by performing summary or aggregation operations for instance)

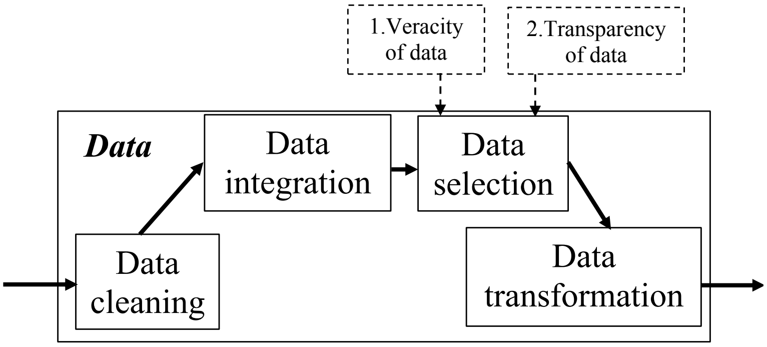


Figure 3.8. Inputs and Outputs of the different levels of control system (based on own study)

At this stage, the most important changes and proposals of the author concern veracity of the data and transparency of the data.

3.2.3.1. Veracity of the data

The veracity of the data, in this case, is primarily an exact definition of the parameters of operations or other recorded events. The author's experience shows that often in the case of manual records made by the operator it was not possible to link the description with the data from control systems due to negligence, misinterpretation of facts, exchanging the description with another event, etc. Therefore, it was assumed that the model is based only on data collected automatically by systems.

The position on the timeline is linked to the point of the veracity of the data and results from the frequent mismatch between manual entry time and automatically recorded data. This is due, among other things, to human errors, differences in system time set on controllers and real-time, etc.

The conjunction with an incorrect machine component is often caused by a lack of proper event identification.

One of the reasons for choosing such a form of data is human reliability and human performance aspects including error caused by unfamiliar/unrecognizable patterns [124] [123], spurious patterns, misleading indications [77], widely described in the literature. The influence of a human factor becomes relevant in two ways when its influence on functional safety aspects is analysed. Firstly, the interaction of the production operator with automation systems through HMI, SCADA, has an impact on the operation of the machine and its safety. Secondly, the information that flows to the production operator and / or maintenance operator in the form of ready-made analysis are also subject to human over organisational factors [150], [34] .

3.2.2.2. Transparency of data

The analysis data can be divided into several categories according to different criteria. The data can be divided into binary, integer, matrix and string data, among others. Data can also be categorised by cause or effect. This division is very important from the point of view of this dissertation because all events can be treated according to the cause and effect division. Input data is also varied due to its format. The format of the data is determined by the system to which it enters and the system from which it is exported. Apart from the value, each of the data, depending on the place from which it is obtained, has its own attributes. Such attributes can be input/output card number, logical address, time of occurrence, name, alias, division, zone, machine name, section name, etc.

$$\text{Event} = \{\text{value, card number, logical adress, time of occurence, name, etc..}\}$$

As can be seen from the description above, there is a lot of data available in different formats, in different notations and with different roles in terms of prediction. This means that in order to be able to process these data, it is necessary to prepare and process them properly and to collect them, if not in one place, then in a few specified places where they can be collected for processing and analysis.

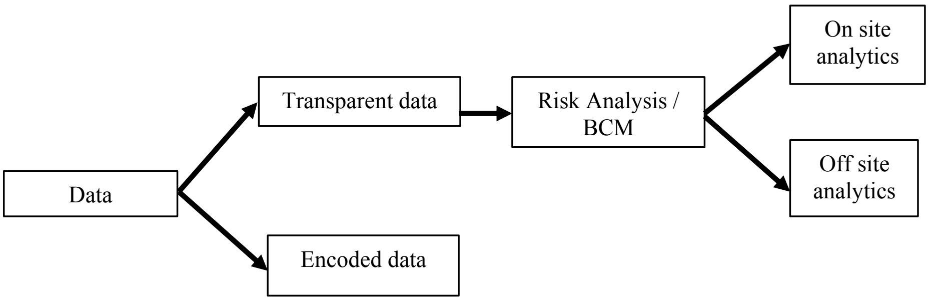


Figure 3.9. The selection of the type of data used depending on the risk analysis and BCM (based on own study)

In order to be able to make full use of the results obtained, it is necessary to identify the incoming data. Therefore, the data must be uniquely identified. The author suggests that despite the cost of losing certain information, the data should be unambiguously marked and identifiable for the user. This causes difficulties in terms of cyber-security and data security, including sensitive and confidential company data such as (recipes, process parameters, etc.). Therefore, one of the assumptions is that BCM and risk analysis should be performed in this aspect and the customer can choose whether the data processing can be performed through network tools or whether it must be based on a system located on the company premises (Fig. 3.9).

3.2.3. Prediction - process stage

This stage has two main parts: the first part is searching (by machine learning models) for or creating rules (expert rules), the second part is using the above-mentioned rules to predict events (Fig. 3.10).

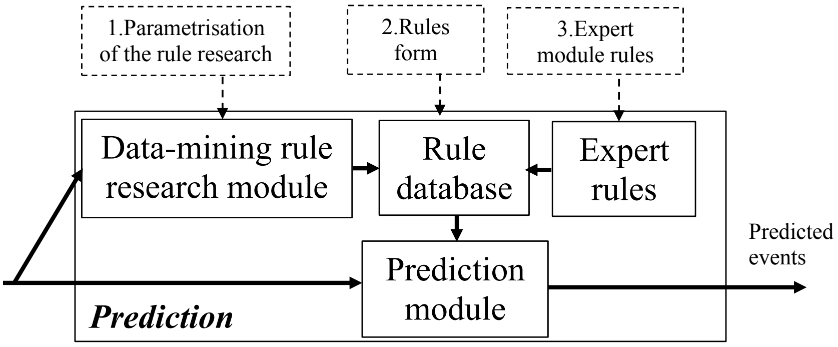


Figure 3.10. Stages of the prediction process (based on own study)

A data mining research module is a machine learning module used for data analysis to find rules from historical data. The expert module is an element of finding rules in an expert way. People with extensive experience in automation and control systems of a given object are able to propose new rules based on their knowledge, experience and knowledge of PLC program logic. The rules created either by the machine learning module or expert rules module are placed in the rule database. Then, the current event data, appearing on the analysed object, are "filtered" by a set of rules from the rule database, leading to the prediction of future events. The elements added here by the author are the parameterization of the rule search, allowing the user to control the rule search process. The second innovative element proposed by the author is the formulation of the rule database. The last element is the ability to add expert rules.

3.2.3.1. Parametrisation of the rule research

The resulting event and the preceding event are linked by a rule. Here too, there is a distinction. These rules can be divided into known (defined) and unknown rules. Known rules are rules that have been foreseen to exist at the planning, installation and commissioning stage and systems have defined appropriate actions in case of their occurrence. The second type of rules are unknown rules, rules that were not known at the project stage and no actions are defined in case of their occurrence.

Most of the simple rules were identified during the planning stage and are already used in control systems (level 1). However, they are also of interest to the author. During the analysis it was found that control systems inform the operator about the same event several or even several dozen times per hour and the total number of messages displayed to the operator reaches several dozen per minute. A very large number of displayed messages causes that they are completely ignored by the operator. This means that a low-risk situation that occurs multiple times could be the cause of failures.

Unknown rules are rules that often result from the interaction of a product with a machine and its control system or from human interaction with the machine or both.

In order to identify unknown rules, access to the widest possible range of available historical data is necessary. Data quality is also crucial. It is about their veracity, proper positioning on the timeline and connection with the relevant system/machine element. With the specified source and form of data, it is possible to proceed to the rule search method. The proposed model involves searching for rules, based on historical data collected and archived. Of course, the longer the history of events, the greater the probability of finding more rules. The analysis of historical data has been adopted in the model because of the fact that the most troublesome failures in machinery occur with a certain frequency, the disadvantage of this assumption is the lack of complete knowledge about all potential failures. However, the model assumes cyclical execution of rule searches within the Deming cycle, which causes the number of potential undetected rules to decrease with each new rule search cycle.

In order to carry out data mining, with a focus on finding association rules, two parameters need to be precisely defined: minimum support level (Eq 3.5 and Eq 3.6) and minimum confidence level (Eq 3.6 and Eq 3.7).

$$s \geq minSupp \tag{3.5}$$

$$1 \geq minSupp \leq 0 \tag{3.6}$$

$$z \geq minConf \tag{3.7}$$

$$1 \geq minConf \leq 0 \tag{3.8}$$

Support *s* is greater than or equal to a certain minimum threshold, marked *minSupp*, and whose confidence *z* is greater than or equal to a certain minimum threshold, marked *minConf*. Proper selection of these parameters has a major impact on the final result of the rules found, and more specifically on their number. The level of support is used to regulate the number of frequent sets, from which the association rules are then created. The level of confidence, on the other hand, regulates which of the rules are sufficiently reliable, i.e. with what minimum probability a given rule is present in the examined data sets. Increasing the support level reduces the number of selected frequent datasets, and the confidence level reduces the number of association rules found. Decreasing both values respectively increases the number of frequent sets and rules association.

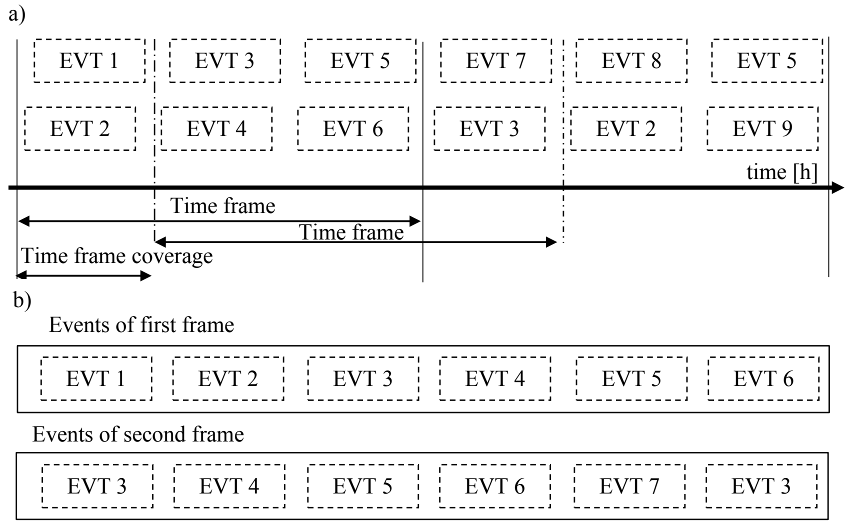


Figure 3.11. Data flow in the data analysis process (based on [47])

Another important parameter is the length of the time frame (Eq 3.9). A time frame is a length of time (in hours) into which historical data are divided and grouped and in which it is assumed that an antecedent and consequent event occur (Fig.3.11).

$$0 \leq TimeFrame \leq \mathrm{T_r} \tag{3.9}$$

The parameter related to the time frame is the time frame coverage parameter (Eq. 3.10). It determines how much time frames overlap; its value is a compromise between the accuracy of the analysis and the load of the computer system data analysis.

$$0 \leq TimeFrameCoverage \leq T_{r1} \tag{3.10}$$

Another parameter is the analysis refresh rate parameter (Eq. 3.11). This parameter is about how often the historical database is to be searched for new association rules.

$$0 \leq AnalysisRefreshRate \leq T_{r2} \tag{3.11}$$

3.2.3.2. Rules form

An important element of the prediction stage is the rule database (Fig. 3.12). Through the rules stored in this module all current events will be filtered out, and on the basis of those

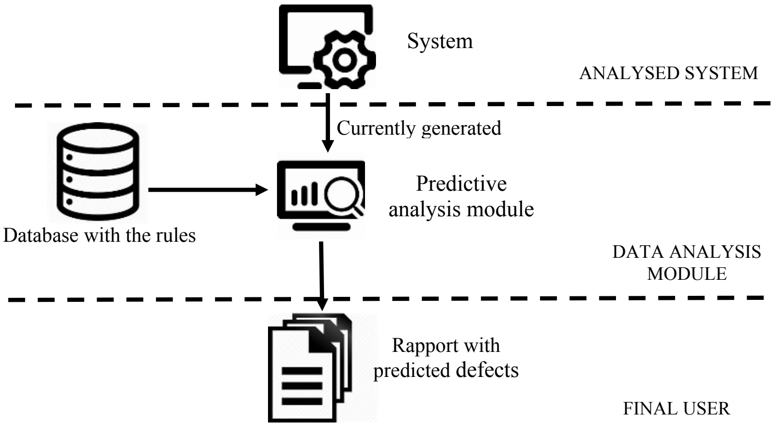


Figure 3.12. Data flow in the data analysis process (based on own study)

rules, events are predicted. For the prediction to be understandable and useful for the user it is necessary to correctly define parameters for each rule.

Table 3.4. Specification of the criteria for each rule

A set of parameters for each rule	
1	*Location in zone, subzone, etc.*
2	*Previous event (antecedent) or more previous events*
3	*Conditions for inclusion or non-sequential occurrence of several preceding events*
4	*Maximum time from the previous event used in analysis.*
5	*Number of occurrences of the preceding event*
6	*Estimated time data of occurrence of the event (e.g.: minimum/maximum time between the predecessor and the successor, expected value (μ) of normal distribution)*
7	*Expected event (consequent)*

The author proposed a list of seven required parameters for each rule (Table 3.4).

a) The first parameter concerns identification of the physical location of the element to which the rule applies. This is key information due to the response time. It is possible that an identical element can be found in several places of the same machine or production line, but depending on the location it is subject to completely different factors.

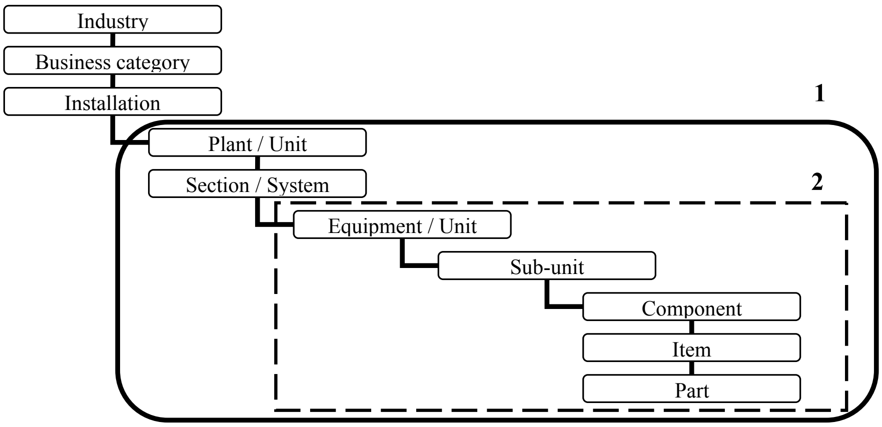


Figure 3.13. Equipment taxonomy examples compliant with the ISO standard [66]

Location identification (Fig. 3.13) is also important when selecting the depth of rule search, e.g.: rules can be searched within one plant unit (selection 1), one equipment (selection 2), or another selected taxonomy level.

b) The second parameter is related to the specification of the event or sequence of preceding events. The author assumed that apart from one possible preceding event, there may be n precedent events whose occurrence will cause the i-subsequent event to occur (Eq 3.12). An example of such an event can be: overfilling the scale with raw material (antecedent -event 1), acceptance of this weight by the operator in the HMI (antecedent -event 2), dropping the raw material on the feeding conveyor and stopping the conveyor (consequent) by switching off the over-current motor breaker in the power supply circuit of the electric motor powering the conveyor.

$$antecendant_1 \text{ and } antecendant_2 \text{ and } \dots\ antecendant_n \text{than } consequent_i \tag{3.12}$$

c) The third point concerns conditions for inclusion or non-sequential occurrence of several preceding events. At this point, it is clarified whether the order of occurrence of the symptoms is interesting for the client, in case of more than one. Therefore, it can be assumed that in some cases the sequence of events influences the occurrence of the event (Eq 3.13 and Eq.3.14 and Eq.3.15). The example from the second point is an example in which the sequence of symptoms is important. An example where the order of symptoms does not matter is the hydraulic cylinder unit connected to the ram system. To consider this system as blocked, two symptoms are needed: no change of position and high hydraulic oil pressure. Depending on the situation, these symptoms appear in variable order and this does not affect the final result.

$$antecendant_1 \wedge antecendant_2 \rightarrow consequent \qquad (3.13)$$

$$antecendant_2 \wedge antecendant_1 \rightarrow \neg consequent \qquad (3.14)$$

or

$$antecendant_2 \wedge antecendant_1 \rightarrow consequent \qquad (3.15)$$

d) The fourth parameter presented concerns maximum time from the previous event used in the analysis (maximum time interval - Eq. 3.14). When choosing the value of this parameter, the user decides what period of time he is interested in (by assumption, what is the time when there is a real correlation of cause and effect between these events).

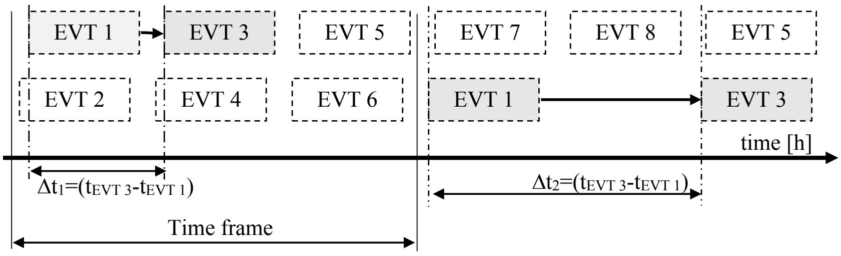


Figure 3.14. Example explaining maximum time between antecedent and consequent

The example shows two cases of rule occurrence with different times between antecedent and consequent. Rule presented on the Fig. 3.14.is in the form if EVT 1 than EVT3.

$$Maximum\ time\ interval(A \rightarrow B) = Max(\Delta t_1, \Delta t_2, ..., \Delta t_n) \qquad (3.16)$$

The maximum time from the occurrence of the first symptom to the occurrence of the event must not be greater than the timeframe set in the search rule parameters (not applicable to expert rules) (Eq. 3.17).

$$Maximum\ time\ \mathrm{int}\,erval(A \rightarrow B) \leq Timeframe(A \rightarrow B) \qquad (3.17)$$

e) The number of occurrences of the preceding event is the fifth point of the rule parameters. This is an important element as there are rules in which a single occurrence of a symptom is not sufficient for a rule to occur. As described above, the author divided the rules into two categories. Rules known and unknown.

Rules that are known in themselves are not the subject of the work, because by definition they are known and used by the designers of a given system. However, the important aspect is that just because something is known does not mean that it is used.

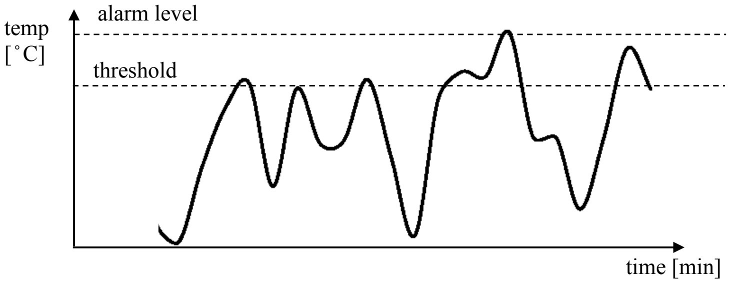


Figure 3.15. Example explaining threshold and alarm levels (based on own study)

The author has met many times with examples where the excess of information reaching the operator caused the symptoms to be ignored and resulted in a failure. Additionally, in the machinery, it is possible to see that the failures are repetitive. Not all root causes of failures are eliminated. It could even be argued that most root causes are not dealt with. Most systems are not redundant due to the cost/potential loss ratio. The same reason often leads maintenance departments that do not eliminate some of the root causes because of the high cost of rebuilding machinery or because of the unification requirements of machinery in the plant/organisation or the inability to put machinery out of production for modification, the small impact of the failure on losses, and ultimately a lack of competence in detecting root causes or performing modifications. Therefore, the proposed model takes into account the rules known in terms of the number of symptoms and their frequency of occurrence (Eq. 3.18). The example shown in Fig. 3.15 shows a diagram of the oil temperature in a hydraulic unit tank. As can be seen from the graph, there is a threshold (symptom) and an alarm level at which the unit will stop. A single occurrence of an event (reaching a temperature level exceeding threshold 1) is not associated with the occurrence of a failure.

$$if \sum |symptom| \geq N \rightarrow event \tag{3.18}$$

After the fourth (switching of the input - ascending slope) temperature exceeding the alarm temperature threshold has occurred. This information can be used and after the second (in case of a repeatable situation) exceeding the temperature, the information about the failure can be generated. Another example of the number of symptom repetitions can be a limit sensor mounted on one side of a conveyer belt, which was attacked 25 times in 10 minutes. Based on these facts, it can be stated that the product has passed under the conveyer belt and corrective action is required.

f) The sixth parameter specified by the author concerns the parameters of the obtained rules in terms of the time of their occurrence based on previous timing. On the basis of the revealed rules, a predicted period of time during which the predicted event occurs may be given. These values are given as the minimum [min] observed time (Eq 3.19) from the preceding events, the maximum [max] time (Eq. 3.20) and the expected value (μ) (Eq. 3.21) of the normal distribution (Fig. 3.16) (Eq.3.22), i.e. the arithmetic mean of the recorded events of that particular rule.

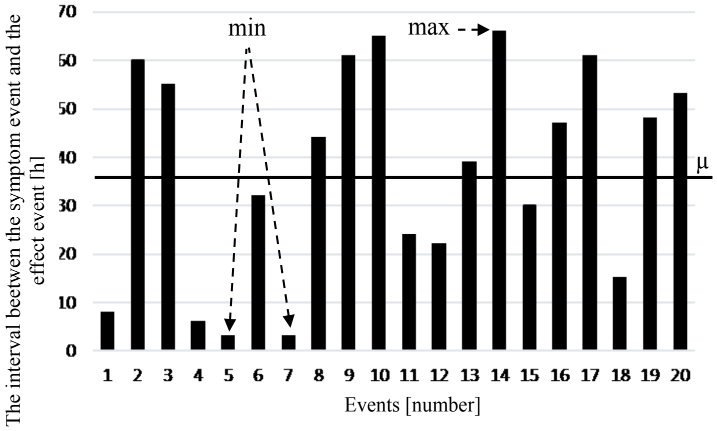


Figure 3.16. Graphical representation of min and max values and the expected value of the time period between the antecedent and the consequent (based on own study)

If a rule occurs more than defined by the user number of times, the minimum and maximum value of two standard deviation (2σ) may be given instead of the minimum and maximum value. For the normal distribution, two standard deviations from the mean value account for 95.45 percent of the set;

$$MinT(A \to B) = Min(t_1, t_2, ..., t_n) \tag{3.19}$$

$$MaxT(A \to B) = Max(t_1, t_2, ..., t_n) \tag{3.20}$$

$$\mu = \frac{\sum_{i=0}^{n}(t_n)}{n} \tag{3.21}$$

$$if \sum\left|(A \rightarrow B)\right| \geq N \text{ than predicted time} \approx \mu \qquad (3.22)$$

In giving time of expected event occurrence, it should be taken into account that the analysed object is subject to changes and the detected events may be subject to analysis ending with some modifications, which means that the system should capture these changes by analysing the time between the occurrence of events (Fig. 3.17) or if there is a significant change in the value of expected normal distribution, the time between the symptom event and the effect event (Fig. 3.18).

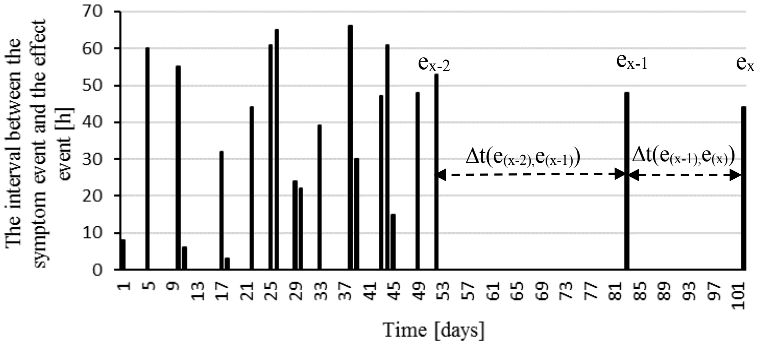


Figure 3.17. Graphical presentation of the reduction in the frequency of the event (based on own study)

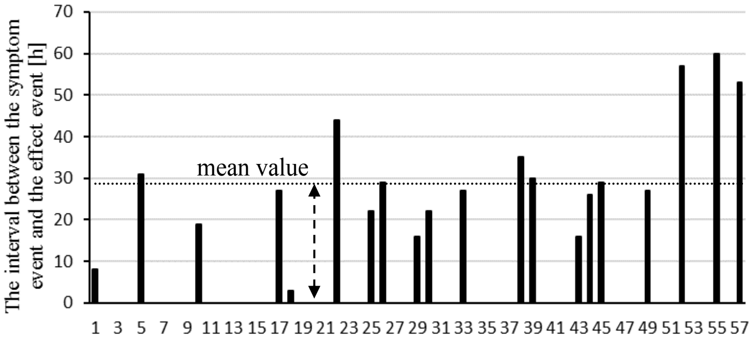


Figure 3.18. Graphical presentation of the increase in the interval between the occurrence of the predecessor and the successor of a specific rule (based on own study)

Both of these changes can be tracked either systematically by an expert or automatically using a tool featuring linear regression analysis or deep neural networks.

3.2.3.3. Expert module rules

The last element proposed by the author in the prediction process is the expert rules module. This functionality significantly increases the possibilities of the prediction tool. This tool allows using the knowledge of people working with machines on a daily basis. Tools analysed by the author do not use this option. This tool can be used to implement known rules, as already mentioned before. According to the author, this module should primarily contain rules:

- repetitive events (for which the cause of the original event was not removed for various reasons),
- events previously described in threshold-based rules,
- events that have been detected on other identical (twin) or very similar machines
- rules for enforcing the level of functional safety.

3.2.4. Action- process stage

The last stage is - Action, this stage consists of generating appropriate reports tailored to the user and taking appropriate actions to prevent the anticipated events Fig. 3.19. The author proposed two main actions here. Allocation of received data and data-based model of operation.

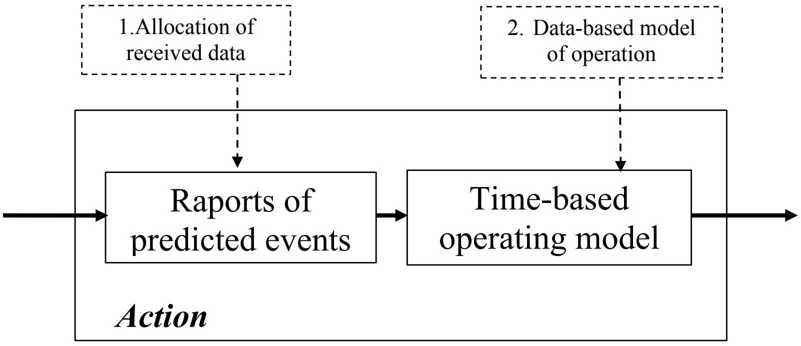

1.Allocation of received data
2. Data-based model of operation
Raports of predicted events
Time-based operating model
Action

Figure 3.19. Inputs and Outputs of the different levels of control system (based on own study)

This solution proposed by the author is innovative due to the fact that apart from the presentation of the obtained results, it also takes into account the assignment of appropriate results to the addressees and the selection of corrective actions.

3.2.4.1. Allocation of received data

The data obtained in the report must be delivered quickly to the final customer of this data. The author presents an option to deliver different data to several types of clients and a division into reports according to the estimated time to event (Fig. 3.20).

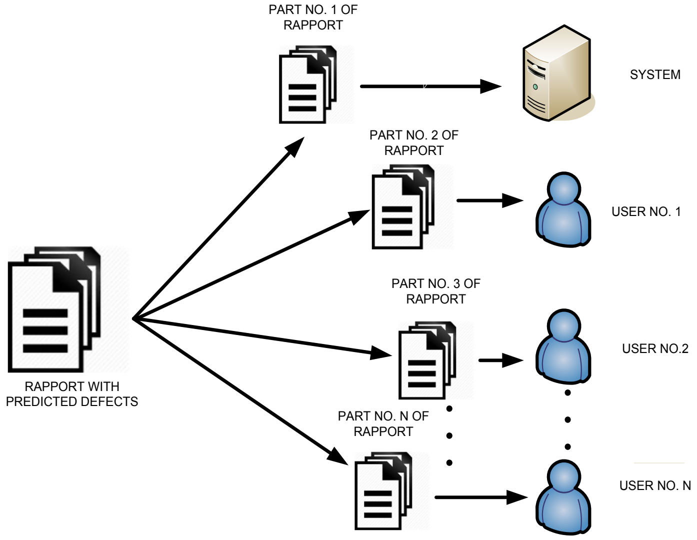


Figure 3.20. Distribution of the report to users as a function of the time remaining to the expected failure (based on own study)

The first division results from the minimum human reaction time. The author assumed, on the basis of the literature, that if the time of the predicted event is less than 3 minutes, then due to the limitations of human reaction (Eq 3.23), the report on such situations must be processed by the system and the actions must be taken independently of humans.

$$t(A \rightarrow B) = \begin{cases} \leq 3\,\text{min} & \text{automatic system reaction} \\ > 2\,\text{min} & \text{defined user reaction} \end{cases} \tag{3.23}$$

The selection of the person to whom the report is addressed is based on three criteria (Fig. 3.21): the physical distance between the user and the interface with the machine or the machine itself, the competence of the user, and the time that event is expected to occur.

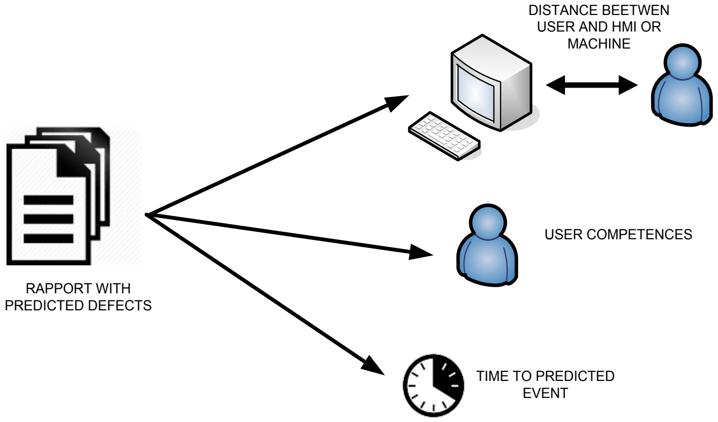

DISTANCE BEETWEN USER AND HMI OR MACHINE
USER COMPETENCES
RAPPORT WITH PREDICTED DEFECTS
TIME TO PREDICTED EVENT

Figure 3.21. Criteria for selecting a client of predictive reports (based on own study)

The distance of the user from the operator panel or the machine is an important criterion in terms of the time between the occurrence of a symptom and an event. Therefore, for example, it is optimal (with a short-expected time to event) to address reports to the user as close to the machine as possible. The second important criterion is the competence criterion. The competence of the user must make it possible to prevent an event from occurring after receiving information. Therefore, depending on the machines, it may be possible to adjust the competence of operators to the needs of prediction or to relocate maintenance services or other services with adequate competence to the defined prediction needs. The third common criterion is the time that is predicted from the symptom to the occurrence of the event. It is the distance between the operator and the machine that depends on it, the time needed to take action and the type of action. All three criteria influence each other and determine the choice of the recipient of the report.

As an example of the application of this method, the author chose an extensive system with multiple prediction elements:

a) failure prediction,
b) cyber-attack prediction,
c) prediction of safety anomalies,
d) prediction of quality deviations.

Table 3.5 A table indicating the time frames defined and the corresponding system/persons and actions

Interval	Who	What
0 – 3min.	Control system	Defect prediction ad-hoc action Cyber-attack prediction ad-hoc action Safety prediction ad-hoc action Quality deviation prediction ad-hoc action
3 min. – 4 hr.	Advanced Autonomous Maintenance Operator	Defect prediction ad-hoc action Cyber-attack prediction ad-hoc action Safety prediction ad-hoc action Quality deviation prediction ad-hoc action
	Quality specialist	Modification of line parameters based on predicted quality deviations
4 hr. – 1 week	Supply chain specialist	Updated delivery plans to the customer

	Quality specialist / Maintenance Engineer	Small stops cause detection
1 week – 1 month	Maintenance Engineer Quality specialist	Spare parts inventory management Planning-scheduling management Realization of small modification Update of rules based on data lake information’s Update of procedures Energy efficiency optimization
1 month – 1 year.	Maintenance engineer Plant management	Risk analysis updates Decision about investments/ modifications/ digitalization/ robotization or humanization BCM actualization

Prediction of these events requires, apart from immediate actions and potentially ad-hoc, medium and long-term actions, such actions are defined in Table 3.5:

a) Ad hoc

- Failure prediction
- Cyber-attack prediction
- Safety prediction
- Quality deviation prediction action

b) Medium-term

- Modification of line parameters based on the prediction of quality deviations
- Updated delivery plans to the customer
- Analysis of causes of micro stoppages
- Spare parts inventory management
- Planning-scheduling management
- Realisation of small modification
- Update of rules based on data lake information's
- Improvement of procedures
- Optimising energy efficiency

b) Long-term

- Modification of risk analysis
- Decision on investment/modification/digitalisation of robotization or
- BCM analysis update

This example shows that the high effectiveness of the proposed method requires a change in approach and involvement of many different departments (quality, planning, production operators and maintenance). This is a change in the process of data flow and taking into account a new type of information such as predictive data.

