MASTERARBEIT

CHEMISTRY 4.0 – DIGITALIZATION AND RISKS

A Case Study

ausgeführt am

CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

Studiengang
Informationstechnologien und Wirtschaftsinformatik

Von: Jörn Saischek
Personenkennzeichen: 1610320036

Graz, am 12. Juli 2018 ....
Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

....

Unterschrift

NOTE OF THANKS

Although writing up a master thesis might be the effort of one person, the reason that a person even gets as far as starting, is thanks to all the people supporting that student. I am grateful for everyone who has been there to support my journey. I'm indebted to and grateful for the following persons…

… my supervisor Univ.-Prof. Mag. et Dr.rer.soc.oec. Helmut Zsifkovits. His lecture inspired me to select this theme. His support, encouragement and feedback made this thesis possible.

… FH Campus02 for providing an enjoyable place to study.

… my uncle Dipl. Ing. Gerald Saischek. His lifelong dedication to science is an inspiration.

… my great and beloved kids Marc and Marie.

… to Andrea, she knows why.

… my mother who always supported and helped me.

… to all who supported me. Without their help, I would not be where I am today.

KURZFASSUNG

Die Digitalisierung in der chemischen Prozessindustrie führt zu dezentralisierten, hochautomatisierten Produktionsumgebungen, in denen intelligente Produkte ihre Produktion überwachen und steuern. In der Literatur finden sich wenige Arbeiten die sich mit der Digitalisierung chemischer Fabriken beschäftigen. Traditionelle Risikomanagementmethoden sind problematisch für hochkomplexe Systeme. Eine für komplexe System geeignete Methode ist die Functional Resonance Accident Method FRAM. Die FRAM Methode analysiert die Performance Variabilität von Funktionen und deren Kopplungen.

Ein Ziel dieser Arbeit war die Analyse und Simulation von Risiken und Performance Variabilität chemischer Fabriken in Abhängigkeit ihres Digitalisierungsgrades. Aufgrund ihres explorativen Charakters war ein weiteres Ziel dieser Arbeit die Identifikation weiterer Forschungsaufgaben.

Eine neue hybride Simulationsmethode, die einer Kombination aus FRAM und Fuzzy-Logik entspricht wurde zur Simulation chemischer Fabriken entwickelt. Diese Simulationsmethode kann generell zur Identifikation von Risiken in komplexen sozio-technischen Systemen verwendet werden. Eine neue Metrik zur Identifizierung kritischer Kopplungen wurde entwickelt.

Als Teil dieser Arbeit wurden drei fiktive chemische Fabriken unterschiedlichen Digitalisierungsgrades im Rahmen einer Fallstudie designed. Die Ergebnisse der FRAM Methode unterstützen die Theorie, dass die Digitalisierung zu einer generell niedrigeren Performance Variabilität führt. Unter dem Einfluss von Störungen auf das System waren die Ergebnisse nicht eindeutig. Ergänzend zur FRAM Analyse wurde eine Fehlerbaumanalyse für die drei chemischen Fabriken durchgeführt und eine Korrelation zwischen dem Digitalisierungsgrad und dem Top Event der Fehlerbaumanalyse festgestellt.

ABSTRACT

The impact of digitalization on the chemical process industry will lead to a decentralized, highly automated production environment, in which intelligent products supervise and control their own production processes. There has been little work directed to the impact of digitalization on chemical plants. Traditional risk management methods are problematic in this highly complex environment. One method suitable for complex systems is the functional resonance accident method FRAM. FRAM analyses examine performance variabilities of functions and the couplings between these functions.

The aims of this study were to analyze and simulate the risk and performance variability of chemical plants in dependence of their digitalization maturity. As this study was also exploratory in its nature, an additional goal was the identification of future research topics.

To accomplish this research agenda, a new hybrid simulation methodology, that combines functional resonance accident methodology and fuzzy logic to simulate chemical plants, was developed. This simulation methodology can generally be used to identify risks in complex socio-technological systems. A new metric was proposed and used to identify critical couplings.

In this study three plants, representing three different digitalization maturity levels, were designed in a case study. The results of the FRAM methods supported the theory that digitalization leads to a general lower performance variability. If disturbances were introduced into the simulation, the results were inconclusive. Supplementing these findings, an FTA analysis for the specific top event run-away reaction showed the correlation between this top event and the digital maturity level of the chemical plant.

TABLE OF CONTENTS

1 INTRODUCTION

"Well Babbage, what are you thinking about? I am thinking that all these tables (pointing to the logarithms) one day may be computed by machinery."

Anecdote about Charles Babbage, c. 1825

1.1 Motivation

The vision of Chemistry 4.0 and Industry 4.0 is a decentralized, highly automated production environment in which intelligent products supervise and control their own production processes as well as factories, information systems and humans interacting in real-time crossing corporate boundaries. This research recognizes the difficulties and challenges posed by increasing dependences of physical production, virtual information systems and humans, and consequently new emerging risks.

The research is needed for two reasons. First, the research on the risk impact of digitalization on plants is still in its infancy. Second, currently used risk assessment methodologies are in most cases not suitable for complex systems. Thus, this study is exploratory in its nature.

1.2 Expected Thesis Contributions

To shed some light on the above-mentioned reasons, this research investigates changing risk expressed as performance variability in chemical plants, as a result of different digitalization maturity levels. Due to the newness of this research field, this study intends to contribute to fundamentals of this field and also discover questions for further research.

Also, this research proposes and develops a new hybrid simulation methodology, that combines functional resonance accident methodology and fuzzy logic to simulate chemical plants. This simulation methodology can generally be used to identify risks in complex socio-technological systems.

1.3 Research Question

In order to explore how digitalization influences chemical production, the research question to be addressed in this thesis is: What is the impact of digitalization on performance variability of chemical plants, specializing in batch reactions?

1.4 Research Objectives and Hypotheses

The prime research objective is to explore, describe and analyze the impact of digitalization on chemical plants.

In order to explore the research domain, the research question has been broken down into three objectives. The three research objectives are:

- The robustness of the chemical plant in terms of performance variability in relation to its digitalization maturity level.
- The impact of maintenance strategies made available through different digitalization maturity levels, on scheduling.
- The safety of the chemical production in view of chemical process deviations, depending on its level of digitalization.

These three research objectives are investigated by the following hypotheses:

Thesis: The risk for a runaway reaction caused by reaction deviations is related to the digitalization of the chemical plant.

Hypothesis **H1**: If the digitalization maturity level of the chemical plant increases, the probability of a runaway reaction, caused by reaction deviations, decreases.

Null Hypothesis $H1_0$: If the digitalization maturity level of the chemical plant increases, the probability of a runaway reaction, caused by reaction deviations, will not decrease.

Thesis:

Hypothesis **H2**: If the digitalization maturity level of the chemical plant increases, the performance variability of scheduling, caused by reactive maintenance, will decrease.

Null Hypothesis $\mathbf{H2_0}$: If the digitalization maturity level of the chemical plant increases, the performance variability of scheduling, caused by maintenance, will not decrease.

Thesis: The robustness of a chemical plant is related to its digitalization

Hypothesis **H3**: If the digitalization maturity level of the chemical plant increases, the robustness of the whole plant, expressed as the accumulated performance variability increases.

Null Hypothesis **H3$_0$**: If the digitalization maturity level of the chemical plant increases, the robustness of the whole plant, expressed as the accumulated performance variability will not increase.

Hypothesis **H4**: If the digitalization maturity level of the chemical plant increases, the robustness of the whole plant, expressed as the accumulated performance variability, when confronted with disturbances, will increase.

Null Hypothesis **H4$_0$**: If the digitalization maturity level of the chemical plant increases, the robustness of the whole plant, expressed as the accumulated performance variability, when confronted with disturbances, will not increase.

1.5 Methodology

In a case study, three fictional chemical plants, representing three different digitalization maturity levels are investigated. These plants are examined by fault tree analysis and by a new proposed hybrid simulation methodology, that extends functional resonance accident methodology with fuzzy logic. Data obtained from expert interviews and literature are used in these simulations.

1.6 Limitations of this study

As this study is an investigative study and exploratory in its nature, the scope of the thesis is limited to performance variability. While other fields of research touching digitalization are also intriguing, this study restricts itself to closely examine the data within a specific context - performance variability of chemical plants with one specific kind of reaction in batch reactors.

The research employs the methodology of a case study, so its findings are consequently most relevant to companies in similar contexts. Results should be referred with caution to apply to other plants and different contexts. The research analyses data based on the perceptions of experts gathered by interviews.

1.7 Outline of the thesis

The thesis is organized as follows. Chapter 2 presents a review of literature related to Industry 4.0 and Chemistry 4.0. Chapter 3 reviews literature related to risk, risk assessment and fuzzy logic. In chapter 4, the case study is presented. Chapter 5 discusses the methodology used in this thesis. The results are presented in chapter 6. Chapter 7 summarizes the conclusions and proposes further research.

2 INDUSTRY 4.0 AND CHEMISTRY 4.0

This chapter is structured as follows: in the first section industry 4.0, its key components, design principles and control structures are discussed. The second section turns to chemistry 4.0, chemical processes, their control and process design. The third section describes digitalization maturity levels and their definitions. The last section investigates maintenance strategies.

2.1 Industry 4.0

The term industry 4.0[1] refers to the fourth industrial revolution – the integration of the manufacturing environment and internet of things. The first industrial revolution beginning in the 18th century, marks the change form an agrarian dominated economy to one based on industry. Driving forces were steam and water power and the mechanization. The widespread use of electricity, mass production and assembly lines characterize the second industrial revolution. The third industrial revolution was the introduction of computers and information technology leading to the automation of processes (Hermann, Pentek, & Otto, 2015).