3.2.4.2. Data-based model of operation

The method of selecting the recipient of the report has been proposed by the author above. This section will present the approach to medium and long-term actions. In order for the prediction to be beneficial, the information obtained in the report should be used, forcing one of the action scenarios:

- The undertaken actions will prevent the failure from occurring (Root cause elimination);
- Potential losses will be minimised if a failure cannot be avoided;
- The failure will not be repeated in the future;
- The failure will significantly reduce its frequency;
- The time between the symptom and the failure will be much longer;
- The control system will automatically take action to eliminate or minimize the impact of the failure.

a. The undertaken actions will prevent the failure from occurring;

The presented event will be analysed, which will result in finding the root cause of the failure. In the next step, there will be an action aimed at completely eliminating the possibility of factors causing this type of failure to occur in the future (Fig. 3.22) by e.g. modifications, change of parameters, change of procedures, adding elements of diagnostics, etc.

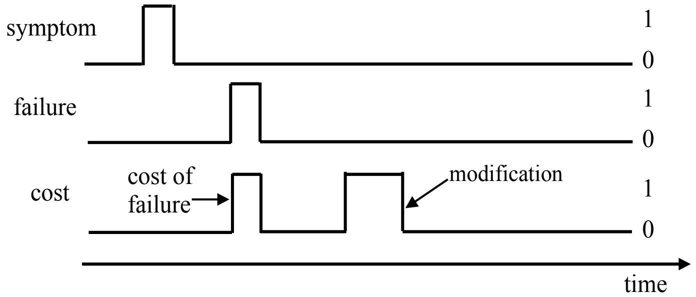


Figure 3.22. Chart of relations between costs, failures and symptoms and actions taken for options a

b. Potential losses will be minimised if a failure cannot be avoided;

The analysis will be done as in the point above. However, due to the lack of technical or cost accounting capabilities to completely eliminate the occurrence of the event, an analysis of the risk of its occurrence will be performed. Once the risks have been determined, actions will be taken to minimize the impact of the estimated risks of this failure on the system in order to limit potential damage to an acceptable level (Fig.2.23).

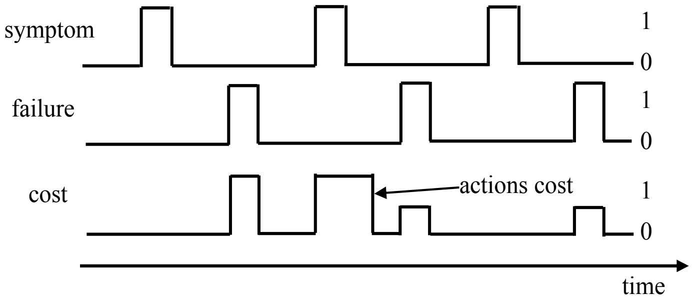


Figure 3.23. Chart of relations between costs, failures and symptoms and actions taken for options b

c. The failure will not be repeated in the future;

An analysis like in the first point will be carried out and the possibility of avoiding the failure (not eliminating it completely) by preventive measures (Fig. 3.24), e.g. introducing systematic replacement of parts will be identified.

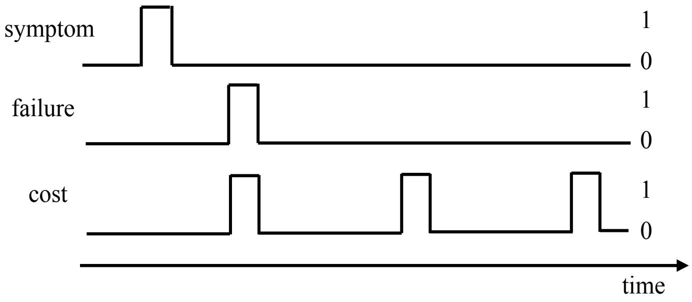


Figure 3.24. Chart of relations between costs, failures and symptoms and actions taken for options c

d. The failure will significantly reduce its frequency;

The failure will be identified and for economic, technical or identified low hazard reasons, only action will be taken to reduce its frequency in the future (Fig. 3.25).

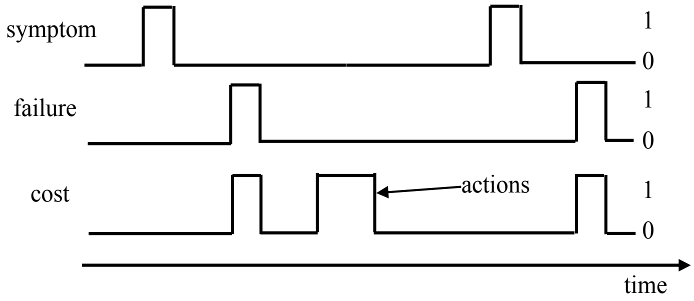


Figure 3.25. Chart of relations between costs, failures and symptoms and actions taken for options d

e. The time between the symptom and the failure will be much longer;

In this case, the analysis carried out will show that from the user's point of view, there are sufficient measures to increase the time between the occurrence of the predecessor and the occurrence of the failure. This will give the user sufficient time to take preventive action (Fig.3.26).

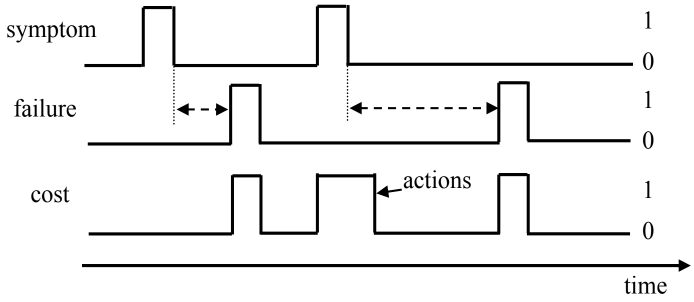


Figure 3.26. Chart of relations between costs, failures and symptoms and actions taken for options e

f. The control system will automatically take action to eliminate or minimize the impact of the failure

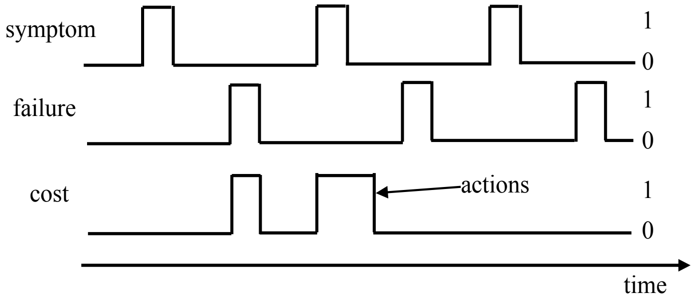


Figure 3.27. Chart of relations between costs, failures and symptoms and actions taken for options f

due to the short time between the predecessor event and the failure, which makes it impossible for a human to act effectively, and due to the technical capabilities of the object. The control system will receive information about the presumed failure and change the configuration of the process, so that the product produced on this line/equipment will have the same parameters as in the case of no failure, or will also cause the output product not to be a waste product (it will be suitable for reprocessing or will need to be repaired in the next stage or a separate process) (Fig. 3.27). As an example, a paper mill can be used here, where a failure of heating elements at the beginning of the process can be compensated by a change in line speed and an increase in temperature of subsequent heating elements occurring in subsequent stages. Due to such an action, the product is not a waste and it is possible to prepare for maintenance intervention by shortening the downtime itself.

3.2.5. Integrated approach

In the presented dissertation two main issues were taken into account by the author. These are the prediction of machine failures and the prediction of safety anomalies. Failures prediction is the first, next to safety deviation detection, author's idea to apply the created method. Minimizing the losses associated with unplanned stops is quite a challenge nowadays, as most of the available techniques in maintenance are at a high level and it has been difficult to make significant progress for several years. The proposed tool gives new possibilities to the maintenance departments and allows to increase the profitability of owned installations.

The second subject of analysis is safety deviation prediction. Today, safety systems are an integral part of machinery or equipment and despite very advanced technologies, the safety aspect still appears in manufacturer presentations as an element that can be developed. This is due to the continuing occurrence of accidents or dangerous events when working with machines. Therefore, the elements of prediction proposed by the author can also maintain the level of safety and be a supporting system for risk analysis. Unfortunately, the elements of safety systems are still vulnerable to human error, especially when it comes to errors in the firmware of control elements, analysis of micro stoppages due to safety systems or operator behaviour. The second application on this subject is a comprehensive analysis of device data and human interaction with the system that can help to detect rules and show the frequency of certain actions or reactions of the system that have not previously been taken into account in risk analysis.

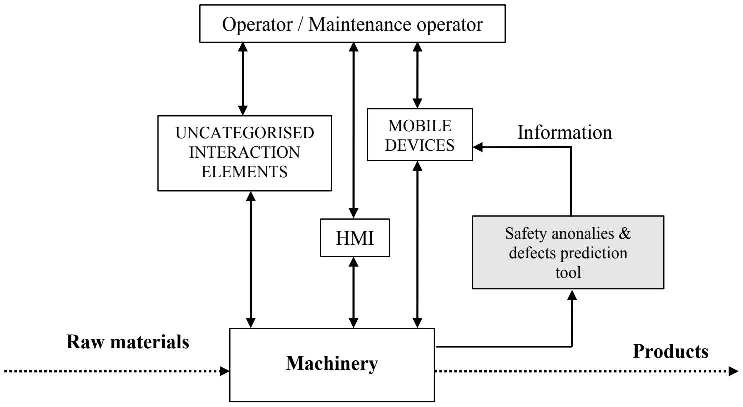

Operator / Maintenance operator
UNCATEGORISED INTERACTION ELEMENTS
MOBILE DEVICES
Information
HMI
Safety anonalies & defects prediction tool
Raw materials
Machinery
Products

Figure 3.28. Tool proposed for operators in time reaction between 3 minutes up to 16 hours (based on own study)

The comprehensive proposed solution predicts events concerning safety anomalies and predicts failures. Prediction of functional safety events is based on the beginning of implementation of expert rules. Two graphs for two types of recipients of predictive reports are presented. On the first one, concerning failures that are expected to occur within 3 minutes to 16 hours, the reports are sent to operators and maintenance employees using mobile devices (Fig. 3.28). Their reaction via HMI, mobile devices and other available ways for interaction with the machine is aimed at preventing a failure or functional safety threat in an ad-hoc perspective.

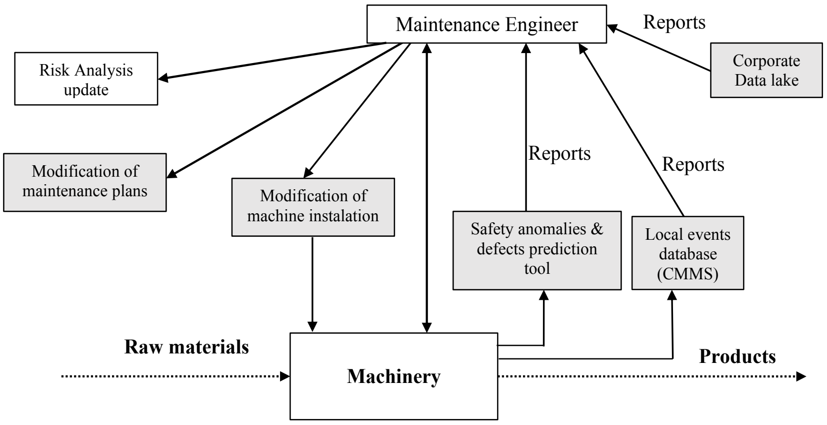

Maintenance Engineer
Reports
Corporate Data lake
Risk Analysis update
Modification of maintenance plans
Modification of machine instalation
Reports
Reports
Safety anomalies & defects prediction tool
Local events database (CMMS)
Raw materials
Machinery
Products

Figure 3.29. Tool and actions proposed for maintenance engineer (based on own study)

The second graph presented (Fig. 3.29) refers to the work of a maintenance engineer. Here, the activity profile is medium and long term. This means that the predictive reports are provided in a different form, more as a summary. Additionally, the engineer receives data from the local event database (CMMS) about all the events that occurred recently. He can receive information via corporate data lake about important events and newly defined rules that occur on twin installations. All this information is used to modify maintenance plans, perform/plan machine modifications and update risk analyses.

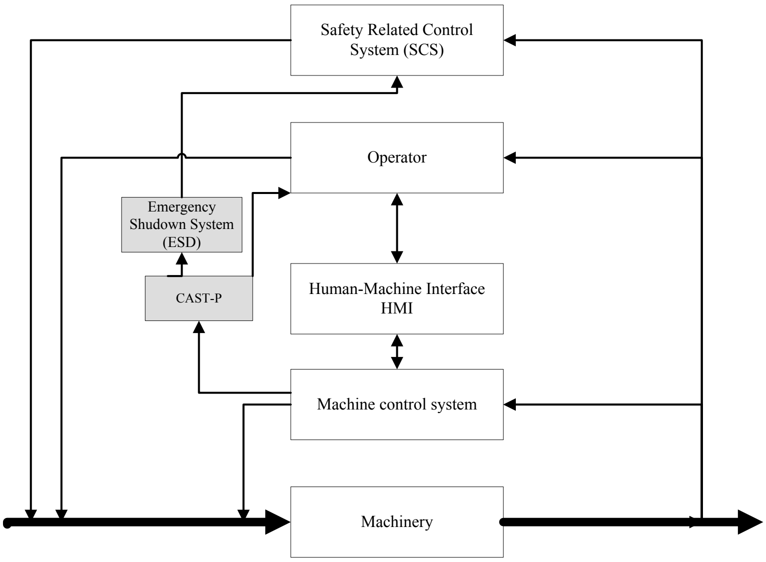
3.2.6. Functional safety system malfunction detection

To ensure coverage for this type of non-compliance, a failure mode and effect analysis (FMEA) is needed that takes into account the main criteria of safety standards and potential risks of injury. After performing this analysis, it is possible to create a whole database of expert rules that in the case of anomalies will stop the production line immediately.

Unfortunately, parts of these rules are not detectable by the prediction system either by basket analysis or DNN because they do not cause shutdowns. Consequently, there is a need for appropriate categorisation of those potentially hazardous events (in terms of antecedent - consequent)

It could be stated that hardware or software errors of delivered products do not exist anymore with so complex international, national and internal regulations and standards, quality verification of product, design to quality and many other organisational and technical methods to eliminate risk for the client. Unfortunately, it quite frequently can be heard in different media about service action of cars in which some safety or reliability problems have been detected after they were sold on the market. The same situation has taken place in equipment produced for industrial use. During the last few years, such incidents also were noticed by the author as a firmware update or product exchange according to safety risk.

Unfortunately, global producers are also making glaring mistakes. According to Polish legislation, the user is responsible for the use of the equipment. Therefore, it is the responsibility of securing oneself in case of similar events as described above. The above-described event was directly related to non-compliance with standards ISO 12100 [62] and ISO 14118 [65]. To protect against such events, the author proposes to use the CAST-P tool developed and presented in a previous subchapter.



Safety Related Control System (SCS)
Operator
Emergency Shudown System (ESD)
CAST-P
Human-Machine Interface HMI
Machine control system
Machinery

Figure 3.30. Schema of tool for safety anomalies detection (based on own study)

Modification of the CAST-P system in relation to the previous solution consists in adding an output signal connected with the automation system (level 1) which after detection of an anomaly would stop the whole production line with a message for the operator about the detected safety irregularity as shown on Fig.3.30.

3.2.7. Outline of the proposed functional test interval optimisation

A certain extension of the safety anomaly prediction method discussed so far is the proposed test interval optimisation method. This is because once an anomaly has been detected, appropriate action must be taken to reduce the risk sustainably over time. This is presented in fig. 3.31 and will be discussed further in this section. At present, all machinery approved for use in the EU must comply with certain safety standards. In the case of machinery, these are usually standards IEC 61508 [56], IEC 62061[57] and ISO 13849 [63]. This is generally done by means of the risk analysis process described in Chapter 2, followed by a risk reduction process and finally the installation of risk-appropriate safety functions. Up to this point, everything in almost every plant is running according to safety standards.

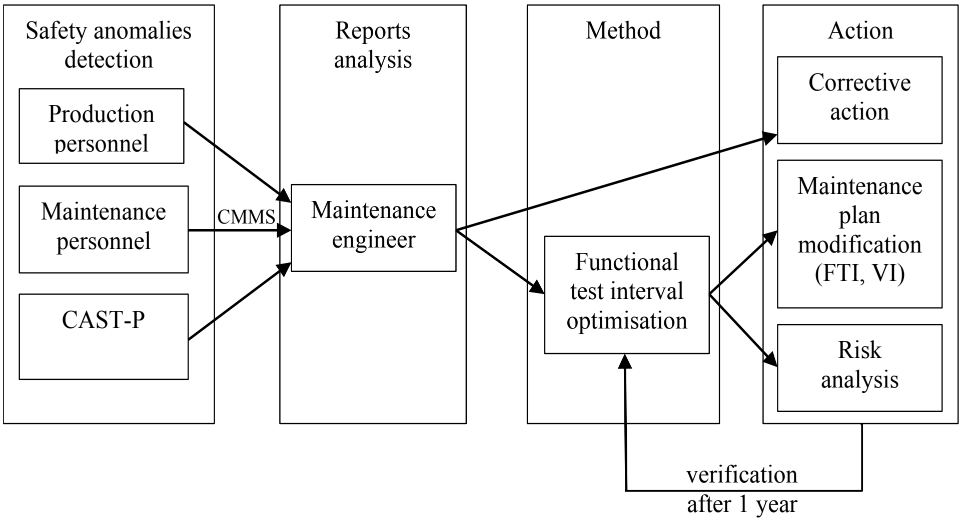


Figure 3.31. Scheme for responding to functional safety anomalies detected

Unfortunately, once these machines have been installed at their place of operation, due to human factors (e.g. turnover), the environment, or a change in the quality of the raw materials, the scope of functional tests originally adopted does not guarantee that the required SIL will be maintained. An example of this is the effect of changing raw materials - an increase in viscosity causing the temperature sensor to stick, or the use of raw materials with a higher hardness causing faster mechanical wear of the temperature sensor. Another example is the employee turnover and reduced competence of operators. Unfortunately, they are much more likely to make mistakes and generate physical damage to equipment when handling means of transport than experienced workers. Many potential risks can be revealed from both the predictive tool and the day-to-day activities of maintenance and production personnel. This risk is very often overlooked because it has become a common misconception among engineers that, according to Fig. 2.20, restarting the risk analysis process is only done if the machine is modified or the purpose of its use is changed (which can also be regarded as an gap in the standard) - this is the first reason. The second reason is that in medium and small-sized plants the machines are often purchased off-the-shelf (the risk analysis is done by the machine supplier) and the process of functional safety life cycle management is unknown as there is no such competence within the end user company.

New emerging risks affect to decrease the PFH_D value of safety functions through the increased failure rate of detectable and non-detectable failures. Which consequently leads to a reduction in SIL and an increase in risk.

The author has noticed this risk and in order to eliminate it, proposes a method that uses frequency increase or additional functional testing as a tool to reduce the risk and return the safety function to its original SIL level. It is important to underline that the proposed method is an enhancement and not a replacement of existing standards.

The method consists of three steps. The first is the identification of new influencing factors. The second is a verification based on a decision matrix. The third stage is to put the actions from the matrix into practice. This method is easy to implement for any maintenance worker with an average level of experience. No expert knowledge of functional safety is needed.

- First stage

For some machines equipped with safety function and complementary protective measures working in high demand mode but infrequent operation because of construction, the specification of production, ergonomics, thermal influences, solid sediments, corrosion, temperature, corrosion, vibration, impact, humidity, personnel - elements of safety function may be deteriorated. That, in the future, can result in incorrect operation of the safety function. The factors listed above form a list of factors that may adversely affect the safety function. Based on information's from production and maintenance operators or information from a predictive tool, the maintenance engineer decides to verify these symptoms using a checklist from Table 3.6. The checklist should be completed on the basis of the results of inspections and/or the failure register of the safety function components.

Table 3.6. A table with a checklist to serve as a template for verification.

Staff influence		Applicable [Y/N]	Detectable [Y/N]	Occurrence frequency [per year]	Remarks
A.1	Use of a guard as a stop button				
A.2	Damaging machine by forklift				
A.3	Putting things away on safety elements				
Media influence		Applicable [Y/N]	Detectable [Y/N]	Occurrence frequency [per year]	Remarks
B.1	Corrosion				
B.2	Temperature				
B.3	Abrasion				

B.4	Pollution				
Environment influence		Applica-ble [Y/N]	Detectable [Y/N]	Occurrence frequency [per year]	Remarks
B.1	Temperature				
B.2	Solar heating				
B.3	Dirt				
B.4	Corrosion				
B.5	Shock				
B.6	Vibration				
B.7	Humidity				
B.7	Radiation				
Technological links		Applica-ble [Y/N]	Detectable [Y/N]	Occurrence frequency [per year]	Remarks
B.1	Cavitation				
B.2	Corrosion				
B.3	Condensation				
B.4	Pulsation				

- Second stage

To assure that safety functions or complementary protective measures are still able to fulfil their function, the author proposes to make the verification shown in Table 3.7 on the basis of checklist (Table 3.6) from the first stage.

The presented method creates a matrix with corrective actions. The first criterion considered is the ability to detect a failure, either by visual inspection or by diagnostics but with the condition of eventual failure detection without stopping the machinery. The second category is the frequency of occurrence of deviations. It is divided into low, medium and high.

Table 3.7. Graph of additional action for systems working in low demand mode

		Detection	
		Possible	Impossible
Frequency of occurrence	Low	N/A	FTI
	Medium	VI	FTI
	High	FTI	Risk Analysis

where:

N/A	-	No action necessary,
VI	-	Visual inspection,
FTI	-	More frequent time interval;

Risk Analysis - A full risk analysis is required - there is a high probability of need to change the design of the machine or the safety features.

As a result, four possible scenarios can be obtained. First, with the lowest risk finish with no actions. The second result is adding into the maintenance plan an additional proof test consisting of visual verification of safety function elements, or complementary protective measures elements state. The frequency of that inspection should be not less than twice as often as the period between two proof or functional tests. The third action is an increase in the frequency of proof or functional test intervals. The frequency of the test should be not less than twice the period between two known accidental activation. In the last scenario, a full risk analysis according to standard 12100 [62] is necessary as there is a high probability that the machine design or safety functions will need to be changed in order to maintain the required SIL level due to newly identified risks. In this case, a company without competence in its own team has to support itself with experts from outside the company.

- Third stage

The last stage is the implementation of the actions resulting from the application of the matrix from the second stage. In addition, a date should be set for the next application of the proposed method. The revision frequency suggested by the author is one year.

3.2.8. Other potential applications for the introduced method

On the basis of experience and analysis of the needs for solutions in manufacturing companies, the author has identified, apart from the two more widely discussed above applications (failure prediction and safety deviation prediction), further possible areas of application of the presented method. The presented method is applicable to the following areas identified by the author (Fig. 3.32):

- Cyber security attack
- Detection of quality deviations cause
- Energy efficiency optimisation
- Analysis of operator behaviour

Description of each of the areas of use:

- Cyber security attack

The multitude of abnormal values collected from a machine can be indicative of a cyber attack on an industrial installation, and with established rules that take into account the most critical parameters of the machine, a potential attack can be identified and countermeasures can be taken very quickly.

The two diagrams shown present the operation of the system for cyber security detection. As Fig. 3.33 shows, the standard control and security system has been enhanced with the CAST-P module and emergency shutdown system. This is due to the fact that in the case of cyber security threats, action should be taken very quickly and human reaction time would be too long to effectively mitigate the effects of threats. Therefore, after predicating a cyber attack threat, the system stops the machines independent of other systems. This is due to the fact that, as an independent system, it is not vulnerable to infection.

Additionally, the operator is informed about the prediction of the event. The predictive system is a separate system independent of the functional safety anomalies and failures prediction system (Fig. 3.34). To avoid false stoppages, the system should be equipped with independent sensors on the basis of which the prediction could be confirmed and the machine stopped. The CAST-P solution presented above can also be used for detection of malicious threats or cyber-attacks and counteracting their effects.

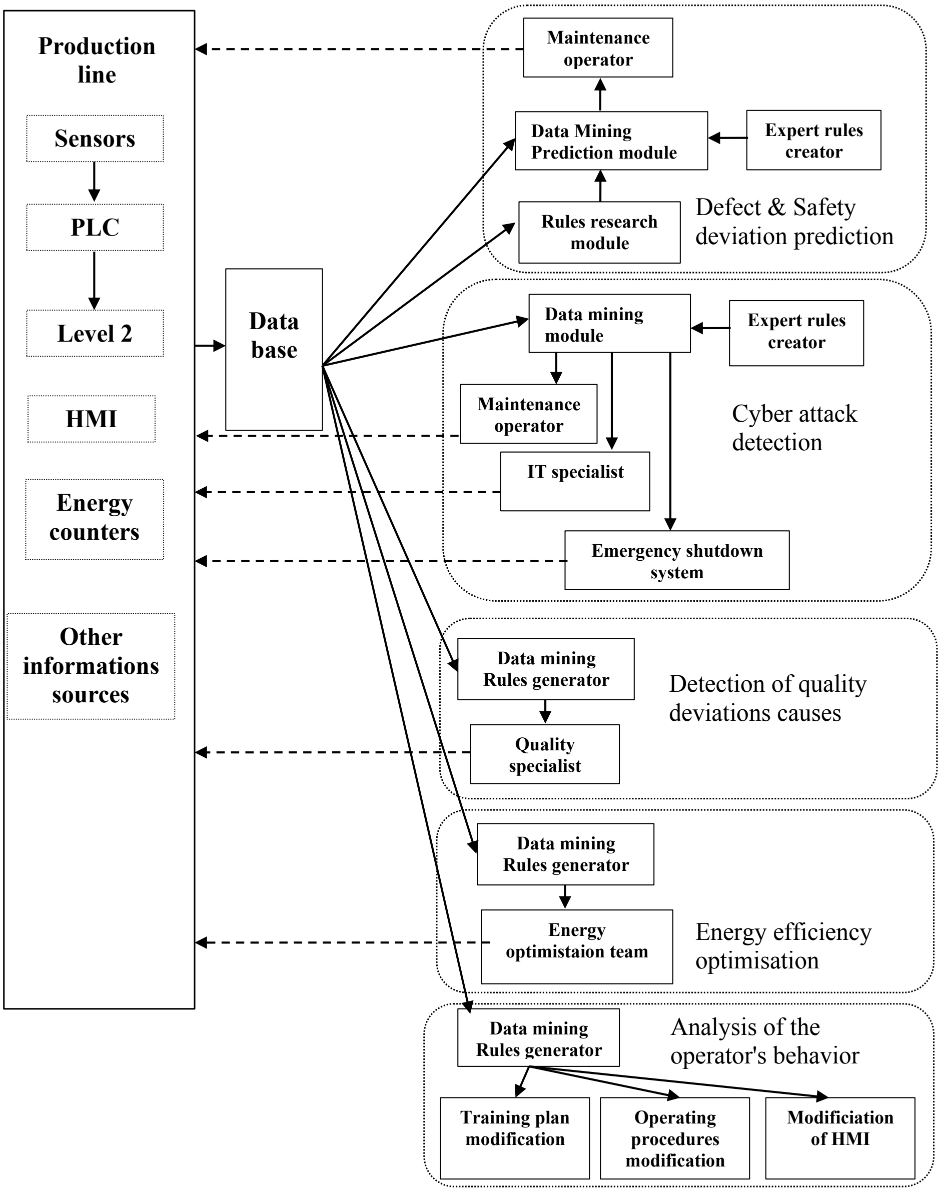

Production line
Sensors
PLC
Level 2
HMI
Energy counters
Other informations sources
Data base
Maintenance operator
Data Mining Prediction module
Expert rules creator
Rules research module
Defect & Safety deviation prediction
Data mining module
Expert rules creator
Maintenance operator
IT specialist
Cyber attack detection
Emergency shutdown system
Data mining Rules generator
Detection of quality deviations causes
Quality specialist
Data mining Rules generator
Energy optimistaion team
Energy efficiency optimisation
Data mining Rules generator
Analysis of the operator's behavior
Training plan modification
Operating procedures modification
Modificiation of HMI

Figure 3.32. Integrated concept of factory data mining and prediction (based on own study)

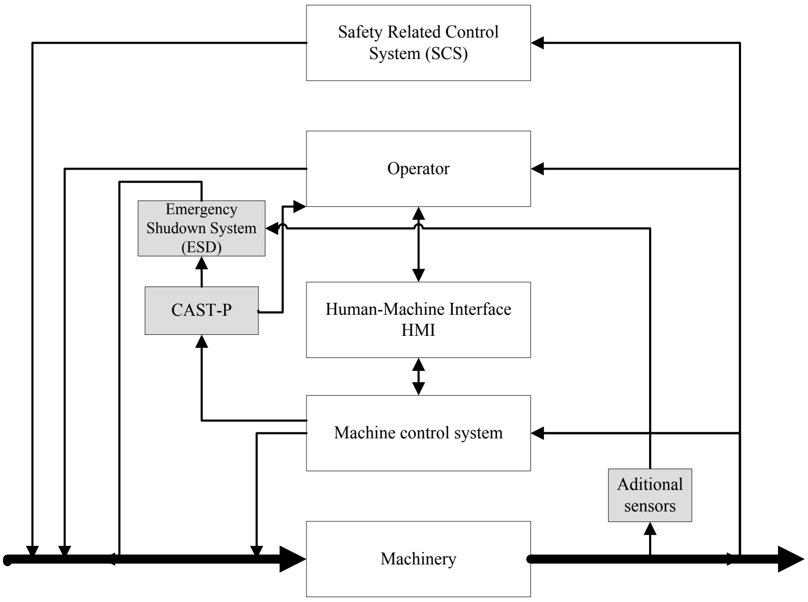

Safety Related Control System (SCS)
Operator
Emergency Shudown System (ESD)
CAST-P
Human-Machine Interface HMI
Machine control system
Aditional sensors
Machinery

Figure 3.33. Integrated concept of cyber-security prediction module (based on own study)

The principle of operation, in this case, does not differ from the methods shown in the previous examples. It assumes that expert rules will be defined through the analysis of the safety risk and vulnerabilities of the system. These rules implemented in the system while working in online mode allow detection of incorrect production line behaviour or not logical operations. After detecting such a defined rule that threatens security, the system through the digital output from the computer activates an independent Emergency Shutdown System which will safely stop the production line making it impossible to make losses.

The presented functionality was not possible to implement during the test launch of the system. Such functionality in case of incorrectly defined rules may cause additional stops and create additional threats.

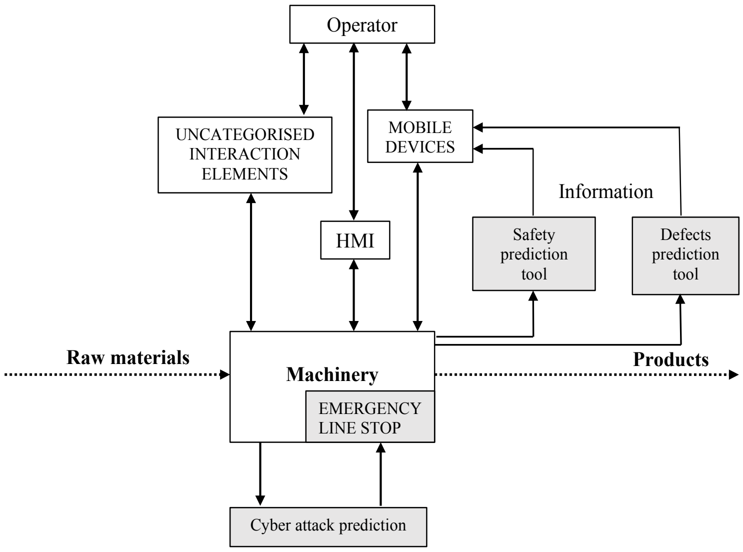


Figure 3.34. Tool proposed for operators in time reaction between 3 minutes up to 16 hours with the implementation of cyber-security module (based on own study)

In order to eliminate such a risk, the optimal solution would be if the Emergency Shutdown System was equipped with additional, independent of control system, sensors that would confirm the anticipated threat. An example of a defined threat can be: switching to the manual mode of the system and manual dosing of raw materials into the mixing chamber in proportions that could result in a fire, contrary to the prescription. This rule of CAST-P can be written as „IF *manual mode* AND *procedure of raw materials dosing finished* AND *conveyer X start demanded* THAN *Error – Safety system abnormal work of machine… AND procedure of machine emergency stop (24V issued on the output).''*The presented solution allows to minimize losses caused by cyber-attacks. The implementation process starts with a thorough BCM analysis and risk analysis and then selecting critical actions. The next stage is the selection and installation of additional sensors on machines operating outside of the control system that will eliminate mistaken activation of the system. The next stage is the implementation of the proposed solution. In summary, this solution aims to minimize significant material, environmental and employee safety losses due to cyber-attacks.

- Detection of quality deviations cause

A very similar mechanism as in the case of cyber-attacks detection can be used to detect quality deviations. Here too, with certain threshold values for the parameters in connection with the relevant product specification, it is possible to identify quality-related deviations very quickly.

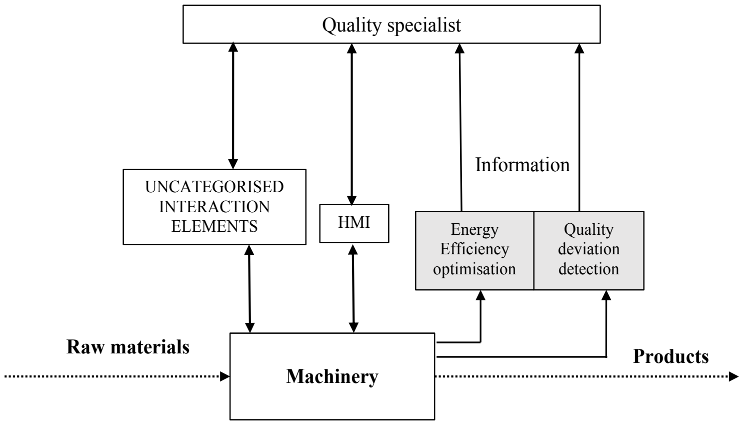

Quality specialist
Information
UNCATEGORISED INTERACTION ELEMENTS
HMI
Energy Efficiency optimisation
Quality deviation detection
Raw materials
Machinery
Products

Figure 3.35. Tool and actions proposed for quality specialists (based on own study)

In the case of quality deviation detection, we are dealing with searching for rules and parameters whose change causes a change in the quality of the output products. In most cases, these changes are known to quality specialists due to their experience, but in cases of implementation of new products, raw materials or modernization of machines, such knowledge may allow for large savings due to the acceleration of the process of detecting the causes of anomalies, which in turn reduces the amount of produced non-compliant products.

Fig. 3.35 shows the work model of a quality specialist who, receiving reports of found rules, can make corrections and changes in process parameters, machine settings or raw material changes.

- Energy efficiency optimisation

In this case, we have one starting point, which is the level of energy consumption. The issue of the analysis is to find the machine settings whose change translates into increased energy consumption. When predicting energy efficiency optimisation events, we are looking for machine parameters, processes, recipes, environments or raw materials that increase the energy consumption of machines. This prediction makes particular sense in highly energy-absorbing production processes. Both the machine parameters and the failure of one of the machine elements can be detected.

A distinction must be made between two different approaches here:

(a) tracking differences in the energy consumption patterns of the cycle vs. the reference cycle - where even minimal differences in energy consumption are captured and this is a very accurate but time-consuming tool

b) finding a rule that causes a sudden increase in energy consumption (e.g. manual operations of the operator, influence of environmental conditions, defects).

The proposed solution is obviously related to the second option and can be a tool supporting the first method and enriching it by proposing a reason for changes in media consumption.

- Analysis of operator behaviour

The last area identified by the author is the analysis of human behaviour. Having a database of data from machines (including safety systems) and human interfaces with machines and information systems, the rules found will also include rules showing how certain human behaviour affects the machine, stops, product behaviour in the machine, etc. The resulting data can be used to change training systems, logic in control systems, machine designs, HMI interface, etc. In addition, this system can be installed in training departments on installation simulators. Giving trainers information about frequent mistakes made by trained operators. It also allows the technicians to change the real object on the basis of experience from the simulators.

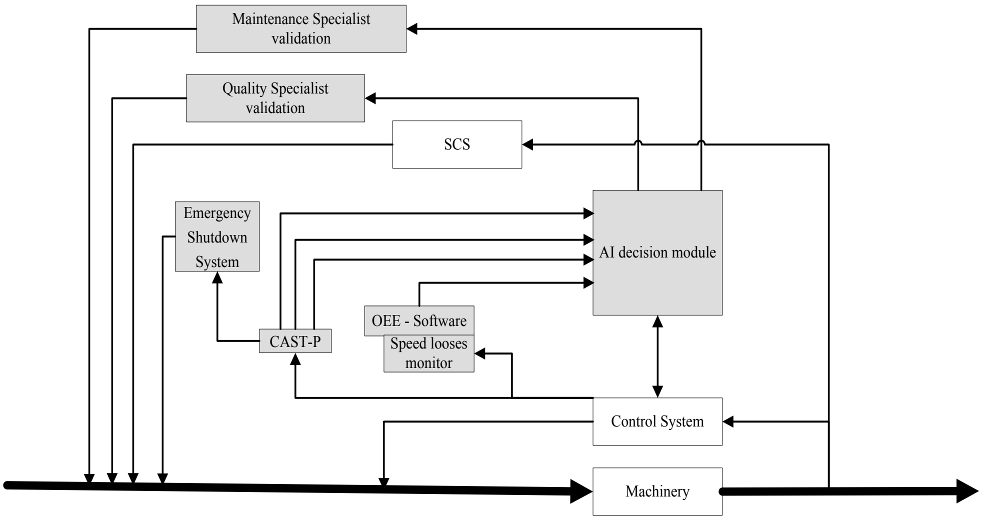

Maintenance Specialist validation
Quality Specialist validation
SCS
Emergency Shutdown System
AI decision module
OEE - Software
Speed looses monitor
CAST-P
Control System
Machinery

Figure 3.36. Integrated concept of factory data mining and prediction supported by advanced AI (based on own study)

3.2.9. Evolution of the tool

Due to the rapid progress of artificial intelligence methods based on deep neural networks, the natural continuation of the proposed solution is the use of tools that support the human decision with AI modules. The scheme of the potential system is presented in Fig. 3.36 and Fig. 3.37. Another tool that is increasingly used is cloud computing. It provides unlimited possibilities for data collection and processing. Thanks to the use of such a data lake solution, it can update the database with new rules created in identical plants scattered around the world. In addition, newly detected threats will be sent to the analyst.

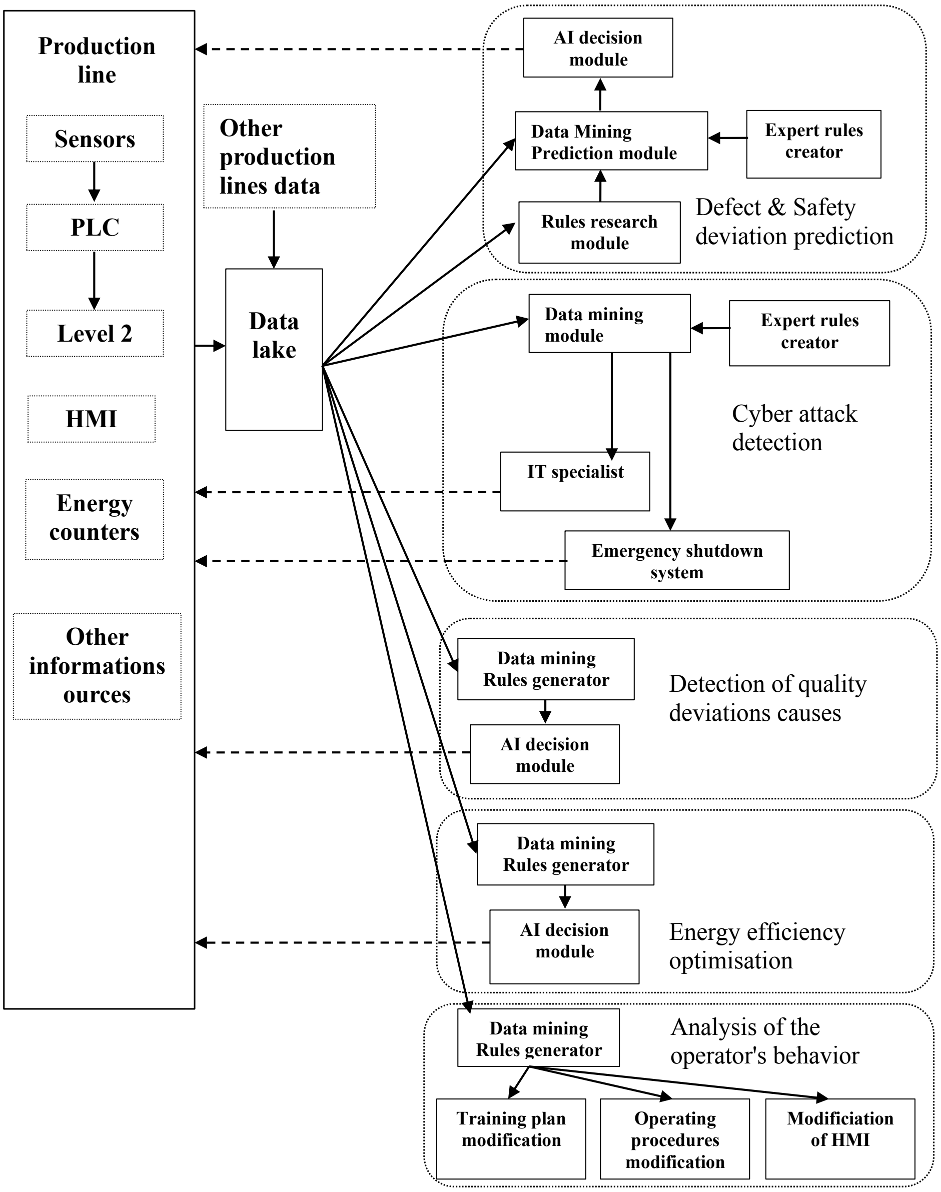

Production line
Sensors
PLC
Level 2
HMI
Energy counters
Other informations ources
Other production lines data
Data lake
AI decision module
Data Mining Prediction module
Expert rules creator
Rules research module
Defect & Safety deviation prediction
Data mining module
Expert rules creator
Cyber attack detection
IT specialist
Emergency shutdown system
Data mining Rules generator
AI decision module
Detection of quality deviations causes
Data mining Rules generator
AI decision module
Energy efficiency optimisation
Data mining Rules generator
Analysis of the operator's behavior
Training plan modification
Operating procedures modification
Modificiation of HMI

Figure 3.37. Integrated concept of factory data mining and prediction supported by advanced AI (auto citation [136])

Points that can be developed thanks to the knowledge gained from the analysis of information and the ever-increasing involvement of artificial intelligence methods are:

- reduction of the spare parts warehouse and purchase as a function of expected failures,
- better management of shift breakdown workers in the functions predicted on a given failure change,
- choice of priorities for AI - safety, security productivity, minimization of asset downtime, increasing the speed of decision making, for example: whether to stop the line now or wait until it breaks down due to timely obligations to clients and gain/ loss cost ratio,
- AI in the function of information about the future failure optimizes the line parameters to avoid a drop in the quality of the products.

3.3. Description of the proposed proof test interval method

3.3.1. Assumptions adopted

As it was presented in previous chapters, a test of machinery issue is not precisely defined taking into consideration two crucial factors: law and standards requirements. The author in this chapter presents a new integrated approach to this subject, based on well-known methodology presented in international standards [56], [62], [57]. Due to the new risk areas managed by companies, counting the stoppage connected to the functional test interval has also taken into consideration other factors, into the direct costs of stoppages, or the costs of potential failures. It can be stated that the brand good image loss, costs a company (e.g. an accident at work) much more than the cost of additional machine stops associated with the proof test or functional test. Direct costs and efficiency of planned maintenance can be evaluated through KPIs. The KPIs can be defined according to international standard ISO 22400 [69]. The proof test objective is to discover dangerous failures not found by the diagnostics.

Determination of the optimal frequency of testing poses difficulties in many companies. The mathematical approach [135] is not very common and demands a high level of technical knowledge and familiarity with the standards and safety aspects. Determining the level of safety after the modification of equipment and adapting it to the requirements put technical departments in the face of new requirements and problems [135]. It was assumed that the hardware component with the smallest value for the proof test interval determines the proof test time for the subsystem. Values of the failure probability requirements are required for the whole safety function, including different systems or subsystems. The probability of failure per hour of a safety function is determined by calculation of all subsystems, which as a whole create a safety function. The end-user of the safety-related system has to make an analysis of PFH based on the data received from the producer of each part of the safety-related system.

The suggestion consists of the proposal of test interval for machinery. The proposal helps also to increase the productivity of the machines by standardisation of test frequency.

The variety of applications in many sectors of industry requires periodic proof testing and functional tests. There is a gap in the law and standards in explaining the frequency of functional tests, proof tests and shutdowns used to detect failures. This mainly affects the functions of SIL 1 or PL=c and PL=b. As is apparent from the literature, the user defining a functional test must rely on the data provided by the machine manufacturer.

From the author's professional experience in working with machines, it follows that the safety components currently used by machine manufacturers have predominantly redundant architectures and frequently the actuators are electromechanical elements. Therefore, this particular perimeter is the scope of the author's analysis. Most of the safety devices encountered by the author with architecture without redundancy are devices from before the year 2000, which at present, according to manufacturers' requirements and standards, qualify them for replacement (lifetime equal to 20 years).

In order to verify the hypothesis numerically, it is necessary to analyse structures that have HFT=1. Common sub-system architectures encountered in the machinery industry are presented in Table 3.8

Table 3.8. Safety architectures versus Hardware Fault Tolerance

Architecture	HFT
1oo1	0
1oo2	1
2oo2	0

The table above shows that the following structure 1oo2, should be analysed. Structures 2oo3 and 3oo4 are not used in machinery therefore this structure will not be analysed. An example of 1oo2 architecture structure is presented in Fig. 3.38.

Frequently, a proof test interval is estimated by the manufacturer to be twenty years. The second source of information can be historical data about the frequency of demands for the safety-related action of the safety related part of the control system. Based on this data, the frequency may be changed. Unfortunately, for machinery, there are practically no datasets that could be used for calculations. For this reason, the author adopted the SINTEF OREDA [48] database values for calculations. This database is very reliable and its results are very restrictive (even by an order of magnitude in relation to EXIDA [21]), which is very important in the analysis of the worst possible scenarios. Unfortunately, this database does not contain information about parameter B_{10} whose values are taken from standard IEC 13849-1 and databases from the world's major manufacturers prepared for SISTEMA software.

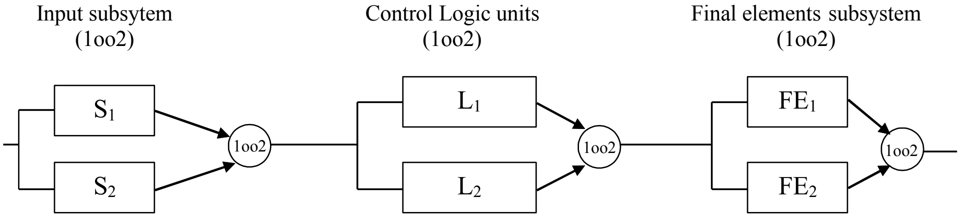


Fig. 3.38. Diagram for safety function in 1oo2 architecture

The objective of the analysis is, under the assumptions of SCS with non-electronic technology and HFT=1 for each subsystem, where SCS is working infrequent operation and taking the most restrictive validated reliability data for the calculation, to achieve a test frequency ensuring SIL=1(PL=c or PL=b) retained over time.

Taking all this into account, the author made the following assumptions used in the calculation and development of the method:

- the lifetime of the elements is 20 years (an assumption that appears in international standards and most manufacturers' specifications);
- the reliability data for the calculations were taken from the PDS Data Handbook database (due to the most restrictive reliability records);
- safety function with electromechanical output;
- safety function working in high demand;
- hardware fault tolerance equal one;
- redundant elements are the same design.

3.3.2. PFH calculation with regard to IEC 61508 standards models

The calculation of the required PFH level is done according to the methods described in IEC 61508-6 Appendix B standard. Detailed calculations can be found in Appendix 1.

$$PFH_{SYS} \cong PFH_S + PFH_L + PFH_{FE} \tag{3.24}$$

where

PFH_{SYS} - is the average frequency of dangerous failure of a safety function for E/E/PE safety-related system

PFH_S - is the average frequency of dangerous failure for the sensor subsystem;

PFH_L - is the average frequency of dangerous failure for the logic subsystem;

PFH_{FE} - is the average frequency of dangerous failure for the final element subsystem;

a) Architecture 1oo2

According to the assumptions presented above, subsystems with redundancy are considered. The first architecture 1oo2 consists of two channels connected in parallel, such that either channel can process the safety function. The equation of average frequency of dangerous failure for the group of voted channels is presented below:

$$PFH \cong 2 \cdot ((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU}) \cdot (1-\beta) \cdot \lambda_{DU} \cdot t_{CE} + \beta \cdot \lambda_{DU} \tag{3.25}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \tag{3.26}$$

where

β - the fraction of undetected failures that have a common cause

β_D - of those failures that are detected by the diagnostic tests, the fraction that have a common cause

λ_{DD} - detected dangerous failure rate (per hour)

λ_{DU} - undetected dangerous failure rate (per hour)

λ_D - dangerous failure rate (per hour)

T_1 - proof test interval (hour)

MRT - mean repair time (hour)

MTTR - mean time to restoration (hour)

b) Calculation results

The lowest reliability data values from the OREDA database were used for the calculations performed and presented below in table 3.9.

Table 3.9. Results of PFH_{SYS} calculations of safety functions

Architecture	PFH_S [h^{-1}]	PFH_L [h^{-1}]	PFH_{FE} [h^{-1}]	PFH_{SYS} [h^{-1}]
1oo2	$2.5 \cdot 10^{-7}$	$3.38 \cdot 10^{-9}$	$4.37 \cdot 10^{-78}$	$6.90 \cdot 10^{-7}$

Additional calculations were made by the author based on standard IEC 61508-6 and using the data tables from Table B.13 where the average frequency of a dangerous failure was assumed for a proof test interval of one year and a mean time to restoration of 8h. Value of λ_D=0,5E-05 and β=20% was used for both architectures and all three subsystems.

Table 3.10. Results of PFH_{SYS} calculations of safety functions based on B.13 table from standard IEC 61508-6

Architecture	PFH_S [h^{-1}]	PFH_L [h^{-1}]	PFH_{FE} [h^{-1}]	PFH_{SYS} [h^{-1}]
1oo2	$1,1\cdot10^{-6}$	$1,1\cdot10^{-6}$	$1,1\cdot10^{-6}$	$3,3\cdot10^{-6}$

The results obtained are summarised in the table 3.11.

Table 3.11. Results of PFH calculations for analysed safety architectures

Reliability data source	Architecture	PFH [h^{-1}]	SIL	HFT
OREDA	1oo2	$6,9\cdot10^{-7}$	2	1
IEC 61508-6	1oo2	$3,3\cdot10^{-6}$	1	1

Analysis of the PFH calculation using SINTEF OREDA and IEC 61508-6 data standard indicates that systems with at least one level of redundancy can in any case satisfy SIL 1 requirements (Table 3.11) achieving SIL 1.

3.3.3. PFH calculations with regard to IEC 62061 standard models

For the full range of calculations, further calculations are based on the machine safety standard IEC 62061.

Assumptions made by the author:

- the lifetime of the elements is 20 years (an assumption that appears in international standards and most manufacturers' specifications);
- the reliability data for the calculations were taken from the PDS Data Handbook database (due to restrictive reliability record);
- safety function with electromechanical output;
- safety function working in high demand;
- hardware fault tolerance equal one;
- redundant elements are the same design (most common at machinery);
- diagnostic coverage on level 60% for all elements;
- diagnostic test interval – 1h.

a) The basic structure of subsystem type B: tolerance to individual failure, without diagnostic function

$$\lambda_{DssB} = (1-\beta)^2 \cdot \lambda_{De1} \cdot \lambda_{De2} \cdot T_1 + \beta \cdot \frac{(\lambda_{De1} + \lambda_{De2})}{2} \tag{3.27}$$

$$PFH_{DssB} = \lambda_{DssB} \ (h^{-1}) \tag{3.28}$$

where:

T_1 - is the proof test interval or lifetime whichever is the smaller,

β - is the susceptibility to common cause failures

b) The basic structure of subsystem type D: tolerance to individual failure, with diagnostic function

The equation PFH for this configuration:

$$\lambda_{DssB} = (1-\beta)^2 \cdot \left\{ \left[\lambda_{De}^2 \cdot 2 \cdot DC \right] \cdot \frac{T_2}{2} + \left[\lambda_{De}^2 \cdot (1-DC) \right] \cdot T_1 \right\} + \beta \cdot \lambda_{De} \tag{3.29}$$

$$PFH_{DssD} = \lambda_{DssD} \ [h^{-1}] \tag{3.30}$$

where:

T_2 - is the diagnostic test interval,

T_1 - is the proof test interval or lifetime whichever is the smaller,

β - is the susceptibility to common cause failures; $\lambda_D = \lambda_{DD} + \lambda_{DU}$; where λ_{DD} is the rate of detectable dangerous failures and λ_{DU} is the rate of undetectable dangerous failure.

$$\lambda_{DD} = \lambda_D \cdot DC \tag{3.31}$$

$$\lambda_{DU} = \lambda_D \cdot (1-DC) \tag{3.32}$$

λ_{De} - is the dangerous failure rate of subsystem element 1 or 2;

DC - is the diagnostic coverage of subsystem element 1 or 2;

Based on the above assumptions, calculations were performed, the results of which are presented in Table 3.12. The obtained results of the demanded probability of failure per hour, allow to achieve safety integrity level equal 2, which exceeds the expected SIL 1 result.

Table 3.12. Results of PFH calculations for analysed safety architectures

Architecture	PFH [h^{-1}]	SIL_{CL}	HFT
DssB	$1.25 \cdot 10^{-6}$	1	1
DssD	$8.04 \cdot 10^{-7}$	2	1

Having calculated subsystem PFH_d by means of the formulas from the IEC 62061, it is important to ensure that the associated SIL_{CL} obtained from Table 3.10 of IEC 62061 is compatible with the constraints imposed by the architecture as the maximum SIL_{CL} attainable by a given subsystem and is restricted by the hardware fault tolerance of the architecture and by S_{FF} as listed in the following Table 3.13.

Table 3.13. Table of constraints on the architecture of subsystems based on IEC 62061 [57]

Safe failure fraction (S_{FF})	**Hardware fault tolerance**		
	0	**1**	2
$S_{FF} < 60\%$	Not allowed	SIL 1	SIL 2
$60\% \leq S_{FF} < 90\%$	SIL 1	SIL 2	SIL 3
$90\% \leq S_{FF} < 99\%$	SIL 2	SIL 3	SIL 3
$S_{FF} \geq 99\%$	SIL 3	SIL 3	SIL 3

Taking into account that two subsystems have S_{FF}<60% maximum SIL value for SRCF will be SIL 1, what is presented in Table 3.14.

Table 3.14. Results of PFH calculations for analysed safety architectures

Architecture	PFH [h^{-1}]	SIL_{CL}	HFT
DssB	$1.25 \cdot 10^{-6}$	1	1
DssD	$8.04 \cdot 10^{-7}$	1	1

3.3.4. Summary

In conclusion, the empirical calculations, by taking the tested and most restrictive data (OREDA, IEC 13849-1 standard and producers data), based on two standards IEC 61508-6 and IEC 62061, confirm the hypothesis that for HFT=1 and SIL=1 the proof test can be performed with an annual frequency (Table 3.14)

Table 3.14. Recommendation for test periods for the machinery

Preconized test interval	Source	SIL	HFT
1/year	Author	1	1
	IEC 62061	2	1
1/month	IEC 62061	3	1

Summarising the above results concerning SIL1 and taking into account the recommendation introduced in the latest version of the standard IEC 62061 (for SIL2 and SIL3), the author obtain a complete method for SCS with non-electronic technology, HFT=1 (architecture with hardware fault tolerance equal 1) in the range of SIL 1 - 3.

One remark from the author's professional experience, the human factors aspect should also be taken into account by the user of this method. When updating the testing frequency (especially by extending it), it must be taken into account that this reduces the frequency of physical work opportunities for the operator with the safety function elements. This may cause lack of development of certain habits, especially in case of high turnover of employees, an example the author knows from practice. Therefore, the potential financial gains from the lack of planned stops must not distract from the risks of missing training aspects. The solution here may be were possible to have a functioning model of the equipment used for training also for the safety functions elements (e.g.: pull safety lines, safety stop pushbuttons).

3.5. Chapter summary

Downtime for maintenance is scheduled as a part of the manufacturing day and, in some cases, as an integral component of the manufacturing process. The goal is to hold emergency and unscheduled maintenance to a minimum or on economically acceptable level [94]. In essence, there are two objectives, (1) determine the maintenance requirements of the physical assets within their current operating context, and then (2) ensure that these demands are met as effective and safe as possible. Unfortunately, the implementation of only one maintenance system does not cover all the problems related to the reliability, maintainability and safety aspects of modern machines and production lines. The lack of such integrated systems convinced the author to begin research in the area of integrated productivity and safety management. In the maintenance strategy and procedures developed, the hardware reliability aspects and functional safety solutions have been taken into consideration. The computer-aided maintenance decision support system is being developed that extends functionally methods and tools used currently in industrial practice. The biggest risk of the tools currently being proposed on the market that includes implemented data mining algorithms and sold as a "black box" is that they can manipulate the data and produce completely misleading results [100].

The solution presented by the author is based on the application of CAST-P. The comprehensive solution presented in Fig. 3.32 for Industry 4.0 covers many issues. Data from the production line are processed by successive tools of the control system. Depending on the rules applicable in a given company, these data can be saved in an external database by collecting from relevant levels of control. Data stored in this database form the basis for further analysis. These data can then be used to predict failures on production lines, and even to detect functional safety related cyber-attacks. Both tools are based on one solution. Other possible applications not analysed in this dissertation are the detection of quality anomalies, optimization of the energetic efficiency and analysis of the operator's behaviour. Benefits resulting from the proposed method are following:

- reduction of the breakdown duration,
- failure detection in advance (prediction),
- more accurate adjustment of production plans, considering the level of failures,
- flattening of quality structures and maintenance,
- in some specific cases, it can replace redundancy

In addition to the first method is a proposed solution of optimizing functional test frequencies. This solution helps to maintain the required safety integrity level (SIL) in case of identified risks and at the same time ensures adequate availability of the machinery. The second important aspect is to combine the frequency of the different tests in order to minimise machine downtime and consequently minimise production loss. The tool includes the impact of the environment in the operational stage of the life cycle. The methods presented above enable a new approach in the domain taking into account the experience of the author. At the same time, it is recommended that an analysis of the causes of newly identified threats would be carried out, in order to eliminate the root cause of the increased risk. An in-depth analysis and subsequent action plan can eliminate potential cause, which can result in a return to a regular interval considered.

The second method for the proposed proof test interval solution allows to verify provide the required SIL, taking into account relevant aspects of risk management in the company, and completes the methods proposed at IEC 62061 [57]. This method takes into account EU recommendations and provisions of the relevant standards. Additional verification or a shorter frequency of proof tests allows to minimize the situation of the safety integrity level decreasing over time.

Chapter 4

RESULTS OBTAINED – CASE STUDIES

This chapter will provide examples of the application of the methods and tool presented in chapter three. The presented examples concern two general issues. The first example concerns the predictive detection of failures in machinery and equipment. The second example shows the development of the same as a previous example tool, concerning the detection of functional safety anomalies and prevention of safety risks. Third example is a presentation of a functional test interval optimisation tool. These examples are directed towards the Industry 4.0 generation.

4.1. Case study concerning predictive maintenance

4.1.1. Object description

Analysed objects have been similar to the system described in Appendix 5 and presented in Fig. E.1. During the analysis of the case study, most of the management methods were based on global group rules. The TPM and the main RCM methodology have already been successfully implemented at the analysed plant. This gives a strong foundation for the implementation of further tools and methods.

4.1.2. Control system architecture

The control system for the analysed production line was made according to the standards taking into account the latest standards for safety and reliability of machines presented in Chapter 2. Level one of the control system gathers all information received from hardware. Some of those information's are used and presented to the operator by HMI, other are used to diagnose the quality of the product, and some to manage the process correctly. Due to a large amount of the generated data, they are not archived. From the availability point of view, much of the important information are lost. As it was verified, on average, new information appears on HMI every 7 seconds.

4.1.3. Safety-related aspects

To ensure that the production line complies with the requirements of Directive 2009/104 / EC, the hazards and assess risks and risk reductions were identified. Risk assessment and risk reduction analyses made internally help to detect and manage risks on the installations in service. After installation, FMEA analysis to detect any additional hazards connected to the plant environment and specifications were made. Controls systems in those installations in view of the large physical area were built as distributed systems. A difference in comparison to process lines is that rubber mixing lines are “batch production lines” which provokes a different approach in many layers of control and quality assumptions. The process is analysed online with the calculation of any differences in the previous batch and parameters set as a reference value.

At the analysed factory, according to European and national regulations, machines are equipped with safety functions and complementary measures. There are several dozens of safety functions on each of the analysed lines. Most common safety function are: guard monitoring, emergency stop control, two hand control, intrusion detection by light curtain control or safety laser. Safety lines, safety stop pushbuttons, two hand safety buttons, safety light barriers, laser scanners are standard safety elements of examines production lines. Machines are prepared for the use of Logout - Tagout [1] systems to improve safety during maintenance interventions.

Table 4.1. Statistics of heavy accidents at rubber mixers in the USA (1992-2010) and GB (2000-2001) [129] [49]

Country	Year	Type of root cause	Activity	Action	Consequence
United States	1992	Ignore of safety rules	Cleaning of the mixer	Loosening and fall of mechanical components	Death
United States	2000	Ignore of safety rules	Cleaning of the mixer	Start of machine by co-worker	Death
United States	2004	Ignore of safety rules	Cleaning of the mixer	Rapture	Crush injury to the right
United States	2010	Inadequate ventilation system, no explosive flaps, systems	Normal work	Explosion	Death
Great Britain	2001	Lack of some safety elements	Breakdown repair	Start of machine by co-worker	Death

Despite many efforts in the improvement of safety aspects, based on the example of data from the United States and the United Kingdom (Table 4.1), it can be stated that rubber production plants are areas that continue within high laden risk [185]. Therefore, the number of collaterals is much higher than in other similar plants installed at a similar size. As an example, can be presented a safety function of safe access assurance to the area where are moving rolls with potential danger for the operator.

The technical state and functioning of safety lines and safety locks for machine access doors are checked periodically by maintenance personnel (the production staff independently makes periodic verification), results are written down to a computerised system. In the case of any malfunction, devices are exchanged and proper personnel informed. Programs of PLC which control safety functions (e.g. safety access) are checked every six months from the point of view of changes not registered in the book of changes. Any change made in the program made during shifts must be noticed after that validated by the proper personnel. That prevents the evaluation of the program with acceptable risk level.

Unfortunately, apart advanced techniques and organizational approaches used, there are still situations that have a negative impact on both reliability and sometimes safety. Some examples that the author has noted in recent years are briefly discussed below:

- PLC Processors with defective chip

The symptom of anomaly was some memory loss and errors in correct functioning of equipment, this situation appears on more than ten percent of one series of PLC processors. User informed the PLC manufacturer about the situation and processors were exchanged. After this exchange campaign error never appear again.

- PLC processor - memory overflow

In one of the applications were used medium range controller (PLC) which was responsible for machine control system of small support process for main production line. What is important controller that provides safety control up to SIL 3 according to IEC EN 61508, and applications up to PLe/Cat.4 according to ISO 13849-1. Generally, once per quarter got into fault mode and was losing its logic program. After analysis it appears that buffer of memory after few months of work became full (the program utilised almost all of the controller's memory) and because of internal error it deleted the logic. Solution made was exchange of processor for different with bigger memory and add modification in the logic to clear automatically buffer after 2 months, what was impossible to made on the previous one because of lack of free memory for logic modification.

- Relay Output card breakdowns

In one application for control of hydraulic valves were used relay output cards. After increase of production were observed frequently repeating problems with work of hydraulic unit after more detailed analysis were found problem with work of relay outputs on card. It appears that some outputs are damaged and signal comes from controller but it was no output to hydraulic valves. Problem were solved after calculating number of cycles (switch) during one day. Multiplied by 3 months it gives over one million cycles what after receiving answer for this question to producer was maximum number of cycles during lifecycle of this card.