In the beginning of the 21th century, it became clear that the dawn of the 4th industrial revolution had set in. Gilchrist (2016) identifies four technological advances that enabled this shift, namely

- the rapid rise of rental computing power, network connectivity and data volumes available to operations.
- increasing analytical capabilities.
- the introduction of augmented reality systems and systems reacting to touch or voice.
- new forms how to bring digital data into the physical world, like 3D printing, rapid prototyping or advanced robotics.

The potential of this 4th industrial revolution seem to be substantial as Hermann et al. (2015) state that "For the first time an industrial revolution is predicted a-priori, not observed ex-post. This provides various opportunities for companies and research institutes to actively shape the future." The economic impact of this industrial revolution is supposed to be huge, as Industrie 4.0 promises substantially increased operational effectiveness as well as the development of entirely new business models, services, and products ". The application of Industry 4.0 principles will change the manufacturing industries substantially (Manhart, 2015).

[1] Industry 4.0 is a somewhat loosely understood term, other synonyms for Industry 4.0 are Smart Industry or Smart Manufacturing, Advanced Manufacturing, Industrial Internet or Integrated Industry (Gilchrist (2016) Gilchrist(2016).

In his publication Kagermann (2013, cited by (Hermann et al., 2015)) present their view of Industrie 4.0:

> *"In the future, businesses will establish global networks that incorporate their machinery, warehousing systems and production facilities in the shape of Cyber-Physical Systems (CPS). In the manufacturing environment, these Cyber-Physical Systems comprise smart machines, storage systems and production facilities capable of autonomously exchanging information, triggering actions and controlling each other independently. This facilitates fundamental improvements to the industrial processes involved in manufacturing, engineering, material usage and supply chain and life cycle management. The Smart Factories that are already beginning to appear employ a completely new approach to production. Smart products are uniquely identifiable, may be located at all times and know their own history, current status and alternative routes to achieving their target state. The embedded manufacturing systems are vertically networked with business processes within factories and enterprises and horizontally connected to dispersed value networks that can be managed in real time – from the moment an order is placed right through to outbound logistics. In addition, they both enable and require end-to-end engineering across the entire value chain."*

This fourth industrial revolution will be built upon networks of cyber-physical systems, which receive and share data over these networks and make intelligent decisions based on this information (Brettel, Friederichsen, Keller, & Rosenberg, 2014; Feeney, Frechette, & Srinivasan, 2015; Lachenmaier, Lasi, & Kemper H.G., 2015). As Feeney et al. (2015) describe:

> *Manufacturing systems in this new era will have to get smart. They need to be autonomous, self-aware, and self-correcting. In short, they should be able to function with as little human intervention as possible, while at the same time work harmoniously with human supervision and collaboration.*

According to Brettel et al. (2014) and Gilchrist (2016), the major characteristics of Industry 4.0 are:

- Individualized Production
- Horizontal Integration in Collaborative Networks
- Vertical Integration of Smart Production Systems
- Acceleration of Manufacturing
- Coverage of complete lifecycle of the product

Lee, Bagheri, and Kao (2015) compare the attributes and used technologies of today's factories and an Industry 4.0 factory (see Table 1).

Table 1 Comparison of today's factory and an Industry 4.0 factory

	Data Source	Today's factory		Industry 4.0	
		Attributes	Technologies	Attributes	Technologies
Component	Sensor	Precision	Smart sensors and fault detection	Self-aware Self-predict	Degradation monitoring & remaining useful life prediction
Machine	Controller	Producibility & performance	Condition-based monitoring & diagnostics	Self-aware Self-predict Self-compare	Up time with predictive health monitoring
Production system	Networked system	Productivity & OEE	Lean operations: work and waste reduction	Self-configure Self-maintain Self-organize	Worry-free productivity

Note: A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing system (Lee et al., 2015).

2.1.1 Key Components of Industry 4.0

To implement the design principles of industry 4.0 – interoperability, virtualization, decentralization, real-time capacity, service orientation and modularity – several key components have been characterized by Hermann et al. (2015) - Cyber-Physical Systems CPS, Internet of Things IoT, Internet of Services IoS and Smart Factories.

In the scientific community, there are some slightly different interpretations what a CPS is. For instance Rajkumar, Lee, Sha, and Stankovic (2010) interpret CPS as systems which "are physical and engineered systems, whose operations are monitored, coordinated, controlled and integrated by a computing and communication core." CPS are "embedded systems together with their physical environment" (Marwedel, 2011). "CPS efforts are concerned with the nature of cyber-physical coupling and the system of systems characteristics of software-controlled systems" (Lu, Morris, & Frechette, 2016). Lee (2008) describes CPS as "integrations of computation with physical processes". Gunes, Peter, Givargis, and Vahid (2014) conclude that CPSs are "complex, multi-disciplinary, physically-aware next generation engineered systems that integrate embedded computing technology (cyber part) into the physical phenomena by using transformative research approaches. This integration mainly includes observation, communication, and control aspects of the physical systems from the multi-disciplinary perspective." A CPS can be described as a system composed of a cyber system, sensors, actuators and the physical world see Figure 1. The cyber systems consist of devices, interpreting and processing information and exchanging data within their network. The physical world is the real-world process or facility, the CPS should monitor and actuate. The sensor, the actuator and the communication network move and convert the data and commands between the physical world and the cyber system. (Gunes et al., 2014)