4.1.4. Availability and productivity issues

By definition, production companies must show a profit. It is possible to achieve this by using a minimum of one of several levers. One of them is the increase of productivity, for example to produce a larger number of compliant products in a shorter time than before. To be able to reliably measure progress and results to date tools of indexes / indicators are used.

The analysed production line has the main indicators defined, which are used to monitor the results. One of the monitored indicators is the OEE indicator. Its components provide information on the main losses on the presented line.

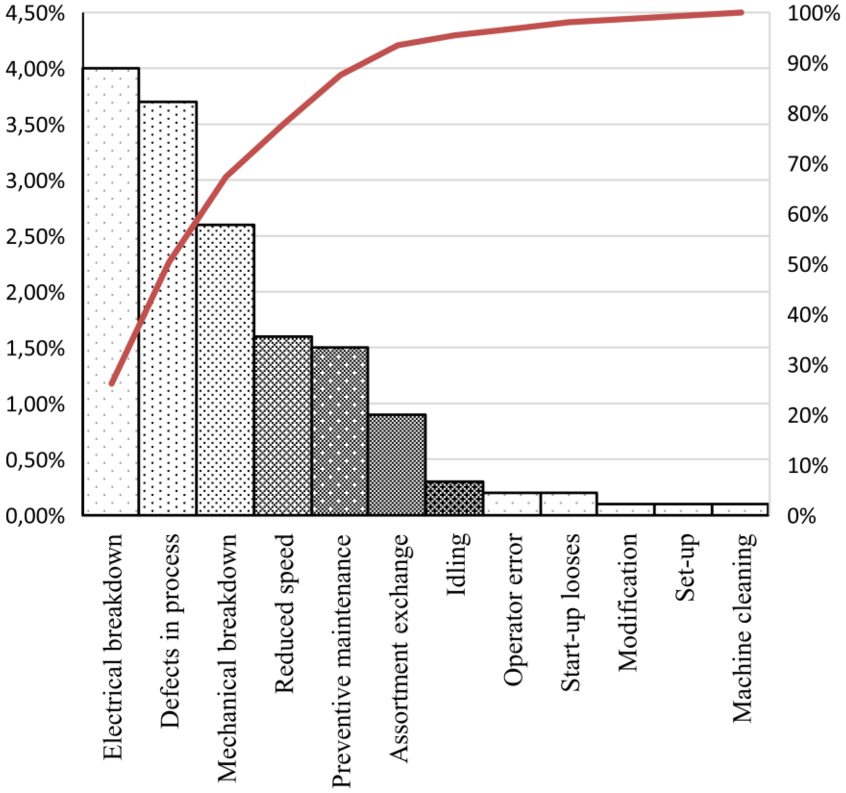


Figure 4.1. Yearly percentage of losses for line A – graph made according to the Pareto rule

As shown in Fig. 4.1 and Fig. 4.2, the three main losses are breakdowns, amounting to 43% of total losses, then failures in the process depending on the type and behaviour of raw materials in their processing, their share in total losses is 24%. The last element is reduced speed which comprises 10% of total losses (divided into two sub-categories).

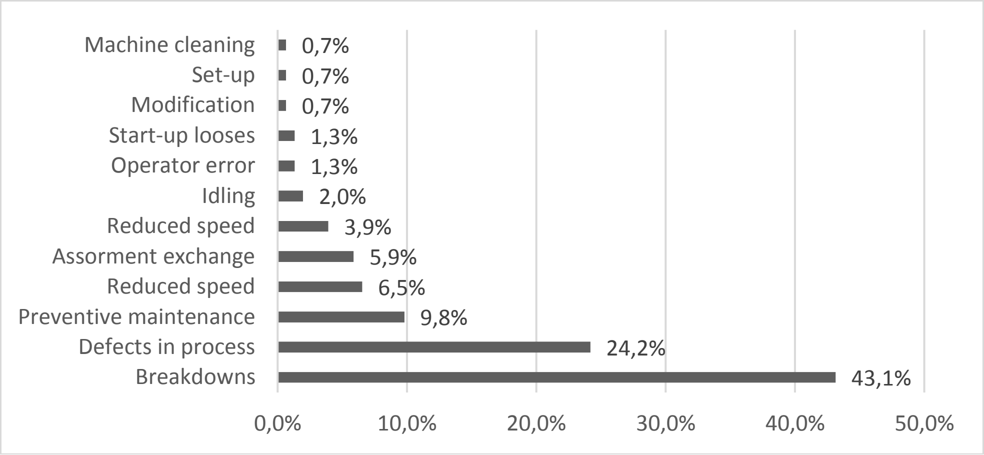


Figure 4.2. Yearly percentage of losses share for line A

Another three reasons are stops planned for preventive maintenance (10%), equipment changeovers (6%) and idling (2%). In total, these six stop categories absorb over 90% of lost time. Fig. 4.2 shows sample results of the year with the percentage share of each of the codes listed. Based on these values, it can be stated that the implementation of the proposed tool is indicated on the given line due to the relatively large number of unscheduled stops.

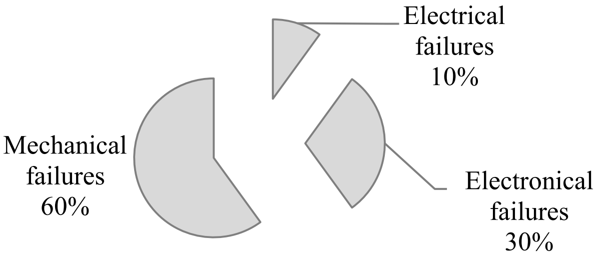


Figure 4.3. Breakdown graph with a diversion into different sources of breakdowns

Analysing the results of stops for breakdowns (Fig. 4.3), it can be seen that mechanical stoppages take the largest share (60%), followed by stops due to electronics (30%) and last electrical failures (10%).

This is a very good distribution for the application of the predictive tool because mechanical failures largely before their occurrence and the stoppage of the machine indicates symptoms and they often appear much faster than the fault.

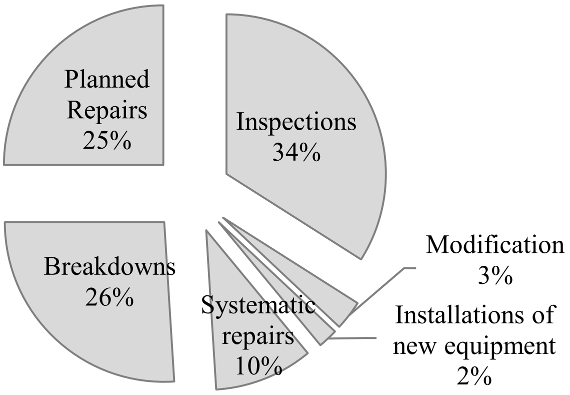


Figure 4.4. Percentage share of maintenance workload time by activity

The next graph (Fig. 4.4) was made on the basis of data from CMMS. It presents the percentage distribution of maintenance workers' work over a year. It shows a good proportion in relation to unplanned failures to other activities. This ratio does not exceed 30%. Planned preventive activities take up 44% of employees time. Planned repairs (25%) are activities that have been planned for execution between stops for prevention. These are works not included in systematic preventive activities. Installations of new equipment and equipment as well as the time devoted to modifications do not exceed 5% of the total working time of maintenance.

Table 4.2. Monthly percentage of availability losses divided into categories and two similar lines

Category of losses	Line A	Line B
Defects in process	4.68%	5.12%
Breakdowns	5.05%	4.58%
Set up's	1.11%	0.52%
Reduced speed	1.36%	1.02%
Minor stoppages	0.38%	0.36%
Line cleaning	0.00%	0.69%
Start-up	0.11%	0.28%
Operator errors	0.10%	0.00%
Other	0.03%	0.00%

Table 4.2. presents the monthly results for two very closely related but not identical lines. Most importantly, they produce different types of products, which significantly affects their

cumulative results. Line B has much more heterogeneous results over time strongly associated with the type of assortments.

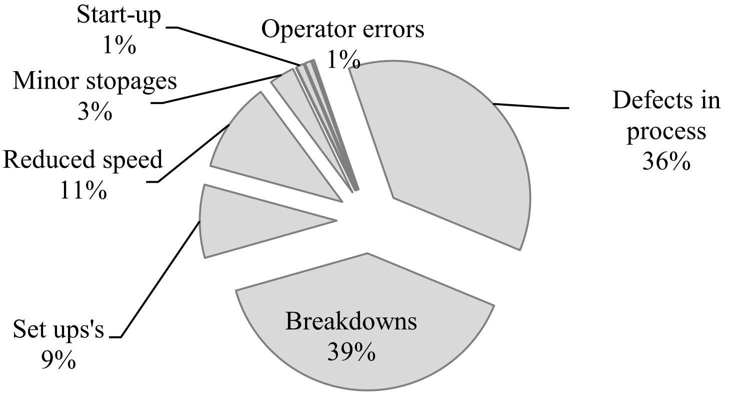


Figure 4.5. Monthly percentage of losses share for line A

This entails not only the coefficients of typical production rates but also maintenance. Further data analysis is carried out mainly on the A line due to the lack of such a significant impact of the product on the results of the entire line as well as individual components. As the data from Fig. 4.5 shows, the values of individual codes in a given month can be significantly different from the average annual value shown previously. These differences concern, in particular, hard-to-plan codes, e.g. breakdowns and failures in the process.

4.1.5. Data gathering

Data on a different level of control systems are gathered in a different manner. Maintenance data were collected in CMMS by manual data entry of maintenance personnel after any intervention made on this line. Production OEE indicators were collected semi-automatically.

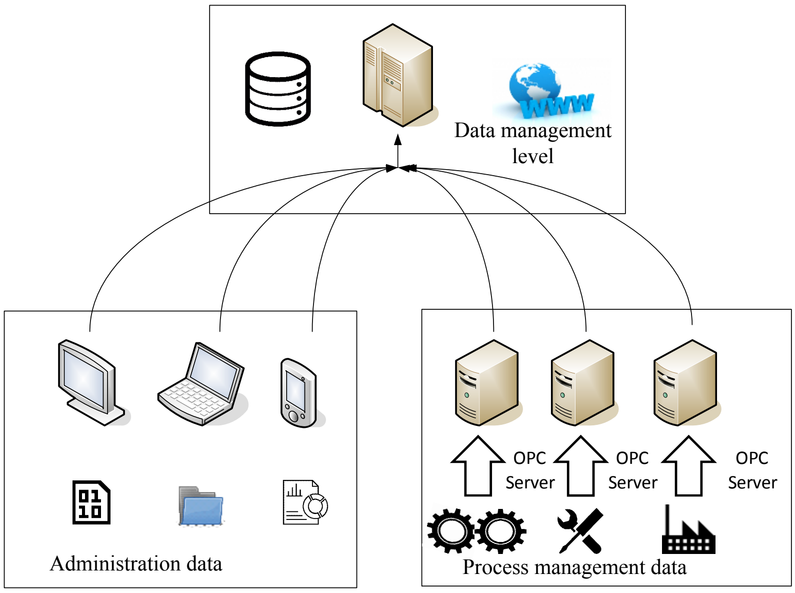


Figure 4.6. Diagram presenting hierarchy of data acquisition system [50]

Some electronic data collection was provided for quality and production realisation. Plant supervisory and production control level data were collected automatically presented in Fig. 4.6.

4.1.6. Reporting system

Analysis was made with daily and monthly frequency. The system of notification on this line can be divided into two sources of data distribution. First, is the CMMS provided by the maintenance department, fulfilled by maintenance staff. The second source of data is production reports fulfilled by the ganger on every shift. Information provided by maintenance personnel considers work orders (the possible cause of intervention, things made during the intervention, used spare parts, time last on intervention, time of intervention start, spent time, and a number of people engaged in this work). Information from production department OEE indicator incorporates beginning & end time of intervention, part of the line where intervention has taken place, and type of intervention. Information about the actual state of the production line and its components are supplied by the supervision system - level two of control system. It helps the leading line operator to react to deviation from the norm. It helps also to maintenance stuff with a diagnosis of machine state and in failure root cause detection.

4.1.7. Human factors

Generally, in examined systems, different families of human factors appear, which are influencing in a different stage of line life cycle and different level of companies' hierarchy. In this work, the author focuses only on the operation stage of machinery life cycle. The human factors in the analysed case study have been divided into two categories by profession:

a) Operators
   - Inappropriate operation of machine because of mistake;
   - Ignore the breakdown symptoms because of lack of technical training;
   - Mistakes connected with wrong training or procedures;
   - Incorrect use of machines

b) Maintenance
   - Inappropriate maintenance actions, procedures, wrong organisation;
   - Improper approach to maintenance due to bad habits;
   - Ignore of symptoms, corrective work instead of proactive;
   - Repairs made temporary - ad hoc to start line without searching real root cause.

The influence of the above-mentioned human factors was not significant due to the high organizational culture, but it is not negligible and had an impact both on the results of the test implementation and the choice of the proposed solutions. However, it is not discussed further in this dissertation.

4.1.8. Preparation phase

The basis which has to be implemented into the organisation before the proposed system implementation is a solid organisation with implemented TPM and the basis of the RCM or organisational concepts very similar to them. This guarantees that production operators, as well as maintenance breakdown workers, are at high organisational culture. That means huge sensitivity to safety, quality and reliability, issues are managed on a daily basis, both teams have common goals. The second important thing is the assurance of human resources for the author project. Adding it to another project will result in a fiasco.

The third thing is specifying correct line equipped with the modern control system and metering with sensors of a different kind.

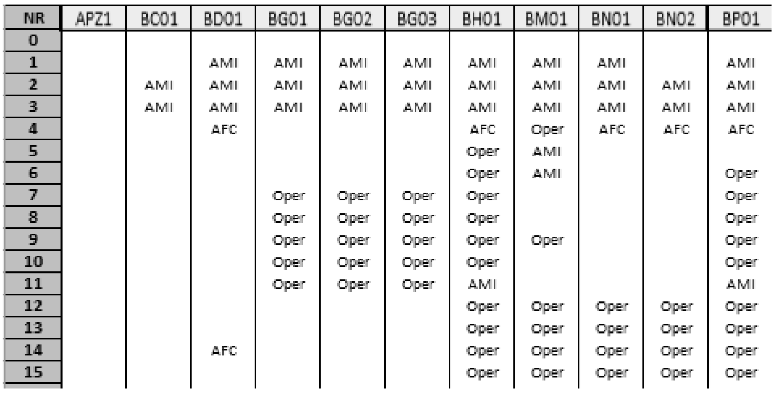
All three mentioned above pillars were implemented with success before the start of the case study.

4.1.9. Implementation

Before implementation of the system, after risk analysis (FMEA) some additional sensors and PLC programs were added and modified to online tracking relevant system parameters which were not installed originally (e.g. vibroacoustic sensors of reducers, hydraulic unit parameters of pressure and flow). This action results in high coverage of machines in sensors of different types connected to one system. After all, most of the machines get complete sensors coverage and those information's get into PLC, some small parts of PLC programs were added to analyse the signals.

The next step in implementing the assumptions of the new approach was the analysis of available IT tools. Due to the extensive statistical modules, Big Data processing capabilities, professional database support and customization software, the author has chosen the Statistica WebEnterprise package. Another argument for choosing this tool was the assumption that the people who will use the tool will be without knowledge of Statistica software and advanced statistical knowledge. That was possible thanks to the use of Statsoft's Enterprise module.

The next stage of preparation was dividing all gathered information into categories. There were specified two main categories. The first one was SYMPTOMS – which means that they do not stop the machine, but their appearance inform that something wrong is going on with some parts of the machine. The second type is EFFECTS - can be translated as messages after the presence of which the machine is stopping. In this type, two subtypes were recognised – errors which provoke intermediate stop of the machine, and second in which machine stops after the end of the cycle occur.



NR	APZ1	BC01	BD01	BG01	BG02	BG03	BH01	BM01	BN01	BN02	BP01
0											
1			AMI	AMI	AMI	AMI	AMI	AMI	AMI		AMI
2		AMI	AMI	AMI	AMI	AMI	AMI	AMI	AMI	AMI	AMI
3		AMI	AMI	AMI	AMI	AMI	AMI	AMI	AMI	AMI	AMI
4			AFC				AFC	Oper	AFC	AFC	AFC
5							Oper	AMI			
6							Oper	AMI			Oper
7				Oper	Oper	Oper	Oper				Oper
8				Oper	Oper	Oper	Oper				Oper
9				Oper	Oper	Oper	Oper	Oper			Oper
10				Oper	Oper	Oper	Oper				Oper
11				Oper	Oper	Oper	AMI				AMI
12							Oper	Oper	Oper	Oper	Oper
13							Oper	Oper	Oper	Oper	Oper
14			AFC				Oper	Oper	Oper	Oper	Oper
15							Oper	Oper	Oper	Oper	Oper

Figure 4.7. Graph of errors classification matrix

To make a complete classification it was necessary to add appropriate classification for over 14000 tags in the software program – the logic part of them is shown in Fig. 4.7. Each of them has to be verified manually with PLC logic programs. During this verification it was checked how each tag is defined in the PLC logic, in what type of above-presented groups it is connected, e.g. type OPER mean that it is operation important for the operator and it is shown in the events on HMI, so it is a symptom. The amount of work done was estimated at about one month of work.

After the classification was finished, all those information's were collected and implemented into the database of the plant supervisory level connected with events history. The following stage of implementation was the collection of the historical event database. For system learning, the important part is gathering as huge as possible database with historical data.

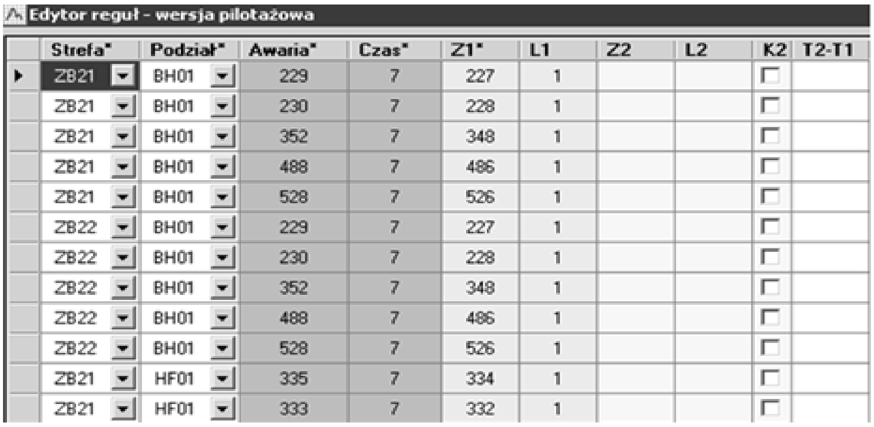
No. of event	Element of line	Sub-element of line	Type of error	Data y-m-d h:m:s	Time duration h:m:s	Description
340	Banbury mixer	Electric motor	OPER	2018-01-01 00:01:01	00:00:30	Alarm temperature of the motor bearings

Figure 4.8. Example of historical data record

To create an archival database, the frequency of data export was set to once per day. During work on the system, this frequency was changed to six hours. To properly conduct the analysis, the input data must be unambiguous, properly processed. The first difficulty encountered was the transmission of data from the surveillance system to the Statistica software database. Enterprise IT security requirements do not allow for the integration of external systems with enterprise databases. The solution turned out to be a periodic export of a data file that could feed the database used by Statistica. In order not to influence on existing reporting systems, all events were exported as *.csv files into one subdirectory in server hard disk, an example of one record is presented in Fig. 4.8. Software package Statistica Enterprise with SQL Server was installed on the mentioned above server. The general architecture of the implemented tool is presented in Fig. 4.10.

For the project, historical data from more than four months (121 days) were collected and analysed. After analysis, it was found that on average is generated 11830 messages from systems per day. Based on such a large amount of data, it was possible to identify rule relationships.

To simplify interface Human vs statistical analysis, a software tool named RULE CREATOR was created.



Edytor reguł - wersja pilotażowa

	Strefa*	Podział*	Awaria*	Czas*	Z1*	L1	Z2	L2	K2	T2-T1
▸	ZB21	BH01	229	7	227	1			□	
	ZB21	BH01	230	7	228	1			□	
	ZB21	BH01	352	7	348	1			□	
	ZB21	BH01	488	7	486	1			□	
	ZB21	BH01	528	7	526	1			□	
	ZB22	BH01	229	7	227	1			□	
	ZB22	BH01	230	7	228	1			□	
	ZB22	BH01	352	7	348	1			□	
	ZB22	BH01	488	7	486	1			□	
	ZB22	BH01	528	7	526	1			□	
	ZB21	HF01	335	7	334	1			□	
	ZB21	HF01	333	7	332	1			□	

Figure 4.9. Rule creator window

At the test version, only simple dependencies were used. That means, that the detection of a single event assigned as a symptom results in generating information about a potential failure. No rules were searched with a sequence of several preceding events. This option is provided in the created rules editor (Fig. 4.9), which gives a wide range of rules. It was developed, taking into account the possibility of occurring up to five events preceding the failure. Two options for mutual symptom relationships are also included. First, when the order of occurrence of symptoms is irrelevant and only counts the occurrence of a specific set of symptoms in a given time interval, resulting in damage and a second option in which the order of occurrence of the symptoms affects the occurrence or not, damage [134].

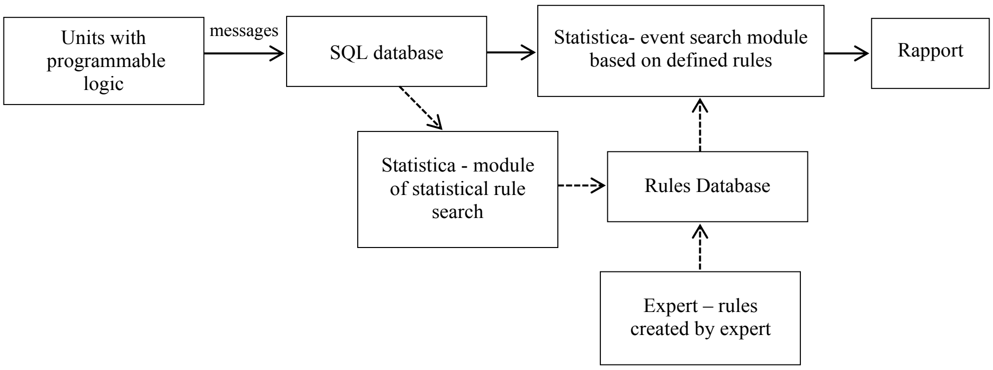

Units with programmable logic
messages
SQL database
Statistica- event search module based on defined rules
Rapport
Statistica - module of statistical rule search
Rules Database
Expert – rules created by expert

Figure 4.10. General system architecture

One of the assumptions of the project was a two-pronged ability to acquire rules. The first method is to create an expert rule based on the experience of a maintenance expert.

This experience may be a result of analysis of existing failures or knowledge of the rules that occur in the PLC program that monitors the process. The second source of the rules is a statistical analysis done during the implementation.

Sequential analysis for detecting recurring patterns in the event sequence resulted in 684 rules with assumed indicator levels: minimum support = 0.1, and minimal confidence= 0.5. Fig. 4.11 shows a graph of each rule with the level of support and trust it was gained. Only simple rules were searched according to the rule "if the predecessor than successor".

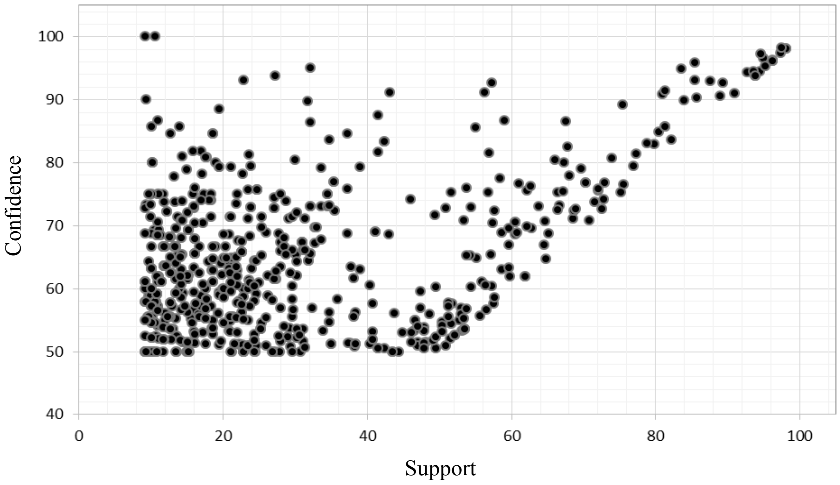
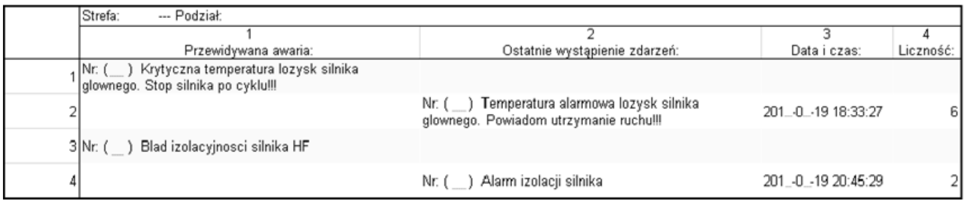


Figure 4.11. Chart of quality of obtained rules

The second inconvenience is generating reports. Reports should be easily readable to the recipient. This was solved through a report generated as a web-formatted file. Another difficulty was the frequency with which maintenance reports would be generated. At the time of the test, the daily frequency was assumed, during the test period, there was no division into different recipients. In the implemented solution, a time horizon is defined as a time frame of 48 hours, in which symptoms are analysed that may cause future damage.

Rapports have generated automatically in hypertext markup language (HTML) format (Fig. 4.12) and put into localisation on the server. They were accessible by remote desktop to all predefined users. After generating the report, it was available for maintenance to undertake corrective actions. After realisation of those actions, the system comes back to the safe state.



	Strefa: --- Podział:			
	1 Przewidywana awaria:	2 Ostatnie wystąpienie zdarzeń:	3 Data i czas:	4 Liczność:
1	Nr: (__) Krytyczna temperatura lozysk silnika glownego. Stop silnika po cyklu!!!			
2		Nr: (__) Temperatura alarmowa lozysk silnika glownego. Powiadom utrzymanie ruchu!!!	201_-0_-19 18:33:27	6
3	Nr: (__) Blad izolacyjnosci silnika HF			
4		Nr: (__) Alarm izolacji silnika	201_-0_-19 20:45:29	2

Figure 4.12. Example rapport from the proposed tool CAST-P

Reports were generated with division into production lines and after into hierarchical levels of machines. In the second column predicted failure were presented and in the third column - symptoms of this failure. The fourth column gives information about the date and time of the last symptom occurrence. In the last column information about symptom occurrence in a period calculated for this report were presented.

Assumptions made before the start of the tests were that report generation frequency once per day will be enough to achieve tremendous progress in diagnostic cover and increase of reliability and quality. So, a report was generated automatically once per day after six o'clock A.M. It was assumed that it would be a tool for reliability engineers to prepare a corrective maintenance action plan for the current day.

4.1.10. Results

4.1.10.1. Tool results

By analysing the results, surprisingly predictable were the proportions in which the symptoms occurred before the damage occurred. In the eight hours before the failure, 80%

of the symptoms appear. Fig. 4.13 shows the incremental graph (continuous line) and the percentage (dotted line) of the occurrences of the symptoms broken down into time intervals that divide the occurrence of the symptom from the occurrence of the failure.

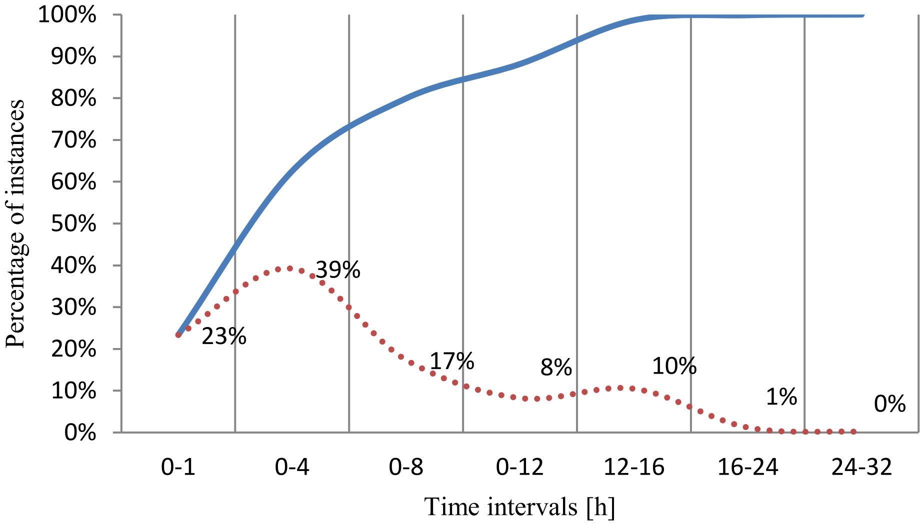


Figure 4.13. Chart of breakdown as a function of time of occurrence of the symptom

It has been observed that nearly 7% of all relationships occur at the same time as the damage occurs. Fig. 4.14 shows a graph of the relationship between the percentage of occurrences of symptoms and the time intervals counted from the occurrence of the symptom to the occurrence of the failure.

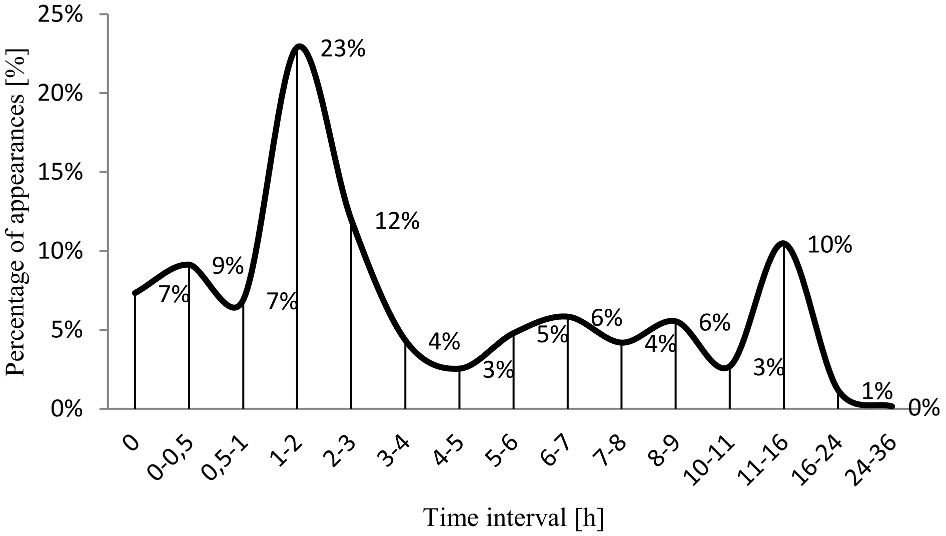


Figure 4.14. Chart symptom-effect relationship broken down by time intervals

Verification of these events has shown that certain rules should be excluded because of their resulting nature. These rules do not add value. They appear because they are the result of another rule.

4.1.10.2. OEE results

The main objective of this tool's implementation was to achieve an increase of the productivity indicator. The duration of the pilot implementation was six months. The analyses presented are related to this period (n+1), for comparison, the period of six months of the previous year (n) is used in the work. The OEE indicator is used as the superior indicator in many manufacturing companies and due to its cross-sectional comparison, the results of this index for the two specific time intervals were compared first. A brief explanation of OEE, the OEE rate for the entire year in which a test implementation of the tool was conducted on the production line A is presented in Fig. 4.15. The first component of the OEE indicator, Availability, for that period achieved a value of 88.5% and it is the ratio of the time difference between gross operating time and unplanned downtime divided by planned production time. Unplanned downtime for this period equal 11.5%. The second component performance rate for that period achieved 98.3% and it is calculated as a difference between net operating time and speed loses divided by gross operating time. Indicator of speed losses equals 1.5%. The last OEE component is quality rate calculated as a difference between effective operating time and quality losses divided by net operating time. For analysed time period it is equal 99.9%.