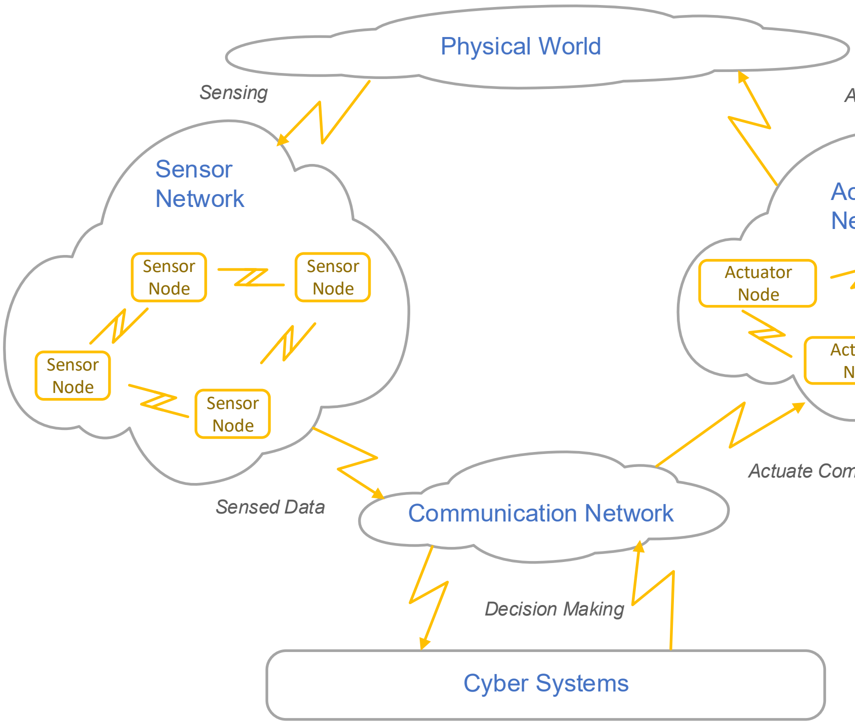


Figure 1 CPS Holistic view Gunes et al. (2014)

Brettel et al. (2014) describe that “CPS will enable the communication between humans, machines and products alike. As they are able to acquisition and process data, they can self-control certain tasks and interact with humans via interfaces”.

The IoT can be regarded as a network of connected devices. Hermann et al. (2015) argue that “… the IoT can be defined as a network in which CPS cooperate with each other through unique addressing schemas”. Gilchrist (2016) distinguishes consumer, commercial and industrial forms of internet, with different IoT strategies. While sensors, producing data to control operations, have been used in industry for decades and machine-to-machine communication is nothing new in industrial settings, the concept of IoT surpasses these in scale. Gilchrist explains:

> *“Huge data streams can be analyzed online using cloud-hosted advanced analytics at wire speed. Vast quantities of data can be stored in distributed cloud storage systems for future analytics performed in batch formats. These massive batch job analytics can glean information and statistics, from data that would never previously been possible because of the relatively tiny sampling pools or simply due to more powerful or refined.”*

Lee and Lee (2015) state that “the true value of the IoT for enterprises can be fully realized when connected devices are able to communicate with each other and integrate with vendor-managed inventory systems, customer support systems, business intelligence applications, and business analytics”. Five technologies are the key elements of IoT, identification, mainly by radio frequency identification RFID, sensor networks, middleware, cloud computing and IoT application software (Lee & Lee, 2015).

Hermann et al. (2015) define the Internet of Services as “a system consisting of participants, an infrastructure for services, business models and the services themselves. Services are offered and combined into value-added services by various suppliers; they are communicated to users as well as consumers and are accessed by them via various channels.”

Some of the main challenges Industry 4.0 implementations face are the increasing complexity of systems, the need for flexibility and the capacity for innovation (Lachenmaier et al.). Hecklau, Galeitzke, Flachs, and Kohl (2016) using the PESTEL-framework (Lynch, 2006) identified Political, Economic, Social, Technical, Environmental and Legal challenges (i.e. PESTEL) and derived necessary core competencies for each challenge. In their study, based on semi-structured interviews with experts, Schumacher, Erol, and Sihn (2016) conclude that these problems arise while implementing Industry 4.0 concepts: the complexity of Industry 4.0 is perceived as immense, lack of precise concepts of Industry 4.0 lead to uncertainty in regard to foreseen benefits and missing standards and guidelines make it difficult for companies to determine their own Industry 4.0 competences, leading to uncoordinated measures.