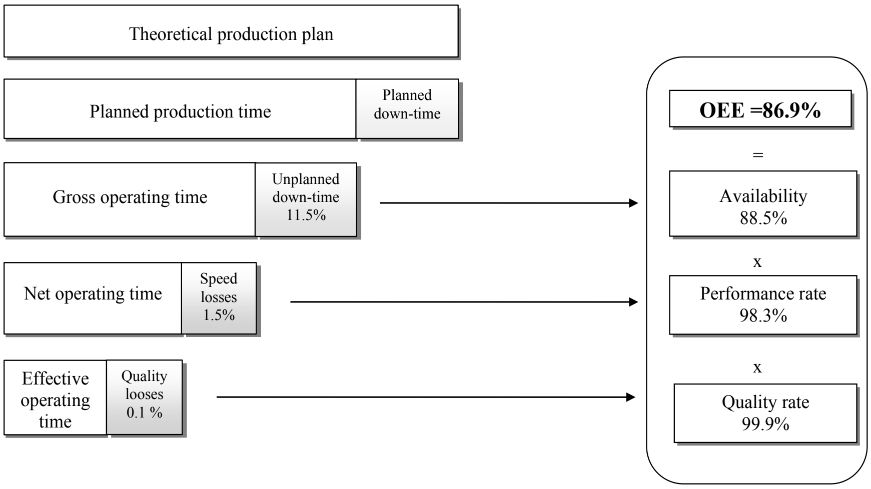


Figure 4.15. Yearly percentage of OEE indicator for line A at the year of case-study duration (n+1)

Comparing results of two following years (six first months of each year), an increase 2.1% of OEE indicator can be observed. The small decrease was observed in performance – 0.42%. It is mainly due to an increase in the speed loss rate from 1.2% to 1.51%. That regress can be explained by the work of quality personnel with new recipes as a result of new raw materials and impact of external temperature to raw materials and after on speed of process cycle.

The biggest increase was observed in the area of availability which value increased from 87.9% to 90%. As can be seen in Fig. 4.16, there are a few components which percentage share gives that final result. Unfortunately, one of the indicator components has increased its value by 0.23%. This component, named as *others*, sums the other components of losses whose single event value does not exceed 0.1% and it is impossible to qualify for any of the described codes. The progress in codes of preventive maintenance (-0.08%) and modification (-0.1%) has to be considered together, because the joint work of maintenance and production teams, over the increase of efficiency, caused that more work in the field of modification was carried out during the masked time of preventive maintenance, which number

Indicator		6 mth year n	6 mth year n+1		
Unplanned Downtime	Breakdowns	6.1%	4.03%		
	Defects in process	3.1%	2.75%		
	Preventive maintenance	1.3%	1.22%		
	Assorment exchange	0.8%	0.83%		
	Operator error	0.1%	0.11%		
	Start-up looses	0.1%	0.16%		
	Modification	0.1%	0.00%		
	Set-up	0.1%	0.13%		
	Machine cleaning	0.1%	0.17%		
	Others	0.4%	0.63%		
		Availability		**87.9%**	**90.0%**
Speed looses	Reduced speed	1.2%	1.51%	x	x
	Idling	0.2%	0.28%		
		Performance		**98.43%**	**98.01%**
	Rework	0.1%	0.1%		
				x	x
		Quality		**99.90%**	**99.90%**
				=	=
		OEE		**86%**	**88.1%**

Figure 4.16. Percentage of OEE indicator for line A in two compared periods

was also optimized (-0.08%). There are also few codes that remained with almost unchanged value (change is less than 0.1%) and those are the operator error, start-up loses, set-up and machine cleaning codes. There are two more codes that are the most interesting from the point of view of this work. This is the breakdowns code which gained -2.07% and defects in the process which gained -0.35%. At the same time, they are the two most significant codes affecting the value of the availability component. Profit in the above codes was obtained thanks to the proposed tool and after as a result of modifications that eliminated the original causes, optimizing the preventive maintenance plan for repeated faults, prediction of failures and failures, and analysis of the causes of these potential failures, the experience of production and maintenance staff that reduced the duration of the downtime. On the next pages, the explanation of the influence of the tool for the predictive failure analysis on the breakdown losses caused by machine failures will be presented. The comparison of the percentage of losses year-on-year (Fig. 4.17) shows certain repeatability in terms of months. This is due to the calendar of production and shutdowns, and the impact of external temperature on installations and, above all, on raw materials entering the process.

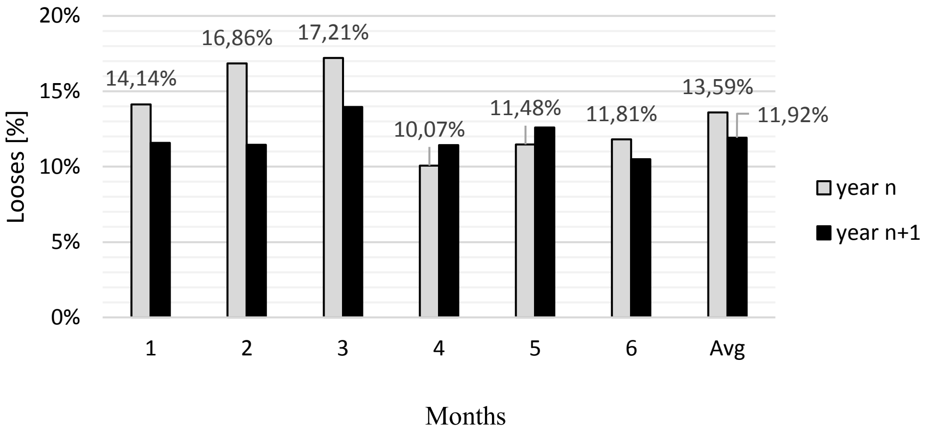


Figure 4.17. The sum of losses caused by unplanned stops and speed losses for line A in the year of tool implementation and previous year, expressed in percentage

This trend is also visible for the machines themselves, even taking into account two very similar production lines (Fig. 4.18). Some deviations year by year are disturbed by individual failures that last more than 400 minutes. It should be remembered that one unplanned stop lasting 8 hours reduces the monthly result by over 1.1%. Analysing the mean time to restoration (MTTR) indicator in Fig. 4.19, it can be seen that the "calming down" of this indicator by the stability of the value over time in the year of test implementation, which proves increased preparation for repairs (knowledge of how to repair, tools) and knowledge of impending

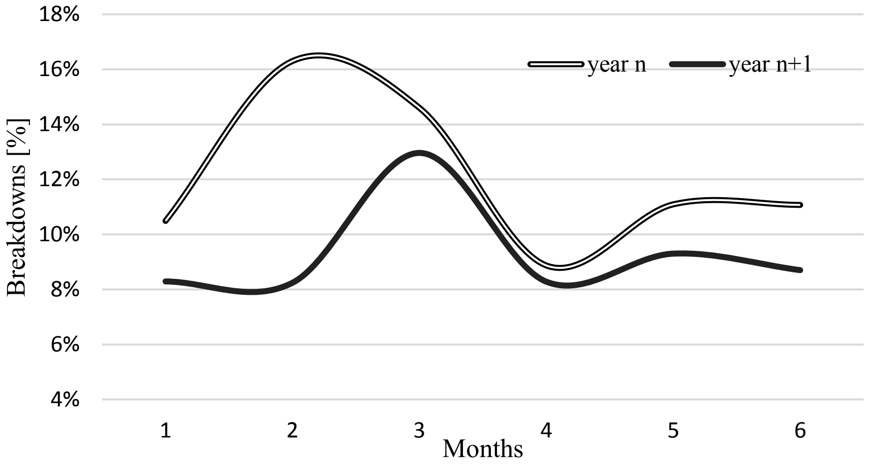
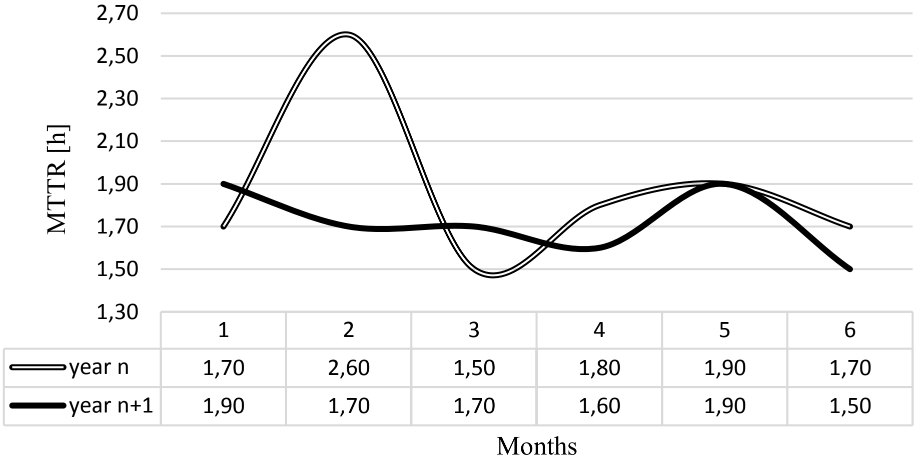


Figure 4.18. Cumulative percentage of breakdowns of line A and B in the year of tool implementation and previous year

breakdown (prediction), which makes it possible to prepare the workplace still in masked time and intervention is shorter in the case of quick detection (e.g.: if we know about the high bearing temperature, it is still possible relubrication it and hold to the planned shutdown with replacing, without prediction, maintenance will react when the bearing is already damaged, and it has to be replaced immediately because it cannot continue work).

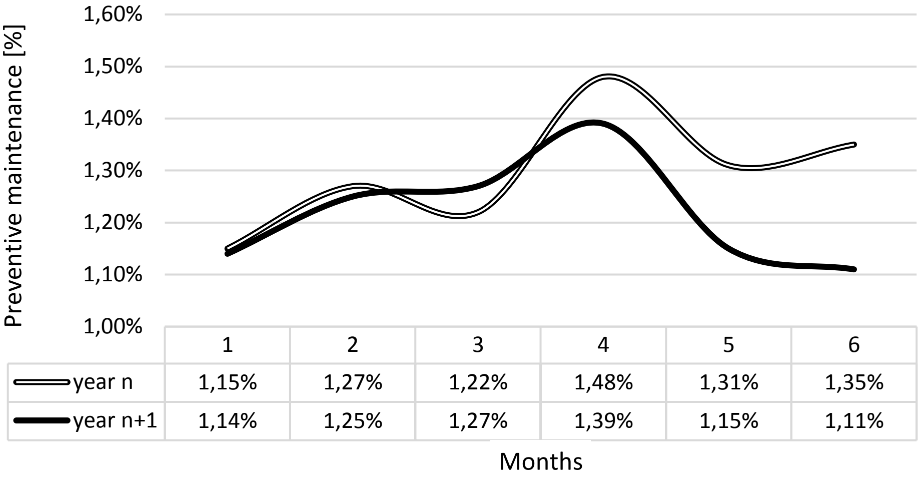


	1	2	3	4	5	6
year n	1,70	2,60	1,50	1,80	1,90	1,70
year n+1	1,90	1,70	1,70	1,60	1,90	1,50

Figure 4.19. MTTR of line A in the year of tool implementation and the previous year

As it was already mentioned above, the amount of time for preventive maintenance of line stop has undergone reduction (Fig. 4.20), but this does not reduce the amount of work and only reduces its frequencies. This has a positive effect on the result of the OEE indicator.

This was possible thanks to better knowledge about the occurrence of faults, planning the time of repairs at the time masked and updating the preventive maintenance plan in terms of anticipated failures.



	1	2	3	4	5	6
═ year n	1,15%	1,27%	1,22%	1,48%	1,31%	1,35%
━ year n+1	1,14%	1,25%	1,27%	1,39%	1,15%	1,11%

Figure 4.20. Preventive maintenance of line A in the year of tool implementation and the previous year

What is important from the point of view of the customer's maintenance services, which is the production department, compared to the previous year (Fig. 4.21), there has been a reduction in the fluctuations in the time load for which the maintenance operations are made. Greater stability results in fewer disturbances, more stable production, which translates into stability of quality results and improvement of production indicators - among other things, the production plan implementation coefficient.

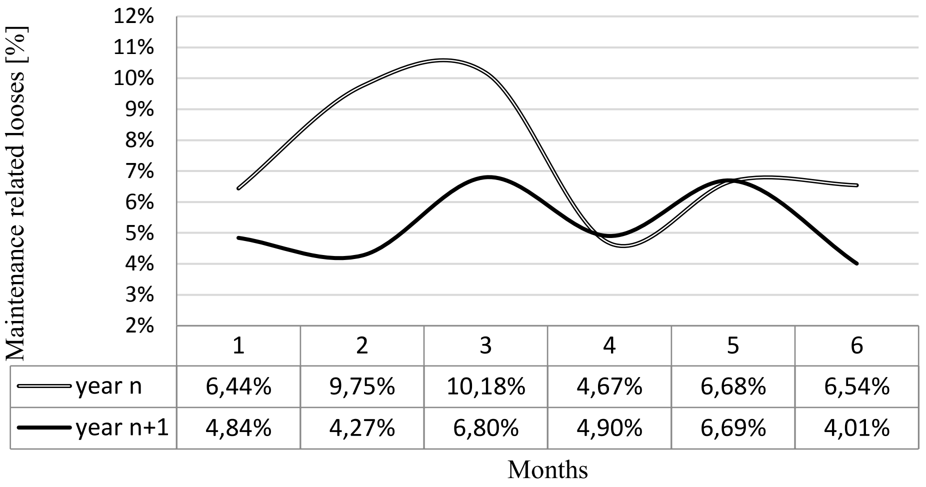


Figure 4.21. Losses due to unplanned and planned maintenance activities on line A in the year of tool implementation and the previous year

Interesting data appears when tables 4.2 and 4.3 are analysed. It can be seen that in the year of the test implementation there were more unplanned stops than in the previous year. It should be emphasized here that the breakdown is coded, every stop that was not planned a month earlier and not taken into account when creating a monthly production plan.

Table 4.2. Ratio of breakdowns numbers of line A in the year of tool implementation and the previous year

$\frac{\text{No. of all breakdowns in year n+1}}{\text{No. of all breakdowsn in year n}}$	126%
$\frac{\text{No. of mechanical breakdowns in year n+1}}{\text{No. of mechanical breakdowns in year n}}$	72%
$\frac{\text{No. of electrical-electronic breakdowns in year n+1}}{\text{No. of electrical-electronic breakdowns in year n}}$	149%

Table 4.3. Ratio of breakdowns time of line A in the year of tool implementation and the previous year

$\frac{\sum \text{of all breakdowns time in year n+1}}{\sum \text{of all breakdowns time in year n}}$	92%
$\frac{\sum \text{of mechanical breakdowns time in year n+1}}{\sum \text{of mechanical breakdowns time in year n}}$	63%
$\frac{\sum \text{of electrical-electronic breakdowns time in year n+1}}{\sum \text{of electrical-electronic breakdowns time in year n}}$	111%

For this reason, also stops that resulted from noticing the symptoms of a future failure and stopping the line to eliminate the primary cause of a possible failure are counted as a breakdown. Thus, seeing that the number of unplanned shutdowns increased by 26% year-on-year. Mainly this was due to stoppages on the electrical side or electronics. At the same time, it can be seen that the sum of the number of stops in the year of the test decreased by 8% compared to the previous year. And more importantly, there was a significant drop in stops due to mechanical breakdown awareness (by 37%).

Table 4.4. Ratio of breakdowns numbers of line A in the year of tool implementation and the previous year

$\frac{\text{No. of all breakdowns at first 6 months of year n+1}}{\text{No. of all breakdowns at first 6 months of year n}}$	101%
$\frac{\text{No. of mechanical breakdowns at first 6 months of year n+1}}{\text{No. of mechanical breakdowns at first 6 months of year n}}$	62%
$\frac{\text{No. of electrical-electronic breakdowns at first 6 months of year n+1}}{\text{No. of electrical-electronic breakdowns at first 6 months of year n}}$	120%

Table 4.5. Ratio of breakdowns time of line A in the year of tool implementation and the previous year

$\frac{\sum \text{of all breakdowns time at first 6 months of year n+1}}{\sum \text{of all breakdowns time at first 6 months of year n}}$	69%
$\frac{\sum \text{of mechanical breakdowns time at first 6 months of year n+1}}{\sum \text{of mechanical breakdowns time at first 6 months of year n}}$	46%

$\frac{\sum \text{of electrical-electronic breakdowns time at first 6 months of year n+1}}{\sum \text{of electrical-electronic breakdowns time at first 6 months of year n}}$	92%

Even more interesting are the data from the six months during which the test was carried out and the six months of the previous year (Table 4.4 and Table 4.5). They show a slight increase in the total number of breakdowns (by 1%). A significant drop in stops due to mechanics (by 38%) and increase in breakdowns on electrical/electronical equipment (by 20%). What is more interesting is that during this period the total amount of time of breakdowns dropped by as much as 31%. In mechanical breakdowns it was up to 54%.

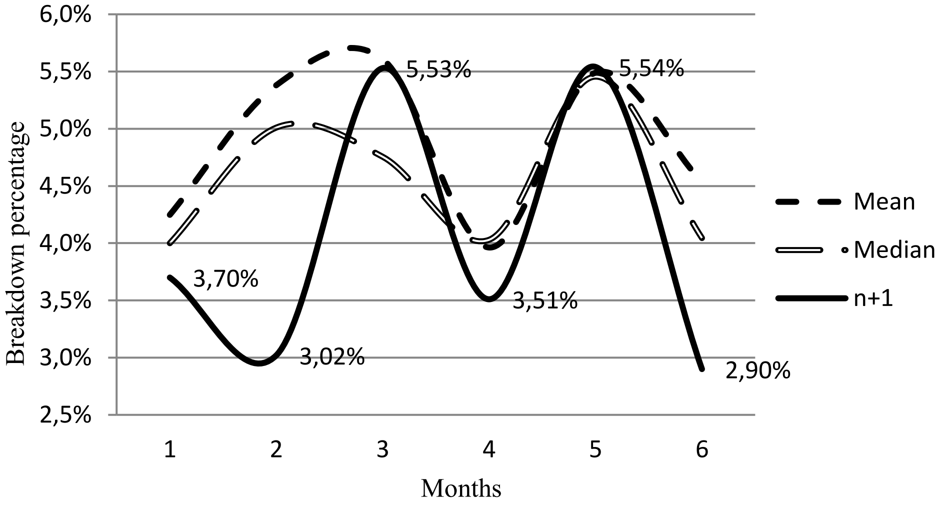


Figure 4.22. Presentation of the mean and median value of breakdowns percentage in four following years (n-2, …, n+1) and breakdowns percentage in the year of test

Looking at Fig. 4.22, it can be seen that the total percentage of losses due to breakdowns is lower than the median and mean value of four following years. It also shows a certain tendency of breakdowns which cause should be seen in relation to the atmospheric conditions (temperature, humidity- indirectly influencing the raw materials) as well as the times of machinery planned downtime (human factors - holidays, etc.) and then their start-ups.

Table 4.6. Comparison of number and summary time of long breakdowns over 2 and 3 hours in the year of test and the previous year

	6 months of year n		n		6 months of year n+1		n+1	
	No.	Σ of time [min]	No.	Σ of time [min]	No.	Σ of time [min]	No.	Σ of time [min]

Breakdowns over 3h	10	3574	14	4776	3	929	6	1747
Breakdowns over 2h	16	4445	20	5607	8	1599	17	3277

Very interesting data is shown in Table 4.6. It can be seen in the manner of reduced number of long stops of machines (more than 2 and 3 hours). During the test period, these values are significantly lower, which confirms the effectiveness of the proposed solutions.

4.1.10.3. CMMS results

The second source of authoritative data regarding the impact of the proposed tool on the improvement of results is CMMS which is used to manage the maintenance department.

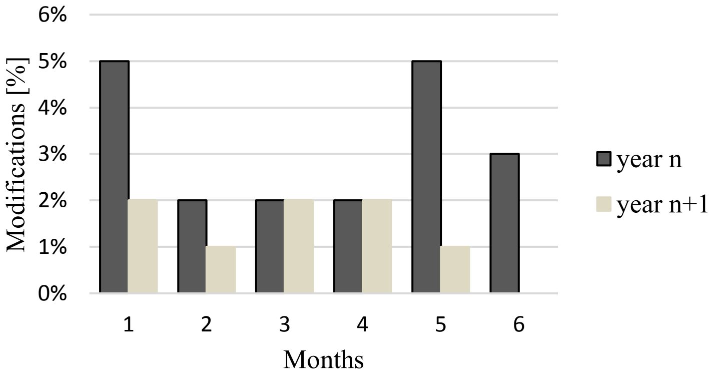


Figure 4.23. Cumulative value of time spends for modification by the maintenance of line A and B in the year of tool implementation and the previous year

In Table 4.7, the results of the various types of interventions performed by maintenance are presented. The first of them are failures which are unplanned maintenance activities, difference between this and the OEE indicator is that in CMMS doesn't mean that the line has to be stopped. The second type of intervention is planned repairs. These are repair activities not planned as preventive maintenance but requiring intervention on the machine during the preventive or masked time. The third type of activity is training. It is only part of the whole training and concerns only those that were carried out on the machines. The next step is planned maintenance activities, in other words, preventive maintenance. The last type of intervention presented is modifications (Fig. 4.23). These are modifications made by maintenance personnel during the stoppage as well as the work of the line.

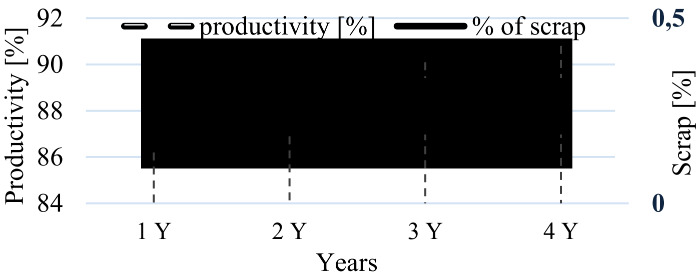
Table 4.7 Quantity of maintenance work orders divided into categories for production lines A and B over two years

Work order type:	year n	year n+1	Ratio	year n	year n+1	Ratio
	Line A	Line A		Line B	Line B	
Failure	1080	989	92%	1162	1138	98%
Planned repair	1588	2416	152%	1488	2307	155%
Training	6	1	17%	5	1	20%
Planned maintenance	601	655	109%	394	540	137%
Modification	49	34	69%	33	32	97%
Σ	3324	4095		3082	4018	

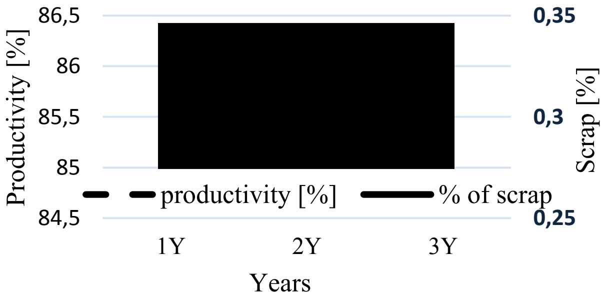
Analysing Table 4.7 with annual results, it can be noticed that the number of failure interventions at line A decreased by 8%. However, the number of planned repair interventions increased by more than 50%. This is the exact opposite value to the number of breakdowns in the same period in the OEE index.

4.1.10.4. Impact of productivity improvements on product quality results

Based on the author's experience and results of chosen results of two production lines productivity and percentage of scrap graphs, it can be stated that increase of productivity influence positively the scrap reduction (Fig. 4.24.).



[redacted]



[redacted]

Figure 4.24. Graphs of the relation between productivity and scrap percentage on sample production lines

That is because increasing productivity decreases unplanned downtime and other MUDA losses. There is a certain level of losses resulting from planned stops and starts and waste arising from the construction of the production process. It can be stated that focus on productivity increase, also results positively in quality. At the current high level of quality and low associated losses, possible progress in this area is very challenging. That is why the author's actions focus on productivity and indirectly influence quality.

4.1.11. Conclusion

Despite the short implementation and the limited possibilities of using data from sensors and machines, the results show very promising results. Return on investment (ROI) (expenditures for the application and implementation to the profit achieved from the increase in machine availability) in this case is between 3 and 4 years. This is a very good result for an IT tool. By developing this tool and using the data lake tool in a very fast way, one can implement this tool in another twin plant in the enterprise. In this way, the ROI will be accelerated again. Additional functionalities presented in the following examples increase the value and validity of the proposed solution.

4.2. Case study - Safety anomalies detection

4.2.1. Description of the case study

Unfortunately, during the test implementation, it was not possible to connect the CAST-P system with any physical input of the control signal of the tested machines and devices. This was one of the restrictions provided that the author obtained permission for tests. The only possible thing was to create expert rules based on the available data that would detect functional safety abnormalities.

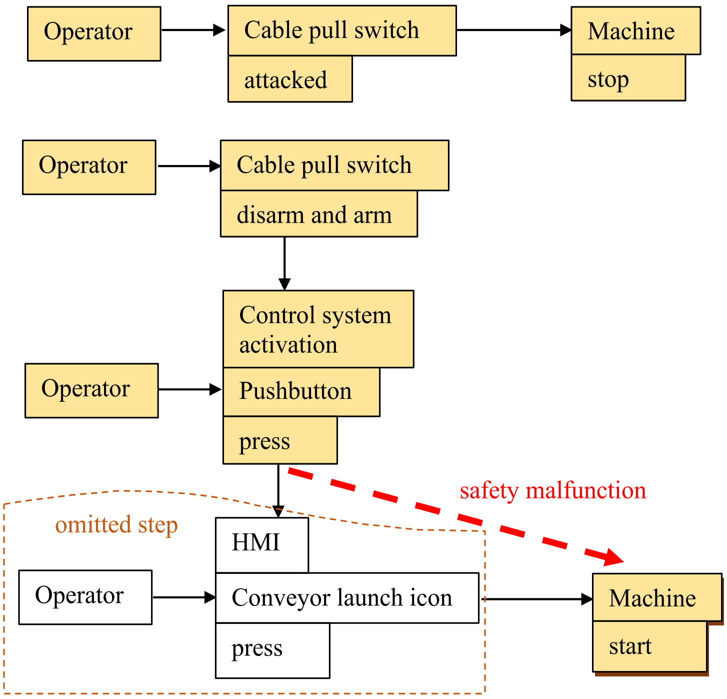


Figure 4.25. Diagram of control system malfunction

One of such expert rules was based on the example from the author's experience. In the machinery analysed in the case study described above, after information about the serious accident in another plant, action was taken to make additional verification of proper work of all safety elements (functional test) during a standard test to check – cable pull switches (safety lines). After an emergency stop (cable pull switch was attacked) according to safety standard ISO 12100 [62], the operator has to disarm attacked element, put it into normal position (armed again), start control systems and push the button on HMI (move forward) to start conveyor again. Surprisingly, after unlocking and arming the safety line, the operator pushed the button to initiate the control system and the conveyor started moving forward without command, which should not have taken place (Fig. 4.25). The start of the machine should happen after starting it intentionally by the operator using the button - start. After analysis, it was stated that the root cause of this anomaly is an error of HMI firmware. The software keeps into memory the table with the previous state of inputs and outputs, among others also all push buttons on the screen. After communication with the HMI producer, the error was removed one month later by the HMI manufacturer with a new firmware version.

It should be emphasized that after uploading the new firmware, functional tests were performed, unfortunately, the error appeared only in one specific sequence of action, which resulted in the non-revealing of this error during the test. Unfortunately, with the growing speed of creating new equipment, software and applications, errors in software can become more frequent what for the user means a higher risk for downtime and what is a much worse increased risk of safety accidents.

Based on this example, an expert rule which will detect the presented above anomaly, which will prevent such accidents in the future, was added in the rule database. This rule can be generally recorded as "IF *safety system armed* AND *errors reset command (HMI)* AND *machine stop (no command to start)* AND *machine start* THAN *Error – Safety system abnormal work of machine....''*. Unfortunately, such a rule had to be duplicated and assigned for each safety circuit separately, as the events of each section have different markings. The entry of expert rules, based on risk analysis and safety regulations and standards, significantly improves the safety of the system and devices, protecting against similar outcomes of faulty firmware and possible PLC program errors in the future.

4.2.2. Conclusion

In the above-presented example, the issue of safety is very important from the point of view of the current rapidly changing environment of industrial automation. In many enterprises, level one software updates are very common, sometimes even without the knowledge of users. Therefore, the proposed solution significantly increases employee safety. The presented solution is the development of the application of the tool presented for the prediction of failures. It increases the importance and justifiability to implement CAST-P in modern production lines.

4.3. Case study of the application the method of functional test optimisation

The chosen case study object is a modern single end impregnation line used to treat yarns made of polyamide, polyester, viscose and other raw materials so they are suitable for applications - use in tires. The pull roll section is a part of a line analysed in this case study.

Following a risk analysis (Failure Modes, Effects and Criticality Analysis), one safety function and one complementary protective measure were identified in this section of the production line. The safety function secures by restricting access to the machine's rotating parts and parts with ingress angles. The first complementary protective measures role is to prevent the hand or forearm from being caught by the thread of textile cord by installing a cable pull safety switch. The safety function has a verified value of SIL 2. The other complementary protective measure has an estimated SIL1. It can be calculated from the manufacturer's data that each of the given safety functions and supplementary measures has reached the claimed SIL level (SIL 2, SIL1).

The first supplementary measure, which prevents staff from being caught by the threads of a textile cord, based on the reliability data of the components of this function, has a functional test equal to a service life of twenty years, which means that there is no need for a control test of this function. The analysis proposed by the author has been carried out taking into account the facts of risk management. During the analysis, it was assumed - SIL1.

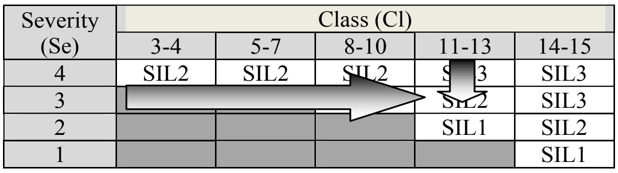
The analysis of entries to the CMMS application and conversations with both production operators and maintenance staff shows that an unintentional activation of complementary protective measures by the operator or product takes place on average once every twelve months. Therefore, it can be qualified to a low probability of occurrence. The last analysis criterion, which is the possibility of detecting a failure, was assessed as practically impossible to detect.

Table 4.8. Graph of additional action estimation for a first complementary measure of a section of impregnation line working in low demand mode

		Detection	
		Possible	Impossible
Probability of occurrence	Low	N/A	FTI
	Medium	VI	FTI
	High	FTI	Risk analysis

Based on the estimation of additional actions (Table 4.8), it can be concluded that it is necessary to change the time interval of the functional test. Taking into account the frequency of activation of the function and damage, on average once a year it is proposed to double the frequency of activation - which corresponds to six months. In conclusion, the result of the analysis is to change the functional test interval to six months.

The case study is based on pull roll section with the safety function of door locking and monitoring. The required safety integrity level is the result of a risk assessment and refers to the amount of risk reduction to be conducted by the safety-related parts of the control system. Part of the risk reduction process is to determine the safety functions of the machine. Safety function which protects by restricting access to the cabinet has estimated SIL2 based on the SIL assignment matrix proposed in the EN 62061 standard. The severity of the injury was estimated as level 3. Frequency and duration note 3, the probability of hazard event as possible and note 4, avoidance as possible with note 4. Cl=Fr+Pr+Av=3+4+4=11 (Fig. 4.28), safety function with value SIL2.



Severity (Se)	Class (Cl)				
	3-4	5-7	8-10	11-13	14-15
4	SIL2	SIL2	SIL2	SIL3	SIL3
3				SIL2	SIL3
2				SIL1	SIL2
1					SIL1

Fig. 4.28. SIL assignment matrix for the analysed safety function.

Analysing available data, it was assumed that the frequency of unplanned activation is frequent, and the detection of possible damages is possible without stopping the machine. The following proposed method, that can be estimated that additional action, is additional visual inspection (Table 4.9) in this case. As the average frequency of unplanned activation or damage was estimated to be six months, visual inspection of that subsystem of the safety-related control system was planned for three months. Manufactures data presents the T1 value for proof test interval as 20 years. So, there is no need to plan an additional test for this element. According to the author’s proposal, a functional test is completed with the frequency of twelve months.

Table 4.9. Graph of additional action estimation for defined safety function of the cord twisting machine.

		Detection	
		Possible	Impossible
Probability of occurrence	Low	N/A	FTI
	Medium	VI	FTI
	High	FTI	Risk analysis

Summarizing achieved results, it can be stated that the use of the proposed method achieved the pursued objectives. Graph of additional action estimation helps the user to minimalize additional risks not covered before. The tool is easy to use and can be easily utilised by maintenance or personnel responsible for safety. Implementation of actions defined in the proposed graph influence on results of risk analysis made at the different level of company management according to ISO 31000 [71].

4.4. Case study of proof test interval proposed method

As an example, a safety function has been chosen for detecting the presence of a worker in the danger area while the robot is operating, and then, upon detection, to stop the robot. Presence detection is done by installing a laser scanner in the robot's operating area (Fig. 4.29). When a worker is in the danger area, even out of sight of other workers, it can be detected and prevented from inadvertently moving/restarting. In this example, as a result of the risk assessment, the PLr / SIL was determined to be PLr=d / SIL=2.

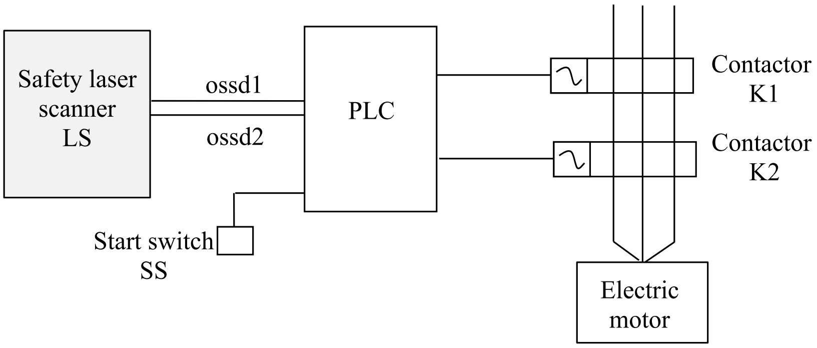


Fig. 4.29. A simplified model of safety function configuration with a safety scanner.

The laser scanner (LS) monitors safety in an area by scanning a laser beam and monitoring the reflected beam (calculating the distance to a surrounding object based on the time it takes for the beam to reflect off the object and be received). Detecting a failure by self-diagnostics or disturbance of the laser scanner (LS) by ambient light. If the laser scanner (LS) is disturbed by ambient light, the output will turn off. The laser scanner (LS) and contactors (K1, K2) that control the output are connected to the PLC.

The PLC program performs the following functions:

- If operation is ready, if the start switch (SS) is pressed after the output of the laser scanner (LS) ((ossd1) and (ossd2)) are turned on, the PLC output will be turned on to start the machine.
- If the laser scanner (LS) output (ossd1 or ossd2) is turned OFF during machine operation, the PLC output will be turned OFF to apply an emergency stop to the machine.
- If an emergency stop occurs, the PLC output will remain OFF even if the start switch (SS) is pushed down.
- If an emergency stop occurs, the machine will revert to the operational ready state if the laser scanner (LS) is turned on (ossd1, ossd2=ON).
- To prevent accidental startup of the machine due to failure of the start switch (SS), the reset of the standby switch (SS). Shall be conditional on the ON→OFF falling.

The evalution of safety related control system have to made by division into subsystems. Three sybsystems of this safety function can be sparated as presented on Fig. 4.30. For each subsystem the relevant safety-related data are available and are assumed as shown in Table 4.10.

Table 4.10. Reliability data of the examined safety function components

Name	Device name	B_{10D}	DC_{avg} [%]	PFH_d [1/hour]	HFT
LS	Laser scanner		90	$1.03x10^{-7}$	1
PLC	PLC		99	$2.31x10^{-9}$	1
K1	Contactor	2 000 000	99 (HFT=1)		0
K2	Contactor	2 000 000	99 (HFT=1)		0

First subsystem design of the input which is safety laser scanner as an electronic part and data provided by the component manfacturer of the pre-designed safety laser scanner, susbsystem can claim SIL 2 with an architecture with a hardware fault tolerance equal to 1 (HFT=1) and DC equal to 90%.

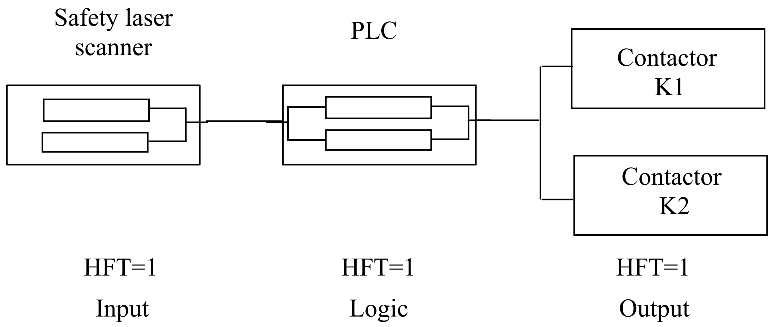


Fig. 4.30. A simplified diagram of analysed safety function.

Second subsystem – PLC is also an electronic part with data provided by component manufacturer of the pre-designed safety contoller and can claim high SIL equal to 3 (PFH=2.31x10^{-9}). Diagnostic coverage of this subsytem is very high with value 99%.

The third subsytem of the analysed safety function is built with an architecture of a hardware fult tolerance equal to 1 (HFT=1). From the analysis it is known that contactors are used for two shifts each day on 300 operation days a year. The mean time beetween the beginning of two successive swithing of the valve is estimated as 1 hour.The evaluation of PFH value is made with the failure rate determined by using B$_{10D}$ (based on IEC 62061 sttandard) This yields the following values:

- d_{op} = 300 days per year;
- h_{op} = 16 h per day;
- t_{cycle} = 3600s per cycle;
- B_{10D} = 2 million cycles.

With those data the following quantities can be calculated:

$$n_{\mathrm{op}} = \frac{d_{\mathrm{op}} \cdot h_{\mathrm{op}} \cdot 3600}{t_{\mathrm{cycle}}} = \frac{300 \cdot 16 \cdot 3600}{3600} = 4800 \text{ cycles/year}$$

$$C = \frac{n_{op}}{8760} = 0{,}5479 \text{ cycles/hour}$$

Having calculated those input values dangerous failure rate can be calculated as follows:

$$\lambda_{De} = \frac{1}{T_{10\mathrm{D}}} \ln \frac{1}{1-0.1} = \frac{0.105}{T_{10\mathrm{D}}} \cong \frac{0.1}{T_{10\mathrm{D}}} = 0.1 \frac{C}{B_{10\mathrm{D}}}$$

$$\lambda_{\mathrm{De}} = 0.1 \cdot \frac{0.5479}{2000000} = 2.74 \cdot 10^{-8} \text{ hour}^{-1}$$

The following assumptions were made for calculation of PFH of this subsystem. The value of the T1 parameter was chosen based on Table 3.14, which assumes a test proof period of one year for functions with SIL=1 and HFT=1. The T_1 value is the proof test interval of the proof test (1 year) as it is smaller than useful lifetime (20 years). T_2 is the diagnostic time interval as in this function diagnostic test is made with switching of the contactors than T_2 value is equal to:

$$T_2 = \frac{1}{C} = 1{,}825 \text{ h}$$

Other values used in calculation of the PFH value of this subsystem are equal to:

DC = 99 %

T_1 = 8760 h

Due to the lack of information from the manufacturer about the value of common cause failure factor (β) it was assumed on the basis of IEC 62061 standard to be 10% (the most unfavorable variant was assumed)

β = 0.1

Finally, as this subsystem has to be analysed as architecture D the equation for PFH gets the form:

$$PFH_O \cong \left\langle (1-\beta)^2 \cdot \left\{ [\lambda_{De}^2 \cdot 2 \cdot DC] \cdot \frac{T_2}{2} + [\lambda_{De}^2 \cdot (1-DC)] \cdot T_1 \right\} + \beta \cdot \lambda_{De} \right\rangle =$$

$$\left\langle (1-0.1)^2 \cdot \left\{ [\left(2.74 \cdot 10^{-8}\right)^2 \cdot 2 \cdot 0.99] \cdot \frac{1.825}{2} + \left[\left(2.74 \cdot 10^{-8}\right)^2 \cdot (1-0.99) \right] \cdot 8760 \right\} + 0.1 \cdot 2.74 \cdot 10^{-8} \right\rangle =$$

$$2.74 \cdot 10^{-9} \text{ [h}^{-1}\text{]}$$

The overall value of PFH for SCS by summation of the PFH of the three subsystems will be equal to:

$$PFH_{\text{SCS}} \cong PFH_{\text{I}} + PFH_{\text{L}} + PFH_{\text{O}}$$

$$PFH_{\text{SCS}} \cong 1.08 \cdot 10^{-7} \text{ [h}^{-1}\text{]}$$

This SCS reaches SIL 2 value, which is consistent with the results of the risk analysis for this function. Additionally, the system should be verified in terms of architectural constraints in subsystems in the context of taking into account the indicator SFF. Each of the subsystems has a high level of diagnostic coverage equal to or greater than 90%, which translates into the SFF value and finally that each subsystem can be assigned SIL 2. Therefore, the entire function also meets the requirements for SIL 2.

The author chose the example with the laser security scanner as it shows on the one hand empirically the correctness of the proposed method and on the other hand shows a certain pitfall. The manufacturer of the scanner, due to the fact that it is built to ISO 13849 category 3, does not have full diagnostics and the manufacturer requires in the user manual a weekly proof test. Unfortunately, from the author's experience, such requirements, which are very important and crucial from the safety point of view, are often forgotten by either the machine manufacturer (to include it in the manual) or the maintenance department, which puts all machines into “one bag” with one proof testing frequency.

4.5. Chapter summary

Considering all data and information presented above it can be claimed that the production of a good, competitive product in safe conditions could be considerably raised by the implementation of proposed solutions. The summary of the outcomes obtained can be divided into two separate results. The first is a prediction tool for failures and the safety anomalies detection tool with the optimisation of functional test frequencies with an impact on machine availability time. The second is a test interval optimization method.

The first part of the case study concerned the results of the test solution of predicting failures based on a statistical analysis of the symptoms recorded by the IACS. Short test lead time and limited resources did not allow the system to expand, but the results confirmed the effectiveness and utility of the tool. The implemented statistical tool allows for a further 2.1% increase in the availability and overall efficiency effectiveness on the examined production line. The proposed tool corresponds to the industry's current requirements for increasing the reliability and availability of machinery and equipment. The tool is designed for modern production lines, as it is based on information collected from all hardware and surveillance systems. On older installations, system deployment would be unprofitable. It is due to the need for additional inputs related to the installation of the measuring system of the equipment and the installation of the data collection system from the machines as well as the recording of the operator's activities. The presented system uses modern methods of collecting, processing and analysing data according to trends of the Industry 4.0.

After a complete optimisation of the solution, the system can easily be copied and installed on other similar (or twin) installations in the enterprise. That results in very fast, inexpensive, and not requiring considerable human resources change that can increase the reliability and availability, which indirectly also affects the quality of manufactured products. The proposed tool is designed for the users, who, by analysing the automatically generated reports, first will eliminate the potential abnormal events (short-term goal). Second, it will take action to eliminate the cause of this anomaly or reduce its impact (long-term goal). Another functionality of this proposed tool is the ability to protect workers' safety by detecting hazardous situation using the same tool (CAST-P) as in the case of failure prediction. Due to the lack of possibility of full implementation of the solution, it is not possible to confirm all advantages of the proposed tool. Despite this, the ability to implement expert rules to ensure that functional safety standards are respected (shown by the example of minimizing the impact of modifications to controller programs and firmware updates) significantly affects the assurance of a designed and verified level of functional safety of machines. The same tool can also be used to protect machinery and employees in the event of cyber-attacks on safety related control systems. This shows that the proposed tool is very versatile, and its application can bring many benefits in terms of both productivity and safety in the broad sense. Thanks to this approach, it is possible to achieve progressive productivity while maintaining an appropriate level of safety.

During the test of the rule editor, only simple one to one rules were used, but in the future, it could be recommended to work with *n* to 1 rules. This can influence on mean time between the first or second symptom and failure, and also finding such rules can be very interesting from the perspective of finding the root cause of failure. The frequency of report generation during the test was defined before the start-up of the test. During the test period, as it was already mentioned, the system generates reports once per day. After six months of tests, the author is convinced that increasing the frequency of generating reports for corrective maintenance is necessary. After analysis mean time between symptom and a failure this time seems to be unadjusted. The alternative is to generate reports close to real time frequency, which would physically result in the appearance of new messages every few minutes on the laptop or mobile phone of maintenance workers. There is a risk that this method at the beginning will disturb work of breakdown workers because their working time, a maximum 30% of its working time is reserved on breakdowns. The rest of the time is spent on planned repairs and preventive maintenance. It is possible to use artificial intelligence in the process of helping to make decisions as described in more details and explained in the section on productivity aspects. The solution can be also equipped and extended with a database of expert rules regarding the type of equipment that has been installed by manufacturers (PLC, sensors, etc).

Concerning functional test optimisation which allows to provide the required SIL, taking into account the aspects of environment and risks in the company, which are not taken into account when calculating the SIL according to IEC 62061 [57]. Additional verification or a shorter frequency of proof tests allows to minimize the situation of the safety integrity level decreasing over time. The third important thing is to combine the frequency of the different tests in order to minimise machine downtime and consequently minimise the production losses. The method considers the impact of the environment in the operational stage of the life cycle. The tool presented above are a new approach taking into account the experience of the author.

The second part of the case study was dedicated to the proof test interval method. From the results obtained it can be stated that the proposed method simplifies and unifies the topic of safety function testing. It allows the plant to have a consistent policy and strategy of safety function testing. The example also shows that one should be careful and verify the machine manufacturer's recommendations before adopting schematic solutions.

Chapter 5

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

This chapter sums up and presents the discussion of the assumptions presented at the beginning of the dissertation. At the beginning of the dissertation, the author presented two assumptions. Each of them will be briefly discussed and a summary of the results will be presented. At the end of this chapter, possible directions of research aimed at developing new methods and tool will be presented

5.1. Summary of the dissertation

5.1.1 Impact of the proposed method on availability and productivity

The first objective of this research was that in a modern machinery plant with already implemented techniques for productivity improvement, by the implementation of the computerised predictive tool, progress in productivity indicator at a minimum of 0.5% can be achieved. As illustrated in the case study, this tool reduces the number of failures and resulting outages by at least 2.1%. That seems to be a small value, however, given that after the TPM and RCM deployments, the fault mean level is between 1.5% and 5%. Therefore, it is relatively a considerable value. All the more, if it is converted into costs. After conversion, 0.5% of productivity loss in the plant operating in the continuous system gives up to 43.8 hours / year. Depending on the production line, this can result in a loss between several dozen and tens of thousands of Euros per year, considering the fixed costs, employment costs, waste and other costs calculated according to the fixed costs method. CAST-tool force is also in its fast adaptation for the same or similar construction of production lines. Implementing the CAST-P tool in the first assembled production line can significantly speed up productivity gains. During the implementation of the CAST-P tool, it was noted that many of the sensors reported anomaly shortly before the occurrence of the failure. That is related to the assumptions of the designers of the analysed production lines. Many of the sensors have only one alarm threshold that protects machines from greater damage or breakdowns. They are not suitable for working with failure prediction tools. As a result, designers should now consider these available capabilities. The cost increase would be negligible, as at present most of the sensors communicate through network protocols or can program multiple outputs in discrete circuits. On the other hand, the effectiveness of predictive detection would improve significantly. The author in the preparation stage of CAST-P implementation has focused on the human aspects of maintenance work. From the author's experience as a manager, one can be tempted to argue that the consistent overall management of personnel in maintenance brings comparable results to the implementation of modern predictive tools. That is why it is so important to properly manage the staff before the tool is to be implemented in place. In the absence of such an approach, positive results will be countered by negative factors such as increased failure on one of the shifts due to lack of competence, examples can be multiplied. In this aspect the objective of dissertation can be deemed to be completed

5.1.2. Impact of the proposed methods and tool on functional safety

The second aim of the research conducted by the author is to maintain functional safety regarding availability aspects. This goal is achievable by using a failure prediction method and tool, proof test interval method and functional test optimisation method.

Based on the first point mentioned above, it can be concluded that it is an effortless profit. Due to the fact that with the implementation of the failure-prediction tool it is possible to use it for other purposes, such as ensuring the functional safety at required level. The method proposed in this aspect requires analysis and implementation of expert rules. However, it is an activity that is anyway required due to the obligation to perform the risk analyses of machines. The user gains at least two important things:

- automatic verification of the compliance with machine safety standards
- knowledge and information required for the risk analysis in form of discovered rules that concern functional safety components, in particular those relating to human/machine interactions.

Respecting the first point allows modifications to be made to the firmware and the PLC or HMI software to remain at the originally designed and validated functional safety integrity level. This is a very important point because in theory, according to existing standards, software should provide a constant level of functional safety, but as practical cases show, this is not the rule. In the second case, the machinery as an element that changes and evolves over time is also subject to periodic verification and risk analysis. The rules found for safety components are very important material for the risk analysis and modification in order to reduce or eliminate future failure events. On the basis of results obtained during the research, it can be stated that the purpose has been fulfilled. From the discussion related to the objectives and questions of the research presented in this dissertation a number of conclusions can be stated.

The second topic discussed was to clearly define the user requirements for the frequency of proof tests regarding the machine's environment. The tool presented by the author serves to improve the ease of correct selection, helps to optimize the functional and proof test intervals considering specific aspects of the risk management in life cycle.

The tool of functional test optimisation presented by the author serves also to improve the productivity KPIs defined above, helps to optimize the functional and proof test intervals taking into account specific aspects of mentioned risk management. This tool is the author's response to problems encountered in his professional practice and regarding typical practical aspects. An important point to emphasize is the fact that many safety system manufacturers assume that the mission time of the machines is twenty years. This fact must be considered by the user for machines that are already around twenty years old, as they have to prepare for the wear-out phase of the systems. Other conditions, which could be included in new versions of the risk management or quality management standards, may necessitate changes to the proposed method. This tool has been used several times so far and further testing is needed to confirm its effectiveness in different cases under changing conditions.

5.1.3. Potential gains in other areas

An important function of the proposed predictive method is its ability to be implemented for the prediction of functional safety threats caused by cyber security attacks. The proposed solution is based on a relatively simple method but has undeniable advantages. Due to the separation of the system from other systems, it is resistant to hacking attacks, by performing prior analysis and selecting the most critical locations is strongly focused on providing risk management for the company. Therefore, it prevents physical damage to the machines. Its purpose is not to analyse the whole spectrum of potential attacks.

The proposed tool can also be used to analyse the impact of changes in parameters influencing energy consumption. This has another measurable effect on company costs where the price of utilities plays an increasingly important role in the global manufacturing costs of a product. The application of this method in the detection of quality anomalies also has a significant potential for the cost reduction effect.

The last proposed place of implementation of the tool is searching for rules in case of the operator's behaviour. The possibility of using this tool already at the stage of operator training in simulated conditions allows, on one hand, to teach the right behaviour and, on the other hand, it is an interesting material for analysing whether changes in the machine or interface available to the operator should not be made due to repeated human errors.

5.2. Proposals of system evolution

The proposed method of failure prediction has many advantages which are described above. However, due to some initial assumptions, it also has limitations to work on in the future presumable changing conditions. Due to the assumption of placing a human being in the middle of the whole system, a lot of data about the rules and the work with the choice of rules must be done by a person. This is an arduous and time-consuming task. In the process of subsequent implementations, gathering experience from implementations, it is possible to work on applying machine analysis in these activities in a balanced way, in order not to lose control over the rule selection process. Another point for analysis may be to change the algorithm of abnormal event prediction. The adopted solution was based on a basket analysis with FP-Growth algorithm. Currently, there is a very fast development of algorithms for big database analysis. Therefore, it is necessary to consider changing the search algorithm as a function of the advantages and limitations of new solutions. Another aspect is to consider the implementation of the proposed method already at the stage of designing new machines. This may significantly speed up the implementation, extend the possibilities of using the tool, and, at low cost, equip machines with sensors adapted to a predictive analysis tool.

The final comments relate to the implementation of applications with artificial intelligence implemented. With the development of Industry 4.0 tools, the trend towards digitalisation with artificial intelligence is popular. This is justified on the grounds of speed of reporting, access to all data, etc. And these advantages are difficult or impossible to refute. Unfortunately, once implemented, some of these applications do not deliver the expected results and profits and are even decommissioned or rejected by the customer. The reasons for this can be found firstly in the inability to meet customer and user expectations. In addition, the author noted that the level of ergonomics of the application and the level at which artificial intelligence interacts with the user have a significant impact.

The interaction levels of human – software (equipped with which artificial intelligence) are presented below:

1. Artificial intelligence requires continuous human interaction throughout the process. It requires the human to have expert knowledge. Generates a lot of unnecessary data for personnel;
2. Artificial intelligence requires interaction to enter data at the initial stage or and select a result from several scenarios obtained. Requires advanced knowledge. Generates a small amount of unnecessary data;
3. Artificial intelligence requires interaction only when getting the results, the first time, requires basic knowledge, as commissioning what can be done by an external specialist, generates no unnecessary data;
4. Artificial intelligence does not require human interaction to obtain a result. Lacks necessary knowledge, does not generate unnecessary data.

Implementing nowadays applications in industrial plants at maintenance or production levels with less than level 2 is, according to the author, subject to a high risk of being unsuccessful. This is due to additional time-consuming activities, human habits and perception, the ambiguity of the results (the fallibility of intelligent systems) and the need for additional skills

REFERENCES

1. Aghenta, E.A.: Mitigating risks associated with Lockout/Tagout (LOTO) of hazardous energy in Nigeria: a tracker approach. North-West University (2012).
2. Agrawal, R., Srikat, R.: Fast Algorithms for Mining Association Rules in Datamining. Proc. 20th int. conf. very large data bases, VLDB. 1215, 487–499 (1994).
3. Åkerman, M.: Implementing Shop Floor IT for Industry 4.0, https://www.researchgate.net/figure/The-automation-pyramid-according-to-the-ISA-95-model-The-five-levels-0-5-are-defined_fig2_326224890, last accessed 2019/01/27.
4. ANSI/ISA-95: Enterprise-Control System Integration. International Society of Automation (1995).
5. ATA MSG-3: Operator/Manufacturer Scheduled Maintenance Development. Air Transport Association of America, Inc. (2003).
6. Bagiński, J.: Zarządzanie jakością. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa (2004).
7. Baptista, M. et al.: Forecasting fault events for predictive maintenance using data-driven techniques and ARMA modeling. Computers & Industrial Engineering. 115, 41–53 (2018). https://doi.org/10.1016/j.cie.2017.10.033.
8. Barringer, H.P.: A Life Cycle Cost Summary. , Perth, Australia (2003).
9. Barringer, H.P.: Predict failures. Presented at the International Mechanical Engineering Conference , Kuwait (2004).
10. Batchkova, I.A., Gocheva, D.G.: IEC-62264 based quality operations management according the principles of industrial internet of things. Scientific proceedings XiV International Congress "'Machines, Technologies, Materials.'" I, VI, 431–434 (2017).
11. Bell, J., Holroyd, J.: Review of human reliability assessment methods, RR679. Health and Safety Executive. (2009).
12. Berry, M.J.A., Linof, G.S.: Data Mining Techniques: For Marketing, Sales, and Customer Relationship Management, 2nd Edition. Wiley Publishing Inc., Indianapolis, Indiana (2004).
13. Bertolini, M. et al. eds: Multi-attribute approaches for maintenance policies selection problem. Presented at the Advances in safety and reliability: proceedings of the European Safety and Reliability Conference (ESREL 2005), Tri City (Gdynia - Sopot - Gdansk), Poland, 27 - 30 June, 2005 , Leiden (2005).
14. Bevilacqua, M., Braglia, M.: The analytic hierarchy process applied to maintenance strategy selection. Reliability Engineering & System Safety. 70, 1, 71–83 (2000).
15. Bicheno, J.: Cause and Effect Lean. Production and Inventory Control, Systems and Industrial engineering books, Buckingham (2000).
16. Bicheno, J.: The Lean Toolbox. Production and Inventory Control, Systems and Industrial engineering books, Buckingham (2000).
17. Birolini, A.: Reliability Engineering: Theory and Practice. Springer Berlin Heidelberg, Berlin, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54209-5.
18. Blazewicz, J. et al.: Handbook on Data Management in Information Systems. Springer-Verlag Berlin Heidelberg, Berlin (2003).

19. Briš, R. et al. eds: Maintenance optimization of a common simple distribution system. Presented at the Advances in safety and reliability: proceedings of the European Safety and Reliability Conference (ESREL 2005), Tri City (Gdynia - Sopot - Gdansk), Poland, 27 - 30 June, 2005 , Leiden (2005).
20. BS EN 15341-2007: Maintenance Maintenance key performance indicators, (2007).
21. Bukowski, J.V., Stewart, L.: Explaining the Differences in Mechanical Failure Rates:, https://www.exida.com/articles/FMEDAvsOREDA_Sept142015.pdf.
22. Campbell, J.D.: UPTIME: Strategies for Excellence in Maintenance Management. Taylor & Francis (2006).
23. Camus, D., Großbritannien eds: The ONS productivity handbook: a statistical overview and guide. Palgrave Macmillan, Basingstoke, Hampshire (2007).
24. Carannante, T.: The introduction and implementation of TPM using a conceptual model developed in-house – phase I. Maintenance & Asset Management. Volume 18, No 5/6, (2003).
25. Carnero Moya, M.C.: The control of the setting up of a predictive maintenance programme using a system of indicators. Omega. 32, 1, 57–75 (2004). https://doi.org/10.1016/j.omega.2003.09.009.
26. Center for chemical process safety: Guidelines for Preventing Human Error in Process Safety. American Institute of Chemical Engineers, New York (2004).
27. Chaudhuri, D., Suresh, P.V.: An algorithm for maintenance and replacement policy using fuzzy set theory. Reliability Engineering and System Safety. 50, 79–86 (1995).
28. Ciesielski, A.: Introduction to Rubber Technology. Rapra Technology Limited, Southampton (1999).
29. Dasic, P. et al.: Models of Reliability for Cutting Tools: Examples in Manufacturing and Agricultural Engineering. Journal of Mechanical Engineering. 10 (2008).
30. Deshpande, V.S., Modak, J.P.: Application of RCM to a medium scale industry. Reliability Engineering & System Safety. 77, 1, 31–43 (2002).
31. DIN SPEC 91345:2016-04: Referenzarchitekturmodell Industrie 4.0. Beuth Verlag, Berlin (2016).
32. Downarowicz, O.: System eksploatacji, Zarządzanie zasobami techniki. Wydawnictwo Instytutu Technologii Eksploatacji-PIB, Gdańsk (2005).
33. Dunn, A.: Assuring Quality in Maintenance. In: Engineering Asset Management. pp. 1156–1164 Springer, London (2006). https://doi.org/10.1007/978-1-84628-814-2_126.
34. Dunn, S.: Managing Human Error in Maintenance. Maintenance & Asset Management. 20, 4, 18 (2006).
35. Dźwiarek, M.: Bezpieczeństwo funkcjonalne systemów sterowania. Centralny Instytut Ochrony Pracy - Panst. Instytut Badawczy, Warszawa (2012).
36. Dźwiarek, M.: Performance Level Validation of the Machinery Control System / Walidacja Poziomu Zapewnienia Bezpieczeństwa Przez Systemy Sterowania Maszynami. Journal of KONBiN. 33, 1, 29–40 (2015). https://doi.org/10.1515/jok-2015-0003.
37. EN 60300-3-11:2009: Dependability management. Application guide. Reliability centred maintenance, (2009).
38. EN ISO 9000-2015: Quality management systems — Fundamentals and vocabulary, (2015).
39. EN ISO 14119:2013: Safety of machinery - interlocking devices associated with guards - Principles for design and selection, (2014).

40. Fernandez, O. et al.: A decision support maintenance management system development and implementation. International Journal of Quality and Reliability Management. 20, 8, 965–979 (2003).
41. Gilsinn, J.D., Schierholz, R.: Security Assurance Levels: A Vector Approach to Describing Security Requirements. National Institute of Standards and Technology,. 13 (2010).
42. Goerdeler, D.A.: Germany's Digital Agenda and the Role of Standardization. Presented at the OMG Model-Based Engineering in PLM and Manufacturing Information Day , Berlin June 18 (2015).
43. Gram, M.: A systematic methodology to reduce losses in production with the balanced scorecard approach. Manufacturing Science and Technolog. 2, 12–22 (2013). https://doi.org/10.13189/mst.2013.010103.
44. Guo, H. et al.: On determining optimal inspection interval for minimizing maintenance cost. In: 2015 Annual Reliability and Maintainability Symposium (RAMS). pp. 1–7 (2015). https://doi.org/10.1109/RAMS.2015.7105163.
45. Habrekke, S. et al.: Guideline for follow-up of Safety Instrumented Systems (SIS) in the operating phase. SINTEF, Trondheim, Norway (2021).
46. Han, J. et al.: Mining Frequent Patterns without Candidate Generation: A Frequent-Pattern Tree Approach. Data Mining and Knowledge Discovery. 8, 1, 53–87 (2004). https://doi.org/10.1023/B:DAMI.0000005258.31418.83.
47. Harańczyk, G.: Modelowanie czasu trwania - model proporcjonalnego hazardu Coxa. StatSoft Polska Sp. z o.o., Kraków (2011).
48. Hauge, S., Onshus, T.: Reliability data for safety instrumented systems PDS data handbook 2010 Edition, (2009).
49. Health and Safety Executive: Statistics, http://www.hse.gov.uk/.
50. HF mixing group: Schema of rubber production line, http://www.hf-mixing-group.com, last accessed 2011/05/06.
51. Hipkin, I.B., De Cock, C.: TQM and BPR: lessons for maintenance management. Omega. 28, 3, 277–292 (2000).
52. HSE: Introduction to rubber processing and safety issues. Health and Safety Executive, Bootle (2013).
53. HSE: Principles for proof testing of safety instrumented systems in the chemical industry, (2002).
54. Huang, L. et al.: Discussion on application of reliability-centered maintenance to reliability improvement in new nuclear power plants. In: Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE), 2013 International Conference on. pp. 707–711 IEEE (2013).
55. IEC 60050-192-2015: International electrotechnical vocabulary - Part 192: Dependability, (2015).
56. IEC 61508 1-7:2005-2016: Functional safety of electrical/ electronic/programmable electronic safety-related systems. International Electrotechnical Commission. (2016).
57. IEC 62061: Safety of machinery - Functional safety of safety-related control systems. (2021).
58. IEC 62264-1:2013: Enterprise-control system integration - Part 1: Models and terminology, (2013).
59. IEC 62443-x: Security for industrial automation and control systems. Parts 1-13 (undergoing development), (2011).

60. IEC TR 63074: Safety of machinery - Security aspects related to functional safety of safety-related control systems, (2019).
61. ISO 9001:2015-10: Systemy zarządzania jakością -- Wymagania. International Organization for Standardization. (2015).
62. ISO 12100:2010: Safety of machinery - General principles for design - Risk assessment and risk reduction. International Organization for Standardization. (2010).
63. ISO 13849-1:2015: Safety of machinery - Safety-related parts of control systems. International Organization for Standardization. (2015).
64. ISO 14001:2015: ISO 14001:2015 Environmental management systems — Requirements with guidance for use. (2015).
65. ISO 14118:2017: Safety of machinery — Prevention of unexpected start-up, (2017).
66. ISO 14224-2016: Petroleum, petrochemical and natural gas industries - Collection and exchange of reliability and maintenance data for equipment, (2016).
67. ISO 15288:2015: Systems and softwareengineering - System life cycle processes, (2015).
68. ISO 22301:2012: Societal security - Business continuity management systems - Requirements. (2012).
69. ISO 22400-1-2014: Automation systems and integration - Key performance indicators (KPI's) for manufacturing operations management - Part 1:Overview, concepts and terminology.
70. ISO 27001:2013: ISO 27001:2013 Information technology-Security techniques-Information security management systems-Requirements. (2013).
71. ISO 31000: Risk management – Principles and guidelines. (2018).
72. ISO 45001:2018: Occupational health and safety management systems — Requirements with guidance for use. 52 (2018).
73. ISO Guide 73: ISO Guide 73:2009 Risk management — Vocabulary, (2009).
74. ISO IEC IEEE 24765: Systems and software engineering - Vocabulary, (2017).
75. ISO IEC 31010:2009: Risk management - Risk assessment techniques, (2009).
76. ISO TR12489:2013: Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems, (2013).
77. James Chang, Y. et al.: The SACADA database for human reliability and human performance. Reliability Engineering & System Safety. 125, 117–133 (2014). https://doi.org/10.1016/j.ress.2013.07.014.
78. Jovanovic, A.: Risk-based inspection and maintenance in power and process plants in Europe. Nuclear Engineering and Design. 226, 2, 165–182 (2003). https://doi.org/10.1016/j.nucengdes.2003.06.001.
79. Juran, J.M., Godfrey, A.B.: Juran's Quality Handbook. McGraw-Hill, New York (1999).
80. Kaplan, R.S., Norton, D.P.: The strategy-focused organization: how balanced scorecard companies thrive in the new business enviroment. Harvard University Press (2001).
81. Keliris, A. et al.: Enabling Multi-Layer Cyber-Security Assessment of Industrial Control Systems through Hardware-in-the-Loop Testbeds.
82. Kelly, T.P., McDermid, J.A.: A systematic approach to safety case maintenance. Reliability Engineering & System Safety. 71, 3, 271–284 (2001).
83. Kletz, T.A.: Hazop and Hazan: Identifying and Assessing Process Industry Hazards - Trevor A. Kletz - Google Książki, https://books.google.pl/books?hl=pl&lr=&id=m2u577x_6U4C&oi=fnd&pg=PR3&d

q=trevor+kletz+hazop+and+hazan&ots=xfDZL2wNnV&sig=sDpCtbg32NAdWc6A26BkZ1_BC0s&redir_esc=y#v=onepage&q=trevor%20kletz%20hazop%20and%20hazan&f=false, last accessed 2017/06/17.

84. Koch, T.: Jak stosować metody Lean manufacturing (Oszczędnego Wytwarzania) do wprowadzania innowacji. Presented at the E-narzędzia i technologie generatywne jako szybka ścieżka do innowacji , Warszawa May 5 (2011).