Gilchrist (2016) compares the traditional production line to a smart factory (see Figure 2). In an industry 3.0 production line, the resources create the lowest level, the Enterprise Resource Planning system (ERP) receiving orders and instructing the Manufacturing Execution System (MES) to produce the goods ordered, setting up the higher levels. He identifies several weaknesses of this approach: upon failing of one resource, the whole production stops, a failing ERP or MES will also block production. It is not easy to update the ERP in real time and changing the production environment may pose a problem due to the complexity and sheer numbers of interface options. Gilchrist argues that substitution of resources by Cyber Physical Systems CPSs with augmented capabilities like embedded sensors, network access and self-awareness, will enhance flexibility, responsivity and interface problems by removing the MES layer. The ERP evolves to a Smart Enterprise Resource Planning System SERP, communicating directly in real time with the CPSs.

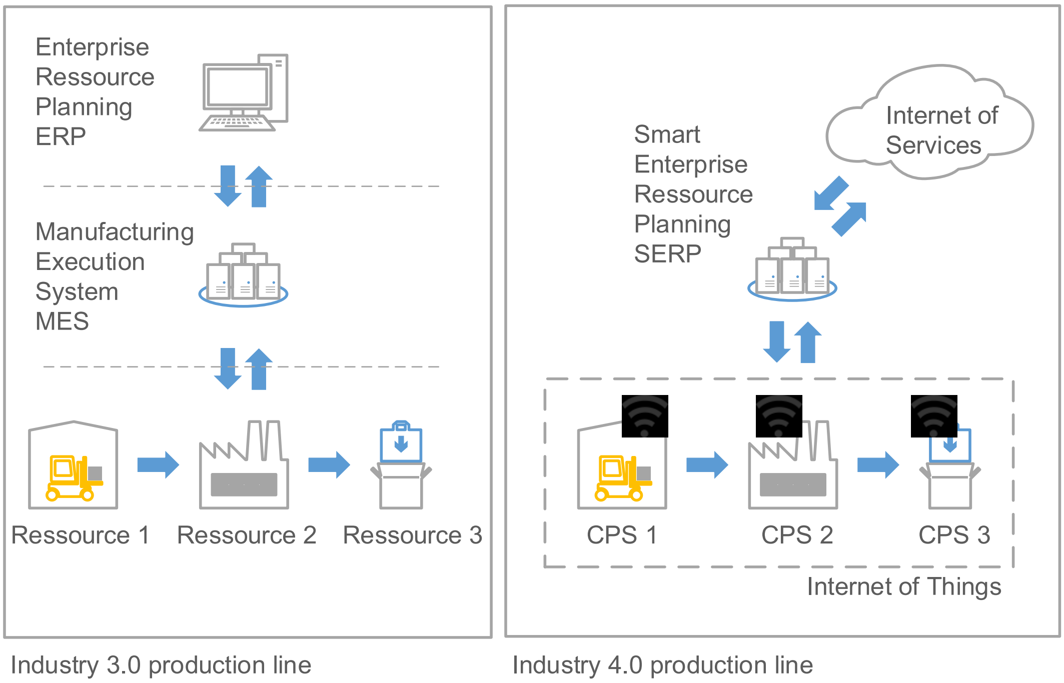


Figure 2 Traditional Industry 3.0 production line and Industry 4.0 production line. Gilchrist (2016)

Veza, Mladineo, and Gjeldum (2015) argue that production networks, one of the three key elements of Industry 4.0, flexible value chains where data and flows in real time across company boundaries, are essentially temporary virtual alliances, virtual enterprises. They argue that with automated bidding processes, automated decision-making processes based on pairwise comparisons should be used for optimal partner selection. In their paper on safety and security concepts for Human-Robot-Collaboration (HCR) Khalid, Kirisci, Ghrairi, Thoben, and Pannek (2017) distinguish between a CPS in which the computational and physical systems are integrated to control and sense the changing state of real-world variables and an extended CPS where humans interact with the CPS (see Figure 3).