85. Kosmowski, K.T. et al.: Czynniki ludzkie w analizie bezpieczeństwa funkcjonalnego. Presented at the Materiały konferencji naukowo-technicznej Jurata 16-18.IX. 2004 , Gdańsk September 16 (2004).

86. Kosmowski, K.T.: Functional safety and reliability analysis methodology for hazrdous industrial plants. Gdansk University of technology Publishers, Gdańsk (2013).

87. Kosmowski, K.T.: Incorporation of human and organizational factors into qualitative and quantitative risk analyses. Presented at the Proceedings of the International Conference (ESREL'04 and PSAM 7) on Probabilistic Safety Assessment and Management , London (2004).

88. Kosmowski K.T. et al.: Integrated Functional Safety and Cybersecurity analysis method for Smart Manufacturing Systems. TASK Quarterly. (2019).

89. Kosmowski, K.T. et al.: Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Business Continuity Management. Energies. 15, 10, 3610 (2022). https://doi.org/10.3390/en15103610.

90. Kosmowski, K.T.: Podstawy bezpieczeństwa funkcjonalnego. Wydawnictwo Politechniki Gdańskiej, Gdańsk (2015).

91. Kosmowski, K.T. et al.: Wybrane metody przydatne w analizie niezawodności i bezpieczeństwa funkcjonalnego systemów technicznych. In: Zarządzanie Bezpieczeństwem Funkcjonalnym. pp. 363–377 Fundacja Rozwoju Uniwersytetu Gdańskiego, Jurata (2004).

92. Kosmowski, K.T., Golebiewski, D.: Functional safety and cyber security analysis for life cycle management of industrial control systems in hazardous plants and oil port critical infrastructure including insurance. Interreg Baltic Sea Region, HAZARD Report. (2019).

93. Kosmowski, K.T., Piesik, J.: Functional safety and maintenance management taking into consideration human and organization factors. Functional Safety Management in Critical Systems. 209–227 (2007).

94. Kosmowski, K.T., Piesik, J.: Methodological and practical aspects of maintenance planning in Hazardous Systems. In: Proceedings of the European Safety and Reliability Conference, ESREL 2005, Tri City, Poland, 27-30 June 2005. Taylor&Francis Group, Tricity (2005).

95. Kosmowski, K.T., Śliwiński, M.: Organizational culture as prerequisite of proactive safety and security management in critical infrastructure systems including hazardous plants and ports. Behaviour-based safety, organizational culture, proactive safety and security management. (2016).

96. Kumar, U. et al.: Maintenance performance metrics: a state-of-the-art review. Journal of Quality in Maintenance Engineering. 19, 3, 233–277 (2013). https://doi.org/10.1108/JQME-05-2013-0029.

97. Ladkin, P.B.: An Overview of IEC 61508 on E/E/PE Functional Safety. (2008).

98. Lapa, C.M.F. et al.: A model for preventive maintenance planning by genetic algorithms based in cost and reliability. Reliability Engineering & System Safety. 91, 2, 233–240 (2006). https://doi.org/10.1016/j.ress.2005.01.004.
99. Larose, D.T.: Odkrywanie wiedzy z danych. Wprowadzenie do eksploracji danych. Wydawnictwo Naukowe PWN, Warszawa (2006).
100. Larose, D.T., Larose, C.D.: Data Mining and Predictive Analytics, 2nd Edition [Book]. John Wiley & Sons Inc. (2015).
101. Lasek, M., Pęczkowski, M.: Enterprise Miner. Wykorzystanie narzędzi Data Mining w systemie SAS Enterprise Miner. Wydawnictwa Uniwersytetu Warszawskiego, Warszawa (2013).
102. Lee, J. et al.: A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters. 3, 18–23 (2015). https://doi.org/10.1016/j.mfglet.2014.12.001.
103. Legutko, S.: Trendy rozwoju utrzymania ruchu urządzeń i maszyn. machines operation, maintenance, RCM, TPM. 2/2009, 8–16 (2009).
104. Leroux, M.: OEE as a performance KPI, https://new.abb.com/industrial-software/digital/oee-overall-equipment-effectiveness/oee-meaning---oee-as-a-performance-kpi, last accessed 2022/06/06.
105. Li, X. et al.: Research on Improved OEE Measurement Method Based on the Multiproduct Production System. Applied Sciences. 11, 2, 490 (2021). https://doi.org/10.3390/app11020490.
106. Lindberg, C.-F. et al.: Key Performance Indicators Improve Industrial Performance. Energy Procedia. 75, 1785–1790 (2015). https://doi.org/10.1016/j.egypro.2015.07.474.
107. Lu, L., Jiang, J.: Analysis of on-line maintenance strategies for k-out-of-n standby safety systems. Reliability Engineering and System Safety. 92, 144–155 (2007). https://doi.org/10.1016/j.ress.2005.11.012.
108. Lukens, S., Markham, M.: Data-driven Application of PHM to Asset Strategies. PHM_CONF. 10, 1, (2018). https://doi.org/10.36001/phmconf.2018.v10i1.245.
109. Luxhoj, J.T. et al.: Trends and Perspectives in Industrial Maintenance Mangement. Journal of Manufacturing Systems. 16, 6, 437–453 (1997).
110. Mathew, S.: Optimal inspection frequency: A tool for maintenance planning/forecasting. International Journal of Quality & Reliability Management. 21, 763–771 (2004). https://doi.org/10.1108/02656710410549109.
111. McKinsey Digital ed: Industry 4.0 How to navigate digitization of the manufacturing sector, (2015).
112. MIL-HDB-217F: Reliability Prediction of electronic Equipment. Department of the Defense United States of America. (1991).
113. MIL-P-24534A: Military Specification, Planned Maintenance System: Development of Maintenance Requirement Cards, Maintenance Index Pages, and Associated Documentation. Department of the Defense United States of America. (1985).
114. MIL-STD-756B: Reliability Modelling and Prediction. Department of the Defense United States of America. (1981).
115. MIL-STD-1472F: Design Criteria Standard Human Engineering. Department of the Defense United States of America. (1999).
116. MIL-STD-2173(AS): Reliability-Centered Maintenance Requirements for Naval Aircraft, Weapons systems and Support Equipment. Department of the Defense United States of America. (1986).

117. Minister Gospodarki: Rozporządzenie Ministra Gospodarki z dnia 15 października 2001 r. w sprawie bezpieczeństwa i higieny pracy przy produkcji wyrobów gumowych. Dziennik Ustaw. (2001).
118. Morzy, T.: Eksploracja danych. Wydawnictwo Naukowe PWN, Warszawa (2013).
119. Mühlenbein, H.: Artificial Intelligence and Neural Networks The Legacy of Alan Turing and John von Neumann. omputational Intelligence. Intelligent Systems Reference Library. (2006). https://doi.org/10.1007/978-3-642-01799-5_2.
120. NASA: Recommended Techniques for Effective Maintainability. National Aeronautics and Space Administration, Washington (1994).
121. Nguyen, T.T.: A Compact FP-tree for Fast Frequent Pattern Retrieval. 10 (2013).
122. Niven, P.R.: Balanced Scorecard Step-by-Step, Maximizing Performance and Maintaining Results. John Wiley & Sons, Inc., Hoboken, New Jersey. (2006).
123. Noroozi, A. et al.: Determination of human error probabilities in maintenance procedures of a pump. Process Safety and Environmental Protection. 92, 2, 131–141 (2014). https://doi.org/10.1016/j.psep.2012.11.003.
124. Noroozi, A. et al.: The role of human error in risk analysis: Application to pre- and post-maintenance procedures of process facilities. Reliability Engineering & System Safety. 119, 251–258 (2013). https://doi.org/10.1016/j.ress.2013.06.038.
125. Norsk olje og gass: 070 - Norwegian oil and gas application of IEC61508 and IEC 61511 in the Norwegian Petroleum Industry. (2004).
126. Nowlan, S.F., Heap, H.F.: Reliability-Centred Maintenance. Report AD/A066-579. U.S Department of Commerce, Springfield, Virginia (1978).
127. Nyman, D.: The 15 Most Common Obstacles to World-class Reliability: A Roadmap for Managers. Industrial Press Inc. (2009).
128. Ohno, T.: The Toyota Production System. Toyota Motor Corporation, International Public Affairs. Productivity Press. (1998).
129. OSHA, US DoL: Commonly Used Statistics, https://www.osha.gov/oshstats/commonstats.html, last accessed 2017/05/01.
130. Pamphlet 750–40: Guide to Reliability Centered Maintenance (RCM) for Fielded Equipment. Department of the Defense United States of America. (1982).
131. Pedregal, D.J. et al.: RCM2 predictive maintenance of railway systems based on unobserved components models. Reliability Engineering & System Safety. 83, 1, 103–110 (2004). https://doi.org/10.1016/j.ress.2003.09.020.
132. Piesik, J.: Metoda zarządzania niezawodnością i procesami obsługi linii produkcyjnej wspomagana statystyczną analizą danych. Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej. 51, 151–154 (2016).
133. Piesik, J. et al.: Wspomagane Komputerowo tworzenie modeli probabilistycznych w ocenie niezawodności i bezpieczeństwa przykładowych systemów. Presented at the Materiały konferencji naukowo-technicznej Jurata 16-18.IX. 2004 , Jurata September 16 (2004).
134. Piesik, J.: Zastosowanie narzędzi statystycznych do poprawy niezawodności i bezpieczeństwa maszyn poprzez predykcję awarii oraz poprawę pokrycia diagnostycznego maszyn. Zastosowanie statystyki i data mining w badaniach naukowych oraz doskonalenie procesów produkcyjnych z wykorzystaniem analizy danych. 191–203 (2015).
135. Piesik, J., Kosmowski, K.T.: Aktualne problemy zarządzania niezawodnością i bezpieczeństwem linii produkcyjnej. Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej. (2016).

136. Piesik, J., Kosmowski, K.T.: Complex Predictive Solution for Computerized Processes in Tire Industry. In: Ahram, T. et al. (eds.) Human Interaction and Emerging Technologies. pp. 812–817 Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-25629-6_127.
137. PN-EN 13306:2010: Obsługiwanie - Terminologia dotycząca obsługiwania Maintenance - Maintenance terminology. Polski Komitet Normalizacyjny. (2010).
138. PN-EN ISO 9001:2015: Systemy zarządzania jakością- Wymagania. Polski Komitet Normalizacyjny. (2015).
139. Popescu, D.E. et al.: Monte Carlo Simulation using Excel for Predicting Reliability of a Geothermal Plant. Presented at the International Geothermal Conference , Reykjavik September (2003).
140. Rausand, M.: Reliability centered maintenance. Reliability Engineering and System Safety. 60, 121–132 (1998).
141. Rausand, M.: Reliability of Safety-Critical Systems. Wiley Publishing Inc., Hoboken, New Jersey (2014).
142. Rausand, M., Høyland, A.: System reliability theory: models, statistical methods, and applications. Wiley-Interscience, Hoboken, NJ (2004).
143. Reynolds, P.: Benchmarking OEE. Packaging Controls&Automation. September 2010, 68–73 (2010).
144. Rockwell Automation: Functional levels of a DCS, www.rockwellautomation.com, (2016).
145. Ross, J.E.: Total Quality Management, Text, Cases and Readings. Kogan Limited, London (1994).
146. Rostianingsih, S. et al.: Hybrid-dimension association rules for diseases track record analysis at Dr. Soetomo General Hospital. In: 2011 International Conference on Uncertainty Reasoning and Knowledge Engineering. pp. 189–191 IEEE, Bali, Indonesia (2011). https://doi.org/10.1109/URKE.2011.6007854.
147. Ruthotto, L., Haber, E.: Deep Neural Networks motivated by Partial Differential Equations. arXiv preprint arXiv:1804.04272. (2018).
148. Sage Clarity: 2017 OEE Benchmark Study, https://sageclarity.com/articles/2017-oee-benchmark-study/, last accessed 2018/06/11.
149. Sammut-Bonnici, T., Russell, R.: Balanced Scorecard. Wiley Encyclopedia of Management.
150. Schönbeck, M. et al.: Human and organisational factors in the operational phase of safety instrumented systems: A new approach. Safety Science. 48, 3, 310–318 (2010). https://doi.org/10.1016/j.ssci.2009.11.005.
151. Shappell, S.A., Wiegmann, D.A.: The Human Factors Analysis and Classification System - HFACS. U.S. Department of Transportation, Springfield (2000).
152. Shirose, K.: TPM Team Guide. Productivity Press, Portland, Oregon (1995).
153. SINTEF: Handbook on Design and Operation of Flexible Pipes, http://www.sintef.no/en/ocean/handbook-on-design-and-operation-of-flexible-pipes/, (2010).
154. Sittithumwat, A. et al.: Optimal allocation of distribution maintenance resources with limited information. Electric Power Systems Research. 68, 3, 208–220 (2004). https://doi.org/10.1016/j.epsr.2003.07.001.
155. Śliwiński, M. et al.: Integrated functional safety and cyber security analysis. IFAC-PapersOnLine. (2018).

156. Soumya, S.B., Deepika, N.: Data Mining With Predictive Analytics for Financial Applications. International Journal of Scientific Engineering and Applied Science (IJSEAS). 2, 310–317 (2016).
157. Suh, S.: Practical Applications of Data Mining. Jones & Bartlett Publishers (2012).
158. Suzuki, T.: TPM in process Industries. Productivity Press, Potland, Oregon (1994).
159. Tchórzewska-Cieślak, B.: Niezawodność i bezpieczeństwo systemów komunalnych na przykładzie systemu zaopatrzenia w wodę. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów (2008).
160. The Japan Institute of Plant Maintenance: Focused Equipment Improvement for TPM Teams. Productivity Press, Potland, Oregon (1997).
161. The Japan Institute of Plant Maintenance: OEE for Operators, Overall Equipment Effectiveness. Productivity Press, Potland, Oregon (1999).
162. The Japan Institute of Plant Maintenance: TPM for Every operator. Productivity Press, Potland, Oregon (1996).
163. Toyo Tires: Tire production processes presentation, www.toyotires.com.
164. Tu, P.Y.L. et al.: An Integrated Maintenance Management System for an Advanced Manufacturing Company. The International Journal of Advanced Manufacturing Technology. 17, 692–703 (2001).
165. Turner, S.: Maintenance Analysis of the Future. International Conference of Maintenance Societies Melbourne, Melbourne 2001. (2001).
166. US NSSC: Reliability Centered Maintenance (RCM) Handbook S9081-AB-GIB-010. Naval Sea Command (2007).
167. Van Noortwijk, J.M. et al.: Expert judgment in maintenance optimization. IEEE Transactions on reliability. 41, 3, 427–432 (1992).
168. Vatn, J. et al.: An overall model for maintenance optimization. Reliability Engineering and System Safety. 51, 241–257 (1996).
169. Vaurio, J.K.: A note of optimal inspection intervals. ", International Journal of Quality and Reliability Management. 11, 65–68 (1994).
170. Verma, A.K. et al.: Reliability and Safety Engineering. Springer London, London (2010). https://doi.org/10.1007/978-1-84996-232-2.
171. Wang, W.: An overview of the recent advances in delay-time-based maintenance modelling. Reliability Engineering & System Safety. 106, 165–178 (2012). https://doi.org/10.1016/j.ress.2012.04.004.
172. Winzenick, M.: Safety of Machinery, Notes on the application of standards EN620611 and EN ISO 13849-1. German Electrical and Electronic Manufacturer's Association, Frankfurt am Main (2012).
173. Wireman, T.: Developing Performance Indicators for Managing Maintenance. Industrial Press Inc., New York (1998).
174. Wojciechowski, M., Zakrzewicz, M.: Dataset Filtering Techniques in Constraint-Based Frequent Pattern Mining. Pattern Detection and Discovery. Lecture Notes in Computer Science, vol 2447. 77–91 (2002). https://doi.org/10.1007/3-540-45728-3_7.
175. Wu, S., Clements-Croome, D.: Preventive maintenance models with random maintenance quality. Reliability Engineering & System Safety. 90, 1, 99–105 (2005). https://doi.org/10.1016/j.ress.2005.03.012.
176. Xia, T. et al.: Dynamic maintenance decision-making for series–parallel manufacturing system based on MAM–MTW methodology. European Journal of Operational Research. 221, 1, 231–240 (2012). https://doi.org/10.1016/j.ejor.2012.03.027.

177. Yi, M. et al.: Benchmarking Cloud-Based SCADA System. In: 2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). pp. 122–129 IEEE, Hong Kong (2017). https://doi.org/10.1109/CloudCom.2017.25.
178. Z-016: Regularity Management & Reliability Technology. Norsok Standard. (1998).
179. Zawiła-Niedźwiecki, J.: Zarządzanie ryzykiem operacyjnym. edu-Libri, Kraków-Warszawa (2013).
180. Zezulka, F. et al.: Industry 4.0 – An Introduction in the phenomenon. IFAC-PapersOnLine. 49, 25, 8–12 (2016). https://doi.org/10.1016/j.ifacol.2016.12.002.
181. Zhao, Z. et al.: Predictive maintenance policy based on process data. Chemometrics and Intelligent Laboratory Systems. 103, 2, 137–143 (2010). https://doi.org/10.1016/j.chemolab.2010.06.009.
182. Zio, E., Compare, M.: Evaluating maintenance policies by quantitative modeling and analysis. Reliability Engineering and System Safety. 109, 53–65 (2013).
183. breakdown | Definition of breakdown in English by Oxford Dictionaries, https://en.oxforddictionaries.com/definition/breakdown, last accessed 2019/01/26.
184. IEC 60050 - International Electrotechnical Vocabulary - Details for IEV number 192-03-01: “failure,” https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=192-03-01, last accessed 2022/06/11.
185. Implementation of International Safety Standard EN ISO 13849 into Machinery of Tyre Industry, https://www.researchgate.net/publication/323095170_Implementation_of_International_Safety_Standard_EN_ISO_13849_into_Machinery_of_Tyre_Industry, last accessed 2020/08/16.
186. Przemysł 4.0 w praktyce - Produkcja zgodnie z Industry 4.0, https://www.copadata.com/pl/przemyslowa/smart-factory-inteligentna-fabryka/smart-factory-insights/przemysl-40-w-praktyce-produkcja-zgodnie-z-industry-40/smart-factory-23/, last accessed 2021/05/28.
187. www.cloud.google.com.

Appendix 1 Definitions

Some definitions and abbreviations are presented below with the intention to facilitate the understanding of the content in the thesis.

Availability (performance) - Ability of an item to be in a state to perform a required function under given conditions at a given instant of time during a given time interval, assuming that the required external resources are provided. Note – This ability depends on the combined aspects of reliability, maintainability and maintenance supportability [137].

Breakdown – Synonym of failure [183].

Corrective maintenance - Maintenance carried out after fault recognition and intended to put an item into a state I in which it can perform a required function [137].

Defect - A defect is a type of nonconformity. It occurs when a product or service fails to meet specified or intended use requirements [38] [74].

Failure - The termination of its ability to perform a required function [142], loss of ability to perform as required [55].

Failure mode – One of the possible states of a faulty item, for a given required function [141].

Fault - The state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources [141].

Machine / machinery – assembly, fitted with or intended to be fitted with a drive system consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application (the term „machinery" also covers an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole) [62].

Machine control system – system that responds to input signals from the machinery and/or from an operator and generates output signals causing the machinery to operate in the desired manner [57].

Maintainability - Ability of an item under given conditions of use, to be retained in or restored to, a state in which it can perform a required function when maintenance is performed under given conditions and using stated procedures and resources [137].

Maintenance - Combination of all technical, administrative and managerial actions during the lifecycle of an item intended to retain it, or restore it to, a state in which it can perform the required function [137].

Maintenance management - All activities of the management that determine the maintenance objectives, strategies, and responsibilities and implement them by means such as maintenance planning, maintenance control and supervision, improvement of methods of the organisation including economic aspects [137].

Maintenance programme - Methods, procedures and resources required to sustain in support of an item throughout its life cycle [37].

Maintenance supportability - Ability of a maintenance organisation of having the right maintenance support at the necessary place to perform the required maintenance activity at a given instant of time or during a given time interval [137].

Preventive maintenance - Maintenance carried out at predetermined intervals or according to prescribed criteria and intended to reduce the probability of failure or the degradation of the functioning of an item [137].

Productivity - the rate at which a company or country makes goods, usually judged in connection with the number of people and the amount of materials necessary to produce the goods [23]

Reliability - Ability of an item to perform a required function under given conditions for a given time interval [137].

Risk - Combination of the frequency, or probability, of occurrence and the consequence of a specified hazardous event [37].

Risk management - Systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risk [37].

System – A combination of interacting elements organized to achieve one or more stated purposes [67].

Safety – freedom from unacceptable risk [57]

Functional safety – part of the overall safety of the machine and the machine control system that depends on the correct functioning of the safety-related control system and other risk reduction measures [57]

Total Productive Maintenance (TPM) - A method for improved machine availability through better utilisation of maintenance and production resources [160].

Total Quality Management (TQM) - is the integration of all functions and processes within an organisation to achieve continuous improvement of the quality of goods and services [145].

Validation – confirmation by examination and provision of objective evidence that the particular requirements for specific intended use are fulfilled [56].

Verification - confirmation by examination and provision of objective evidence that the requirements have been fulfilled [56].

Appendix 2. PFH calculations for analysed safety architectures with HFT=1 and SIL=1

B.1. Sources of reliability data

The reliability data for the calculations were taken from the SINTEF PDS Data Handbook 2010 Edition Table B.1.

Table B.1 Reliability data adopted from the SINTEF PDS Data Handbook

Component group	λ_{DU}	λ_{DD}	λ_{D}	β	S_{FF}	MTTR	PTC
Input devices	$3\cdot10^{-6}$	$0.5\cdot10^{-6}$	$3.5\cdot10^{-6}$	0.06	47%	8	50
Control logic units	$0.48\cdot10^{-6}$	$4.32\cdot10^{-6}$	$4.8\cdot10^{-6}$	0.07	80%	8	90
Final elements	$3.5\cdot10^{-6}$	$0.9\cdot10^{-5}$	$4.4\cdot10^{-6}$	0.1	49%	8	40

B.2. Calculation according to IEC 61508 standard

a) The calculation for architecture 1oo2

$$PFH \cong 2\cdot((1-\beta_D)\cdot\lambda_{DD}+(1-\beta)\cdot\lambda_{DU})\cdot(1-\beta)\cdot\lambda_{DU}\cdot t_{CE}+\beta\cdot\lambda_{DU} \tag{B.1}$$

$$t_{CE}=\frac{\lambda_{DU}}{\lambda_D}\cdot\left(\frac{T_1}{2}+MRT\right)+\frac{\lambda_{DD}}{\lambda_D}\cdot MTTR \tag{B.2}$$

$$PFH_S \cong 2.5\cdot10^{-7}h^{-1}$$
$$PFH_L \cong 3.38\cdot10^{-9}h^{-1}$$
$$PFH_{FE} \cong 4.37\cdot10^{-7}h^{-1}$$
$$PFH_{SYS} \cong 6.9\cdot10^{-7}h^{-1}$$

B.3. Calculation according to IEC 62061 standard

b) The calculation for architecture type B

$$PFH_S \cong \left[(1-\beta)^2\cdot\lambda_{De1}\cdot\lambda_{De2}\cdot T_1+\beta\cdot\frac{(\lambda_{De1}+\lambda_{De2})}{2}\right]=$$

$$\left[(1-0.06)^2\cdot3.5\cdot10^{-6}\cdot3.5\cdot10^{-6}\cdot8760+0.06\cdot\frac{(3.5\cdot10^{-6}+3.5\cdot10^{-6})}{2}\right]=3.05\cdot10^{-7}$$

$PFH_S \cong\ 3.05 \cdot 10^{-7} h^{-1}$
$PFH_L \cong\ 5.10 \cdot 10^{-7} h^{-1}$
$PFH_O \cong\ 4.36 \cdot 10^{-7} h^{-1}$

$$PFH_{SCS} = PFH_S + PFH_L + PFH_O \tag{B.9}$$

$$PFH_{SCS} = 1.25 \cdot 10^{-6}\ [h^{-1}]$$

c) The calculation for architecture type D

$$PFH_S \cong \left\langle (1-\beta)^2 \cdot \left\{ [\lambda_{De}^2 \cdot 2 \cdot DC] \cdot \frac{T_2}{2} + [\lambda_{De}^2 \cdot (1-DC)] \cdot T_1 \right\} + \beta \cdot \lambda_{De} \right\rangle =$$
$$\left\langle (1-0.06)^2 \cdot \left\{ [\left(3.5 \cdot 10^{-6}\right)^2 \cdot 2 \cdot 0.47] \cdot \frac{1}{2} + \left[\left(3.5 \cdot 10^{-6}\right)^2 \cdot (1-0.47)\right] \cdot 8760 \right\} + 0.06 \cdot 3.5 \cdot 10^{-6} \right\rangle =$$
$$2.60 \cdot 10^{-7}$$

$PFH_S \cong\ 2.60 \cdot 10^{-7} h^{-1}$
$PFH_L \cong\ 3.39 \cdot 10^{-8} h^{-1}$
$PFH_O \cong\ 5.10 \cdot 10^{-7} h^{-1}$

$$PFH_{SCS} \cong PFH_S + PFH_L + PFH_O$$

$$PFH_{SCS} \cong 8.04 \cdot 10^{-7}\ [h^{-1}]$$

Appendix 3. Maintenance KPI- examples

Below are presented chosen most common maintenance KPI indicators from standard BS - 15341:2007 based on author experience:

Table C.1. Chosen key Performance indicators for maintenance department [20]

Indicator	Definition	Comments
Technical Indicators		
T1	$\frac{\sum PW_t}{\sum PW_t + \sum D_t} \cdot 100$	Availability of machines
T8	$\frac{\sum PM_t}{\sum D_t} \cdot 100$	Ratio of preventive time causing downtime to total downtime related to maintenance
T17	$\frac{\sum PW_t}{\sum F_n}$	Mean Time Between Failures (MTBF)

Indicator	Definition	Comments
Technical Indicators		
T21	$\frac{\sum TR_t}{\sum F_n}$	Mean Time to Repair (MTTR)
O1	$\frac{\sum SM_n}{\sum S_n} \cdot 100$	Ratio of the sum of the number of maintenance personnel to the sum of the total number of staff
O18	$\frac{\sum PM_n}{\sum MT_m} \cdot 100$	Ratio of preventive maintenance man-hours to total maintenance man-hours

where:

W_t	– work time [h]
F_n	– number of failures [number]
D_t	– downtime due to maintenance [h]
MT_m	– maintenance man-hours [h]
PM_n	– preventive maintenance man-hours [h]
PM_t	–preventive time causing downtime [h]
PW_t	– operating time [h]
SM_n	– number of maintenance labour [number]
S_n	– number of internal employees [number]
TR_t	– time to restoration [h]

Appendix 4. Description of chosen methods of prediction

D.1. Association rule search algorithms

In 1993, the first algorithm to find strong association rules was presented. It used relational operators in the rule discovery process. A year later, R. Agrawal and R. Srikant presented two completely new algorithms: the Apriori algorithm and its extension AprioriTID [2]. They became a pillar of many new algorithms for detecting binary association rules. All algorithms searching for strong binary association rules have a certain common feature - the same general scheme of operation. Association rules that involve two or more dimensions or predicates can be referred to as multidimensional association rules. Rather than searching for frequent itemsets (as is done in mining single-dimensional association rules), in multidimensional association rules, we search for frequent predicate sets. In general, there are two types of multidimensional association rules, namely interdimension association rules and hybrid-dimension association rules. Interdimension association rules are multidimensional association rules with no repeated predicates. Hybrid dimension association rules are a multidimensional association rule that allows the repetition of the predicate on each of the rules [146].

D.1.1. Apriori algorithm

The Apriori algorithm consists of two basic stages (after setting minimum support and confidence values, i.e. *minSupp* and *minConf* parameters). These two steps are [99] [157] :
1) generating frequent sets based on the *minSupp* parameter,
2) based on the created frequent sets building rules with more confidence than *minConf.*
More substantial and difficult than step two is step one - generating all frequent sets. In the definition of a frequent set, it is not necessary to specify which elements belong to the predecessor and which belong to the successor of an association rule.

The Apriori algorithm is an iterative algorithm, i.e. it finds frequent sets of sizes {1, 2, ..., *k*} in successive steps. A data set should be lexicographed if it is not in the first step the algorithm should sort the set. In the beginning, the algorithm selects from a database or other data set, all one-piece sets and checks which one is a frequent set. In the next step, candidate itemsets are created on the basis of the frequent sets and their support in the whole database or data set is calculated for each of them. If the candidate's support is greater than or equal to the minimum support, the candidate is added to the list of frequent sets and in the next step will be taken into account when generating the candidate sets. In each subsequent step the algorithm shall be based on the frequent sets found in the previous step, it creates candidate sets with a size increased by 1. The algorithm stops working when no more candidate sets can be created. Fig. D.1 shows the Apriori algorithm.

```
$L_1$ = {frequent one-element data sets};
for (k = 2; $L_{k-1} \neq Ø$; $k$++) do
begin
        $C_k$ = apriori_gen($L_{k-1}$);
        for each transaction $t \in T$ do
        begin
                $C_t$ = subset ($C_k$,$t$);
                for each candidate dataset $c \in C_t$ do
                c.count++;
        end;
        $L_k$ = {$c \in C_k$ | c.count $\geq$ minsup}
end;
Result = $\cup_k L_k$;
```

Figure D.1. Apriori pseudo code [174] [18]

The following notation was used in the description of the algorithm: C_k means a family of candidate k-element sets, L_k means a family of frequent k-element sets, c.count means a counter counting the number of transactions supporting the set of element c, apriori_gen ( ) means a function that generates candidate sets, while subset ( ) means a function that for a given transaction t returns all candidate sets supported by t. As a first step, the algorithm counts the occurrences of all elements in database D in order to extract the frequent 1-element sets (L_1). Each subsequent k-th step of the algorithm consists of two phases. In the first, the apriori_gen ( ) function, based on the frequent sets belonging to $L\{k\text{-}1\}$, generates the candidate k-element sets (C_k). In the second phase of the k-th step, the database readout D is performed and for each candidate set c from the C_k set, the support for set c in the database D is calculated – Supp(c). In order to ensure that the procedure for calculating support for candidate sets is sufficiently efficient, the Apriori algorithm uses the data structure of the form hash tree, which is used to store candidate collections. Procedure subset( ) returns those candidate collections belonging to C_k that are supported by transaction t. If candidate set c meets the minimum support condition, that is, support(c)≥ minSupp, this set is added to the list of frequent sets. Otherwise, this set is removed from the list of candidate collections. The basic efficiency problems of the Apriori algorithm are two things: how to ensure the efficiency of the procedure for generating candidate collections, and how to ensure the efficiency of the procedure for calculating support for these crops. The first of these problems concerns the efficiency of the apriori_gen function ( ). The apriori_gen ( ) function is shown in diagram D.2.

```
function apriori_gen ($C_k$)
        insert into $C_k$
        select $p.item_1, p.item_2, ..., p.item_{k-1}, q.item_{k-1}$
        from $L_{k-1}\, p, L_{k-1}\, q$
        where $p.item_1 = q.item_1, ..., p.item_{k-2} = q.item_{k-2}, p.item_{k-1} < q.item_{k-1}$;
        forall itemsets $c \in C_k$ do
        forall ($k$-1) - subsets $s$ of $c$ do
        if ( $s \notin L_{k-1}$ ) then
        delete $c$ from $C_k$;
end function;
```

Figure D.2. Pseudo code of apriori_gen( ) [157] [18]

The apriori_gen ( ) function is performed in two steps: (1) join step and (2) prune step. In the first step, the k-element candidate sets (C_k) are generated by combining the frequent (k-1)-element sets (L_{k-1}). In step two, those candidate sets whose any subset is not a frequent set are removed from the C_k set.. The second step of the apriori_gen ( ) function requires checking whether the created set is actually a candidate set, i.e., it requires checking whether each subset of that set is a frequent set.

It is sufficient to create a counter c.count for each candidate set c, which will count the number of transactions supporting set c. The Apriori algorithm requires either k or $k+1$ readings of database D, where k is the maximum size of a frequent set. The Apriori algorithm uses the monotonic property of the support for a set of items. This means that if a set is a frequent set, then all its subsets are also frequent. It also follows from the monotony property that there is no need to calculate support for a set whose subset is not a frequent set. The monotony of the support measure allows to reduce the number of frequent data sets.