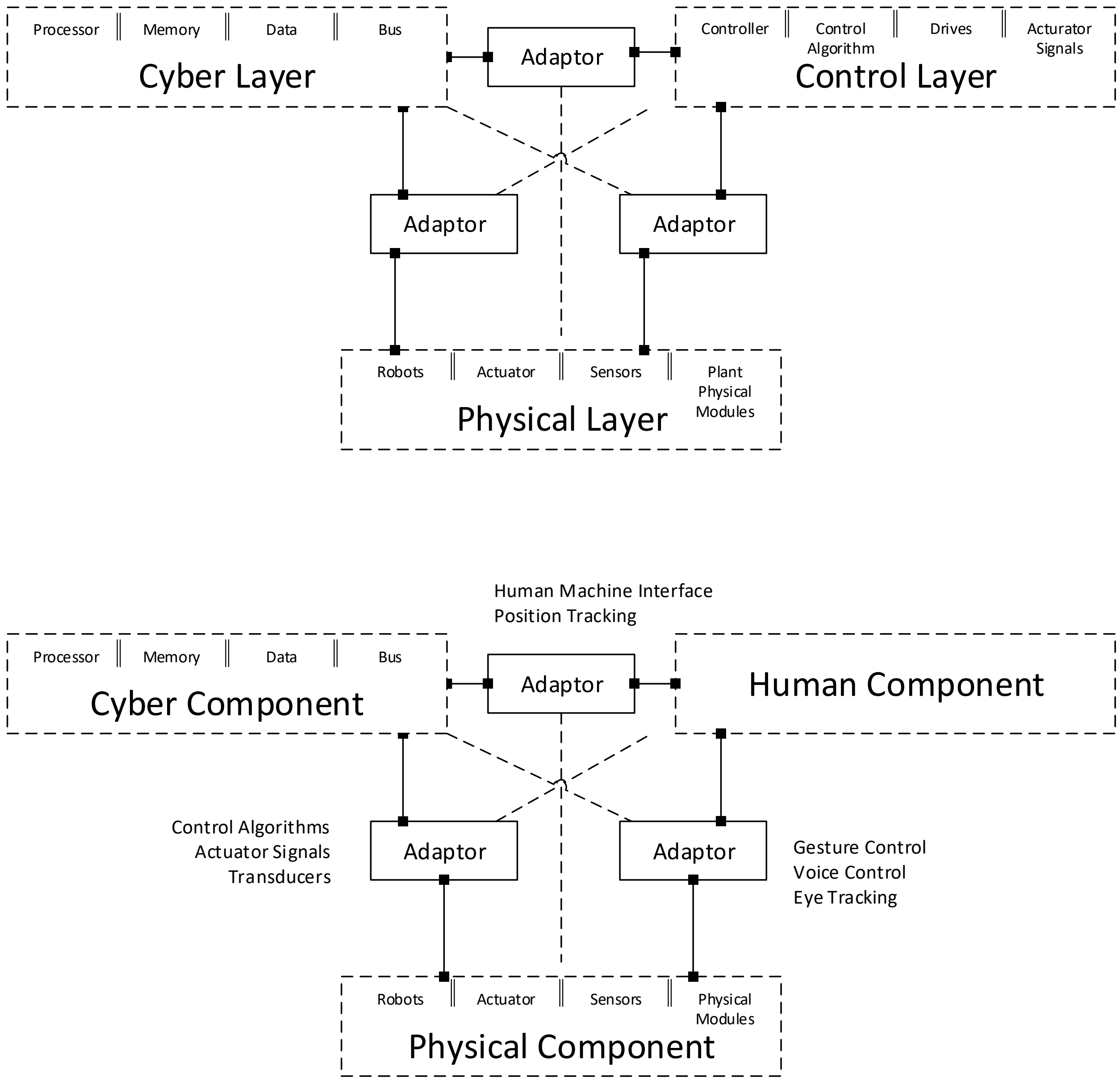
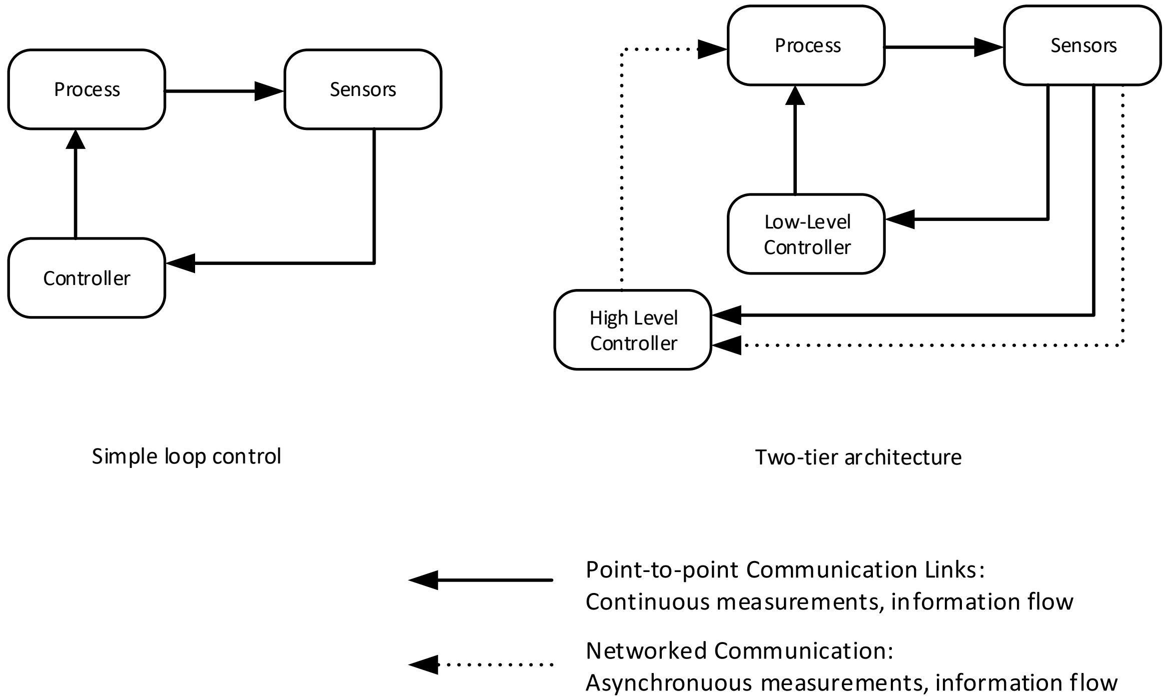


Figure 3 CPS Interactions (Khalid et al., 2017)

2.1.2 Control structures

In its simplest form, a control loop consists of a process which is to be controlled, sensors which measure state variables and transmit these measurements to a controller acting on this information and adjusting process parameters (see Figure 4). This control architecture relies on flawless, continuous communication. Networked control systems are often handicapped by packet delays or losses. Poor network performance can even lead to continuous packet loss. To remedy this problem, Liu, La Muñoz de Peña, Ohran, Christofides, and Davis (2010) proposed a two tier architecture incorporating synchronous and asynchronous protocols for controlling chemical processes. A low level Controller is part of an inner control loop based on a point-to-point communication, a high level controller receives synchronous and additionally asynchronous information and acts on it. Liu et al. (2010) argue that “the two-tier control architecture takes advantage of both the continuous and asynchronous measurements to improve the performance of the closed-loop system while guaranteeing that the stability properties obtained by the lower tier controller are maintained.”. Figure 4 shows a simple loop control architecture and the tow-tier architecture. For simplification, actuators by which controllers control the process are not shown.


Process
Sensors
Controller
Process
Sensors
Low-Level Controller
High Level Controller
Point-to-point Communication Links:
Continuous measurements, information flow
Networked Communication:
Asynchronuous measurements, information flow

Simple loop control

Two-tier architecture

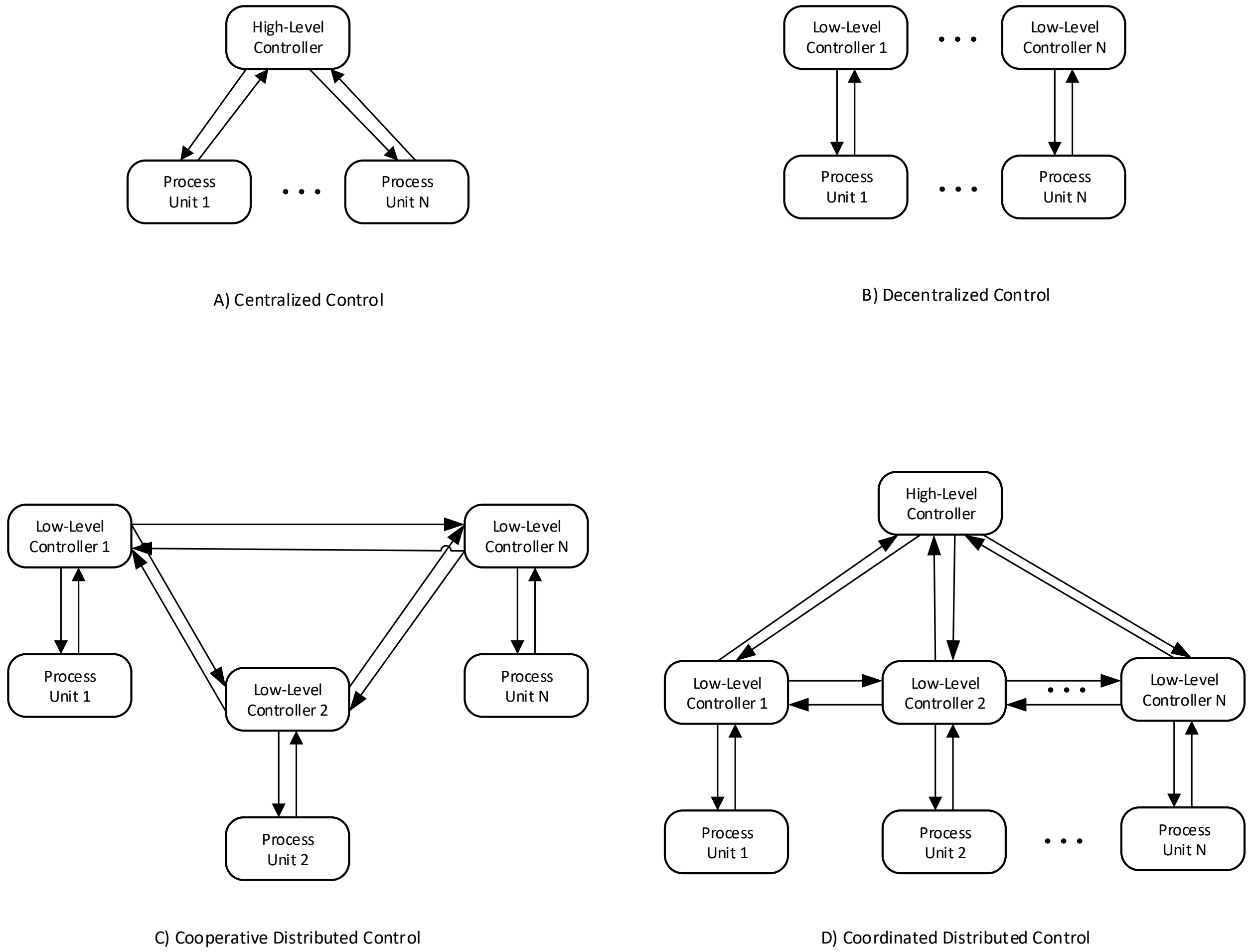
Figure 4 Simple loop, two tier architecture (Liu et al., 2010)