D.1.2. Algorithm Apriori example

Consider the association rule and its characteristics - support, confidence, lift. In the collection of N=1000 events, there were 200 items of system failures (n(failure)) and 50 items of operator intervention (n(operator)). In the case of 20 transactions, both failure and operator intervention (n(failure&operator) happened in the same time frame. Hence, it can be calculated that:

$$\mathrm{supp}(defect) = \frac{n(defect)}{N} = \frac{200}{1000} = 0.2 \qquad \text{(D.1)}$$

$$\mathrm{supp}(operator) = \frac{n(operator)}{N} = \frac{50}{1000} = 0.05 \qquad \text{(D.2)}$$

$$\operatorname{supp}(defect \to operator) = \frac{n(defect \,\&\, operator)}{N} = \frac{20}{1000} = 0.02 \tag{D.3}$$

$$conf\,(defect \to operator) = \frac{n(defect \,\&\, operator)}{n(defect)} = \frac{20}{200} = 0.1 \tag{D.4}$$

$$lift(defect \to operator) = \frac{conf\,(defect \to operator)}{P(defect) \cdot P(operator)} = \frac{0.10}{0.01} = 10 \tag{D.5}$$

where:

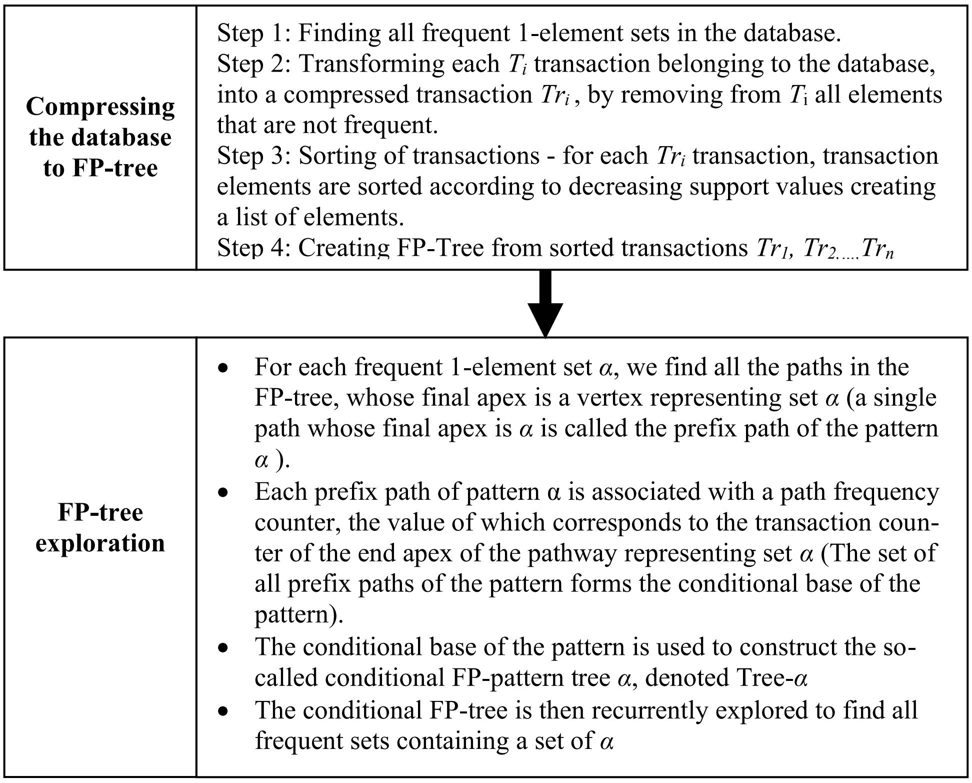
$$P(defect) = \frac{n(defect)}{N} = \frac{200}{1000} = 0.2$$

$$P(operator) = \frac{n(operator)}{N} = \frac{50}{1000} = 0.05$$

Support of 2% means that among the examined transactions, the predecessor and successor occur together in two percent, and confidence of 10% means that in 10% of the examined transactions there is also a successor.

D.1.3. Algorithm FP-growth

Frequent pattern growth algorithm (FP-Growth) has been presented by Han, Pei & Yin in the year 2000 [46]. The FP-Growth algorithm uses a completely different set of frequent sets. It contains two basic steps, which are presented in diagram D.3.



Compressing the database to FP-tree	Step 1: Finding all frequent 1-element sets in the database. Step 2: Transforming each T_i transaction belonging to the database, into a compressed transaction Tr_i, by removing from T_i all elements that are not frequent. Step 3: Sorting of transactions - for each Tr_i transaction, transaction elements are sorted according to decreasing support values creating a list of elements. Step 4: Creating FP-Tree from sorted transactions $Tr_1, Tr_{2.....}Tr_n$

FP-tree exploration	• For each frequent 1-element set α, we find all the paths in the FP-tree, whose final apex is a vertex representing set α (a single path whose final apex is α is called the prefix path of the pattern α). • Each prefix path of pattern α is associated with a path frequency counter, the value of which corresponds to the transaction counter of the end apex of the pathway representing set α (The set of all prefix paths of the pattern forms the conditional base of the pattern). • The conditional base of the pattern is used to construct the so-called conditional FP-pattern tree α, denoted Tree-α • The conditional FP-tree is then recurrently explored to find all frequent sets containing a set of α

Figure D.3. FP-Growth algorithm steps [118]

In the first step, the algorithm searches the database for all one-element frequent sets. The next step is to remove the uncommon elements from the T_i transaction, which results in a modified set of $T = T_1, ..., T_n$ transactions, consisting only of one-element sets of frequent. Then, the set of transactions is sorted in decreasing order of support for each transaction. After this step, the transactions are transformed into FP-Tree. FP-tree is a rooted, vertex-labelled acyclic graph. The root of the graph has a 'null' label, the other vertices of the graph, both inner vertices and leaves, represent a 1-element frequent set. Each vertex of the graph, with the exception of the root, has a label representing a 1-element frequent set and a transaction counter representing the number of transactions supporting the set [118].

```
procedure FP-Growth (Tree, $\alpha$)
    if Tree contains a single path P
    then for each combination of $\beta$ vertices of pathway P do
      generate a set $\beta \cup \alpha$ with support equal to the minimum element support
          belonging to $\beta$
    end do
    else for each $\alpha$-i belonging to the table of headers Tree elements do
          generate a set of $\beta$ = $\alpha$-i $\cup$ $\alpha$ with support = support($\alpha$-i);
          create a conditional base for the $\beta$ pattern;
          create a conditional FP-tree of pattern $\beta$ - Tree-$\beta$;
    if Tree-$\beta \neq \emptyset$ then FP-Growth(Tree-$\beta$, $\beta$);
end procedure;
```

Figure D.4. FP-Growth pseudo code [121]

The FP-Growth algorithm has two initial parameters (Fig. D.4): *Tree* = FP-tree and *α* = null. If the FP-tree has only a single path *p*, then for each combination of *β* vertices of path *p* is created a set $\beta \cup \alpha$ with support equal to the minimum support of the elements in the *β* set. If an FP-tree contains more than one path, then each element *α* - *i* belonging to the array *Tree* header is created set $\beta = \alpha - i \cup \alpha$ with support equivalent to that of elements *α* - *i*. Then, a conditional base of pattern *β* and a conditional FP-tree of pattern *β*, marked *Tree-β*, are generated. After this step it is checked if *Tree-β* is not empty. If it is empty, the algorithm is interrupted, otherwise the FP-Growth procedure is restarted with the parameters *Tree* = *Tree-β* and *α* = *β*. Evolution of Apriori algorithm as FP-growth algorithm benefits in the fact that the algorithm only needs to read the file twice, as opposed to Apriori who reads it once for every iteration, it removes the need to calculate the pairs to be counted, which is very processing heavy, this makes it much faster than Apriori.

Limitations:

a) Computationally Expensive. Even if the Apriori algorithm reduces the number of candidate item sets to be taken into account, this number can still be huge when store stocks are large or when the support threshold is low. However, an alternative solution would be to reduce the number of comparisons by using advanced data structures, such as hash tables, to more efficiently sort candidate item sets.

b) False associations. Large inventory analysis would involve more itemset configurations, and the support threshold might need to be lowered to detect certain associations. However, lowering the support threshold could also increase the number of parasitic associations detected. To ensure that the identified associations are generalizable, they can first be distilled from a set of learning data, before their support and trust are evaluated in a separate set of test data.

c) Interestingness problem occurs as in the generated rules appears that:
    - o some generated rules can be self-evident
    - o some marginal events can dominate
    - o interesting events can be rarely occurring

d) There exist subjective and objective measures. Where subjective measures can be the result of earlier user experience and feelings. Also, it appears the user can treat rules as interesting if he can get an advantage by using them but this depends on the time and user. The objective measures are based on thresholds values controlled by the user.

e) Difficulties to find rarely occurring events

f) Alternative methods (other than Apriori) can address this by using a non -uniform minimum support threshold

Advantages:

a) Quality of defined rules can be assessed by means of objective rules which can be characterized by the user,

b) Length of the rule can be limited by the user by defined threshold

c) Quantitative values can be quantized

d) Usefulness of a rule can be measured with a minimum support threshold

Appendix 5. Description of the analysed object

As an object of the examination was chosen the process of radial tire built, concentrating especially on two of its stages named processed raw materials - mixing (semi-finished) process and the process of fabric. The process of tire construction can be divided into processes as follows [28] (Fig. E.1):

- Processing raw materials (semi-finished production);
- Tire Parts Production e.g.: process of fabric, metal calendaring;
- Tire Parts Build up;
- Curing;
- Finishing;

- Final Inspection.

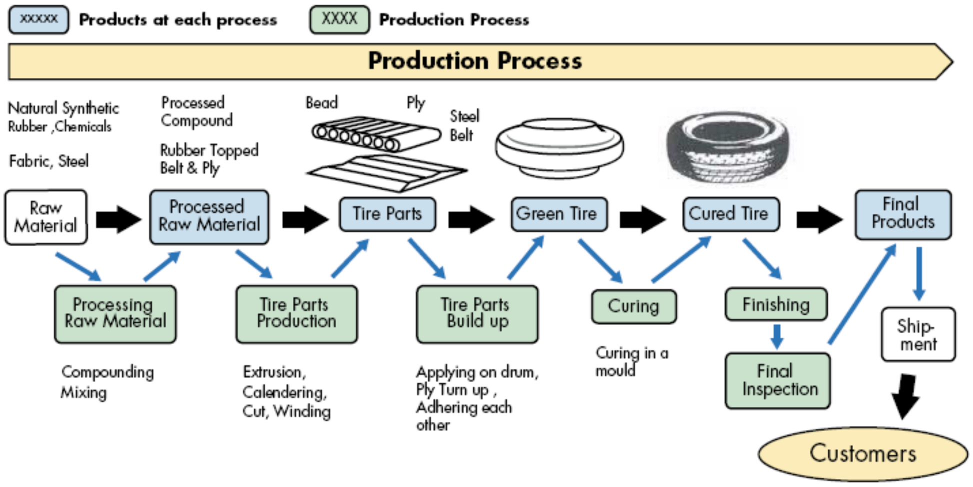


Figure E.1. Tire production processes presentation [163]

- Processing raw materials

In the process of tire production, many kinds of raw materials - pigments, chemicals, depending on tire type around thirty different kinds of rubber, tire cord fabrics, bead wire, etc. are used. The tire production process begins with the mixing of blended rubber with process oils, carbon black, pigments, antioxidants, accelerators and other additives, each of which contributes certain properties to what is called a compound. These ingredients are mixed in huge blenders called Banburies or mixers. They blend the compounds together, producing a black, gum-like material that will be milled again later for use in a tire.

- Tire Parts Production;

Next, the rubber is carried to the breakdown mills to be fed between massive pairs of rollers, over and over, mixing and blending the material to prepare the different compounds for the feed mills, where they are slit into strips and carried by conveyor belts to become sidewalls, treads, or other parts of the tire. Another kind of rubber coats the fabric that will be used to make up the tire's body. The fabrics come in huge rolls, and they are as specialized and critical as the rubber blends. Several kinds of fabrics are used: polyester, rayon or nylon. Another key component is the tire’s bead. The bead’s backbone is formed from high-tensile steel wire. The strands are aligned into a ribbon and coated with rubber for adhesion, then wound into loops that are wrapped together to secure them until they are assembled with the rest of the tire.

- Tire Parts Build up;

The tire-building machine pre-shapes radial tires into a form very close to their final dimension to make sure the many components are in the proper position before the tire goes into a mould to be cured or vulcanized. When building a tire, the tire builder starts with a double layer of synthetic gum rubber called an innerliner. The innerliner makes it possible to seal air in a tire and eliminates the need for an inner tube that once came inside each tire. Next come two layers of ply fabric, which are sometimes referred to as the cords. Two strips called apexes stiffen the area just above the bead. Next, a pair of chafer strips is added. They are called chafer strips because they resist chafing from the wheel rim when mounted on a car. Now the tire builder adds the steel belts that resist punctures and hold the tread firmly against the road. The tread is the last part to go on the tire. After automatic rollers press all the parts firmly together, the radial tire, now called a green tire, is ready for inspection and curing.

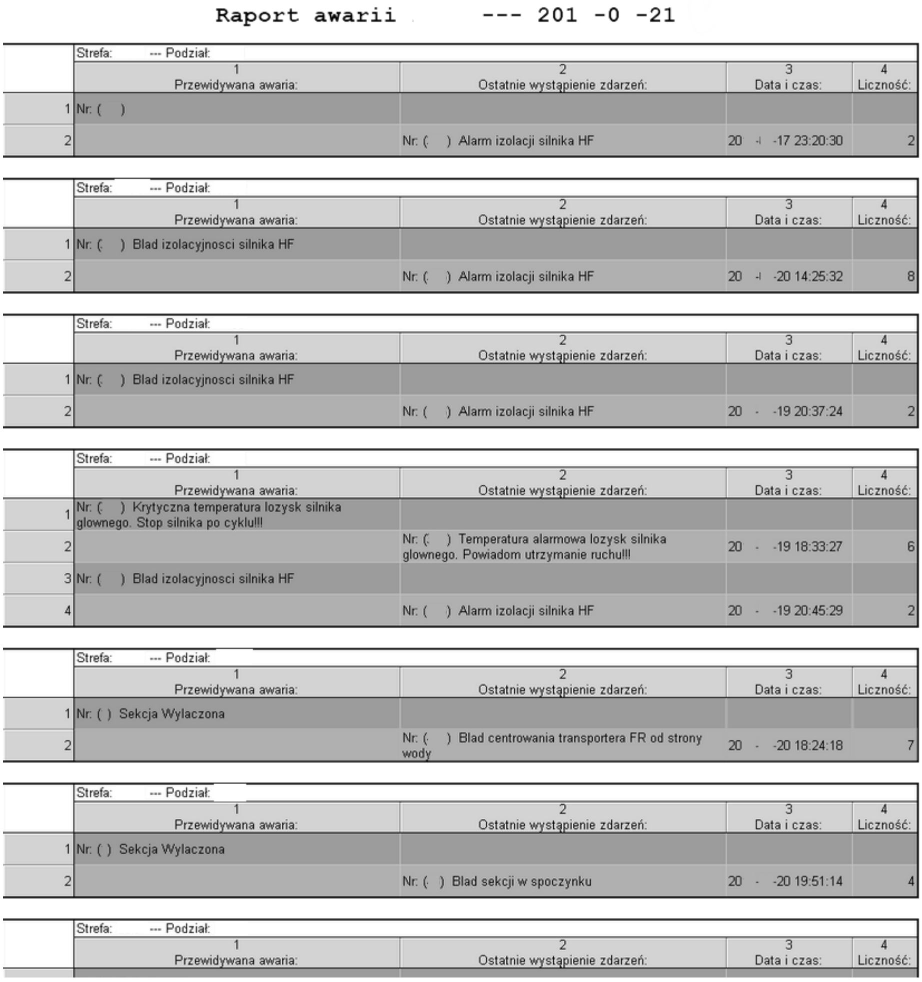
- Curing & Finishing;

The curing press is where tires get their final shape and tread pattern. Hot moulds like giant waffle iron shape and vulcanize the tire. The moulds are engraved with the tread pattern, the sidewall markings of the manufacturer and those required by law. Each press cures two tires at a time; they operate twenty-four hours a day. Passenger tires are cured at over 300 degrees for 12 to 25 minutes, sometimes much longer as in the case of large earthmover tires. As the press swings open, the tires are popped from their moulds onto a long conveyor that carries them to the final finish and inspection.

- Final Inspection.

Inspection is both visual and internal. Some tires are pulled from the production line and X-rayed. Additionally, quality control engineers regularly cut apart randomly chosen tires and study every detail of their construction that affects performance, ride or safety [28].

Appendix 6. Screens and additional data of implemented predictive tool



Raport awarii --- 201 -0 -21

	Strefa: --- Podział:			
	1 Przewidywana awaria:	2 Ostatnie wystąpienie zdarzeń:	3 Data i czas:	4 Liczność:
1	Nr: ( )			
2		Nr: ( ) Alarm izolacji silnika HF	20 - -17 23:20:30	2

	Strefa: --- Podział:			
	1 Przewidywana awaria:	2 Ostatnie wystąpienie zdarzeń:	3 Data i czas:	4 Liczność:
1	Nr: ( ) Blad izolacyjnosci silnika HF			
2		Nr: ( ) Alarm izolacji silnika HF	20 - -20 14:25:32	8

	Strefa: --- Podział:			
	1 Przewidywana awaria:	2 Ostatnie wystąpienie zdarzeń:	3 Data i czas:	4 Liczność:
1	Nr: ( ) Blad izolacyjnosci silnika HF			
2		Nr: ( ) Alarm izolacji silnika HF	20 - -19 20:37:24	2

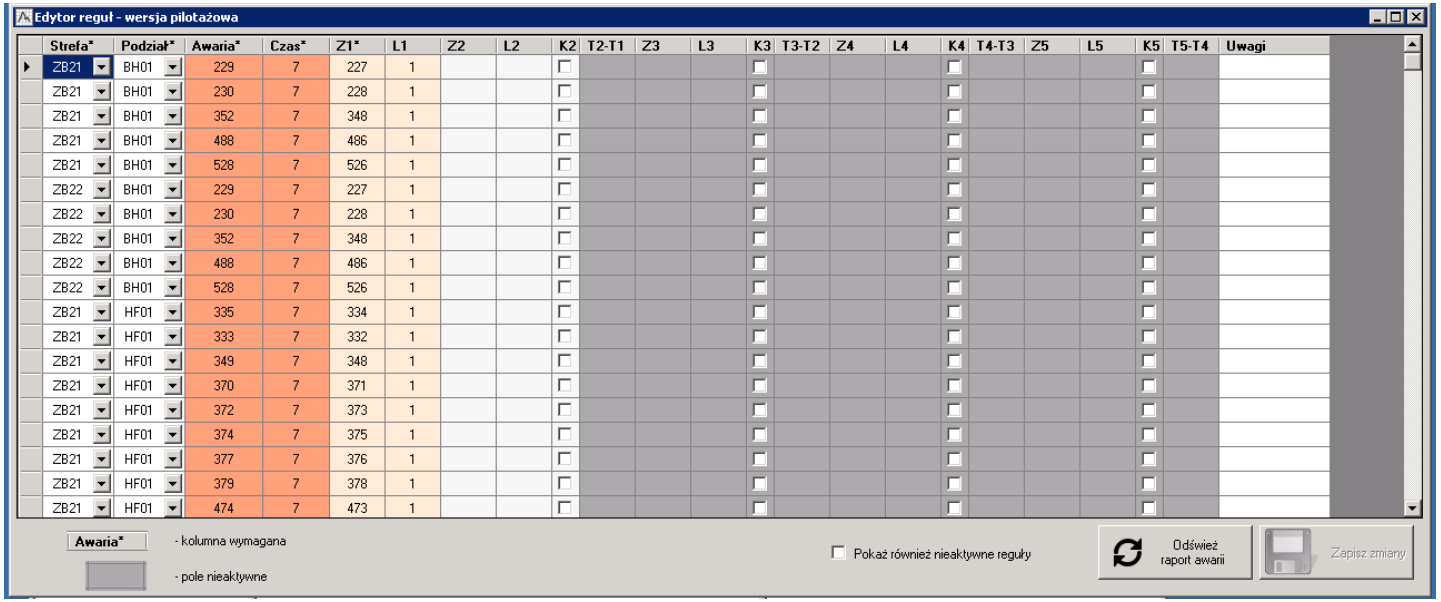
	Strefa: --- Podział:			
	1 Przewidywana awaria:	2 Ostatnie wystąpienie zdarzeń:	3 Data i czas:	4 Liczność:
1	Nr: ( ) Krytyczna temperatura lozysk silnika glownego. Stop silnika po cyklu!!!			
2		Nr: ( ) Temperatura alarmowa lozysk silnika glownego. Powiadom utrzymanie ruchu!!!	20 - -19 18:33:27	6
3	Nr: ( ) Blad izolacyjnosci silnika HF			
4		Nr: ( ) Alarm izolacji silnika HF	20 - -19 20:45:29	2

	Strefa: --- Podział:			
	1 Przewidywana awaria:	2 Ostatnie wystąpienie zdarzeń:	3 Data i czas:	4 Liczność:
1	Nr: ( ) Sekcja Wylaczona			
2		Nr: ( ) Blad centrowania transportera FR od strony wody	20 - -20 18:24:18	7

	Strefa: --- Podział:			
	1 Przewidywana awaria:	2 Ostatnie wystąpienie zdarzeń:	3 Data i czas:	4 Liczność:
1	Nr: ( ) Sekcja Wylaczona			
2		Nr: ( ) Blad sekcji w spoczynku	20 - -20 19:51:14	4

	Strefa: --- Podział:			
	1 Przewidywana awaria:	2 Ostatnie wystąpienie zdarzeń:	3 Data i czas:	4 Liczność:

Figure F.1. Example of generated report



Edytor reguł - wersja pilotażowa

Strefa*	Podział*	Awaria*	Czas*	Z1*	L1	Z2	L2	K2	T2-T1	Z3	L3	K3	T3-T2	Z4	L4	K4	T4-T3	Z5	L5	K5	T5-T4	Uwagi
ZB21	BH01	229	7	227	1			□				□				□				□		
ZB21	BH01	230	7	228	1			□				□				□				□		
ZB21	BH01	352	7	348	1			□				□				□				□		
ZB21	BH01	488	7	486	1			□				□				□				□		
ZB21	BH01	528	7	526	1			□				□				□				□		
ZB22	BH01	229	7	227	1			□				□				□				□		
ZB22	BH01	230	7	228	1			□				□				□				□		
ZB22	BH01	352	7	348	1			□				□				□				□		
ZB22	BH01	488	7	486	1			□				□				□				□		
ZB22	BH01	528	7	526	1			□				□				□				□		
ZB21	HF01	335	7	334	1			□				□				□				□		
ZB21	HF01	333	7	332	1			□				□				□				□		
ZB21	HF01	349	7	348	1			□				□				□				□		
ZB21	HF01	370	7	371	1			□				□				□				□		
ZB21	HF01	372	7	373	1			□				□				□				□		
ZB21	HF01	374	7	375	1			□				□				□				□		
ZB21	HF01	377	7	376	1			□				□				□				□		
ZB21	HF01	379	7	378	1			□				□				□				□		
ZB21	HF01	474	7	473	1			□				□				□				□		

Awaria* - kolumna wymagana

▨ - pole nieaktywne

□ Pokaż również nieaktywne reguły

Figure F.2. Screen of the rule generator

Table F.1. Percentage distribution of events by type

Category	Number of events	Percentage
S2	280169	20%
S1	973365	68%
E2	40090	3%
E1	129709	9%

S1 - Event classified as an important predecessor;

S2 - Event classified as a not important predecessor;

E1 - Successor event resulting in an immediate stoppage of the machine;

E2 - Successor event resulting in a stoppage of the machine after a cycle has been completed.

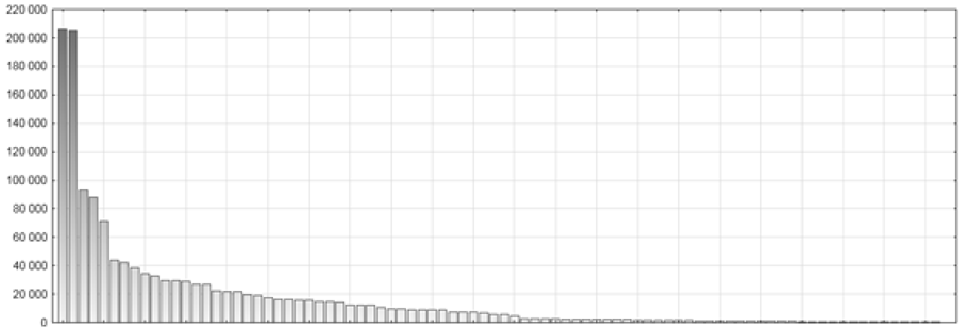


Figure F.3. Distribution of the number of events by sections of production lines

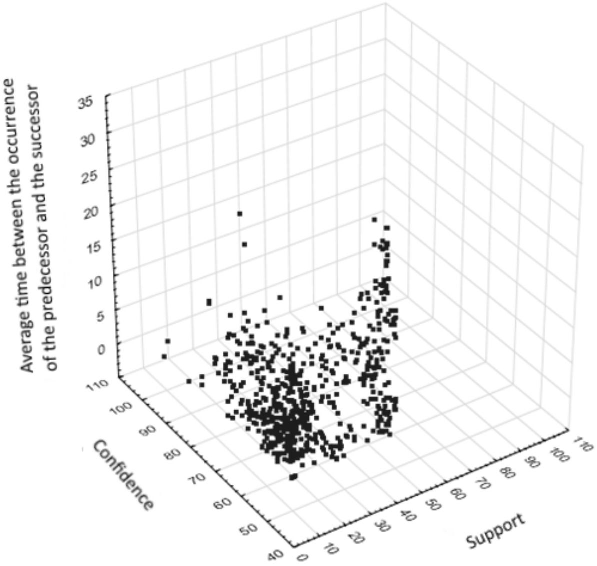


Figure F.4. The relationship between support, trust and the average time between the performance of a predecessor and a successor

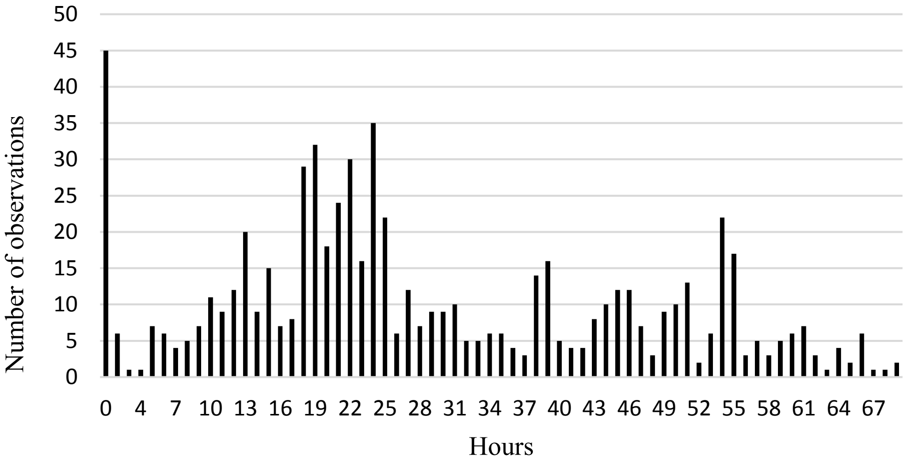


Figure F.5. Distribution of the maximum time between the occurrence of the predecessor and the successor

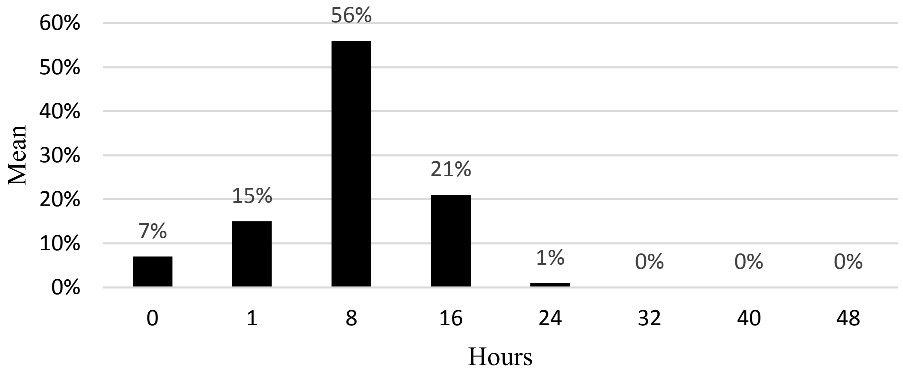


Figure F.6. Distribution of the median value of the time between the occurrence of the predecessor and the successor

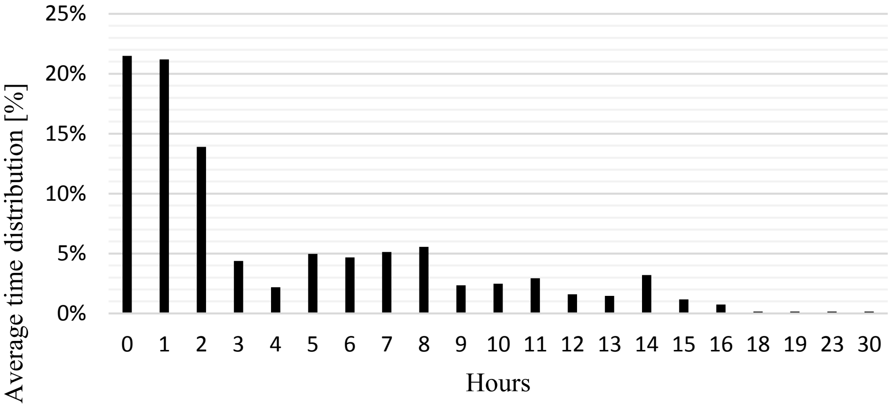


Figure F.7. Distribution of the average time between the occurrence of the predecessor and the successor

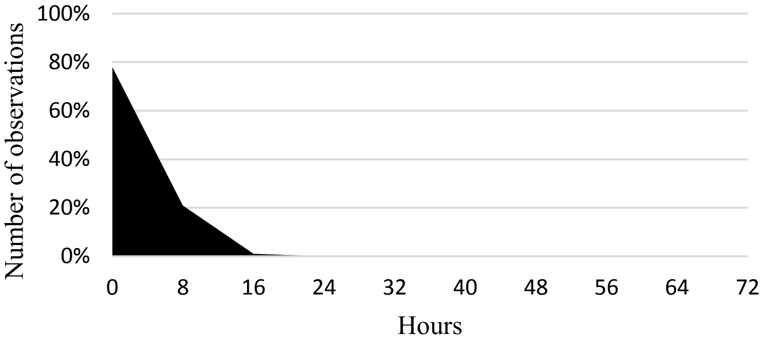


Figure F.8. Distribution of the average time between the occurrence of the predecessor and the successor

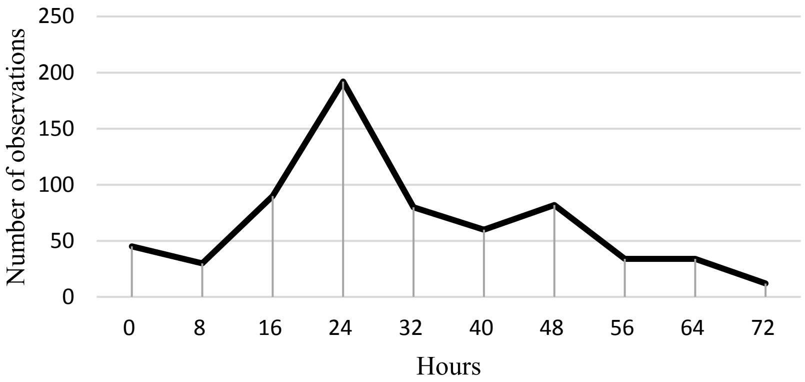


Figure F.9. Distribution of the average time between the occurrence of the predecessor and the successor

Table F.2. A list excerpt of rules found during the analysis of historical data using association rules

Zone	**Predecessor event [P]**	**Successor event [S]**	**Support [%]**	**Confidence [%]**	**Number of events [Units]**	**Mean time between P and S [h]**	**Max time between P and S [h]**
Ligne_1 _E1401	144_S1	1_E1	10.47	69.23	9	30	39
Ligne_1 _E1401	92_S1	1_E1	17.44	75	18	23.2	46
Ligne_2 _E1001	30_S1	1_E1	19.75	64	20	19	50
Ligne_1 _E1402	92_S1	1_E1	9.8	58.82	16	18.7	61
Ligne_2 _E1402	62_S1	49_E1	48.11	51.52	81	16.9	60
Ligne_2 _E1132	11_S1	1_E1	29.7	55.56	66	16.7	61
Ligne_2 _E1122	11_S1	1_E1	24.53	50	69	16.3	61
Ligne_2 _E1131	11_S1	1_E1	29.29	53.7	69	16.1	61
Ligne_2 _E1112	11_S1	1_E1	27.27	50	70	16	61
Ligne_2 _E2602	281_S1	304_E1	10.17	50	51	15.8	54
Ligne_2 _E2602	281_S1	303_E1	10.17	50	51	15.8	54