Decentralized, multivariable control or and more recently distributed control are different approaches to tackle this problem. In a centralized control model, the whole plant is regarded as a unique complex system and a single, central multivariable controller coordinates all processes. The disadvantages of this approach are multifold: as the complexity increases, the difficulties with correct model design multiply and the computational effort builds up exponentially. Failure of a single sensor may introduce severe disturbances and deteriorate plant stability. (Bakule, 2008; Jogwar & Daoutidis, 2017) . .” The implementation of this method yields a star network topology.

In a decentralized control method, each process unit is controlled by a single controller without knowledge of the actions of the plants remaining process units. Seck and Forbes (2012) states that while the advantages of an decentralized control system - operability, resiliency, maintainability, flexibility and reliability are remarkable, that this approach leads often to poor performance or operational safety issues. Jogwar and Daoutidis (2017) claim that “as an integrated network involves coupling between various sections of the system, control of individual sections, as in the case of decentralized control, is generally not effective. These individual regulatory loops are frequently activated owing to disturbance propagation through coupling channels.” From a network’s point of view this represents a fully connected network.

Seck and Forbes (2012) argue that “the current interest in distributed control systems is therefore driven by the desire to merge the benefits of decentralized control with the higher performance that may be achieved via centralization”. The distributed control approach divides the process system into subsystems. For each of these process subsystems an information connection to a controller is established and all distributed controllers are communicating with each other over a communication network. (Bao & Xu) (2012), Ydstie (2002). The decisions of one controller are computed by using the local sensor output in conjunction with information received from other controllers. One disadvantage of enhancing control networks to distributed control is that bandwidth for information flow has to increase considerably, that the computational complexity is higher and that due to increase network traffic delays or loss of packets may result. Advantages of using distributed, autonomous controllers are reliability, resilience, flexibility and maintainability. Failure of some controllers do not lead to plant shutdown, changes in some controllers do not necessitate plant redesign. Distributed control systems can be divided into cooperation and coordination-based networks. While the former is based on the fully connected network scheme, the later are based on the star scheme. In cooperation-based networks each process control unit has its own performance goals and is in competition with other controllers for resources leading to a Pareto or Nash equilibrium. The communication between controllers require significant bandwidth capacity. Coordinated control strategies introduce a coordinator which mediates between controllers and acts as a central moderating controller. Coordinated distributed control is reported suitable to replace centralized structures due to the same control performance as centralized control and the advantages of reliability and resilience. (Seck and Forbes, 2012). Liu et al. (2010) introduced a two tier control architecture for non-linear process systems with synchronous and asynchronous sensing and actuation. Tippett and Bao (2015) state that distributed control structures are more suited for flexible manufacturing than older control structures. Heidarinejad, Liu, La Muñoz de Peña, Davis, and Christofides (2011) propose in their study on handling communication disruptions in distributed networks, a distributed model predictive control design incorporating stability constraints for all controllers and a controller responsible for network stability. Vasudevan and Rangaiah (2012) propose several performance measures for plantwide control systems. The total variation in manipulated variables is an indicator of the control effort required for restabilising process variables after disturbances

Figure 5 depicts the different control architectures. In centralized control all communications rely on a central node (Figure 5 A), in decentralized control controllers have no knowledge of other controller's actions (Figure 5 B). In a cooperative distributed control architecture, all controllers are heavily connected, but the resulting network traffic is burdensome (Figure 5 C), while in a coordinated distributed control, the advantage of distributed control is increased by a higher-level controller (Figure 5 D).



A) Centralized Control

B) Decentralized Control

C) Cooperative Distributed Control

D) Coordinated Distributed Control

Figure 5 Control Architectures

Lee et al. (2015) propose a 5-level architecture for developing and deploying CPS (see Figure 6). The architecture relies at its lowest level on smart communication for acquiring reliable data. The transformation from data to information based on algorithms is the next layer. The next level is the cyber-level where information from connected sensors is received and processed to build a machine network. On the cognition level processed information is provided to experts for decisions. The highest level is the configuration level which acts as supervisory control to make machines self-configure and self-adaptive by relaying back data from the cyber system to the real world.

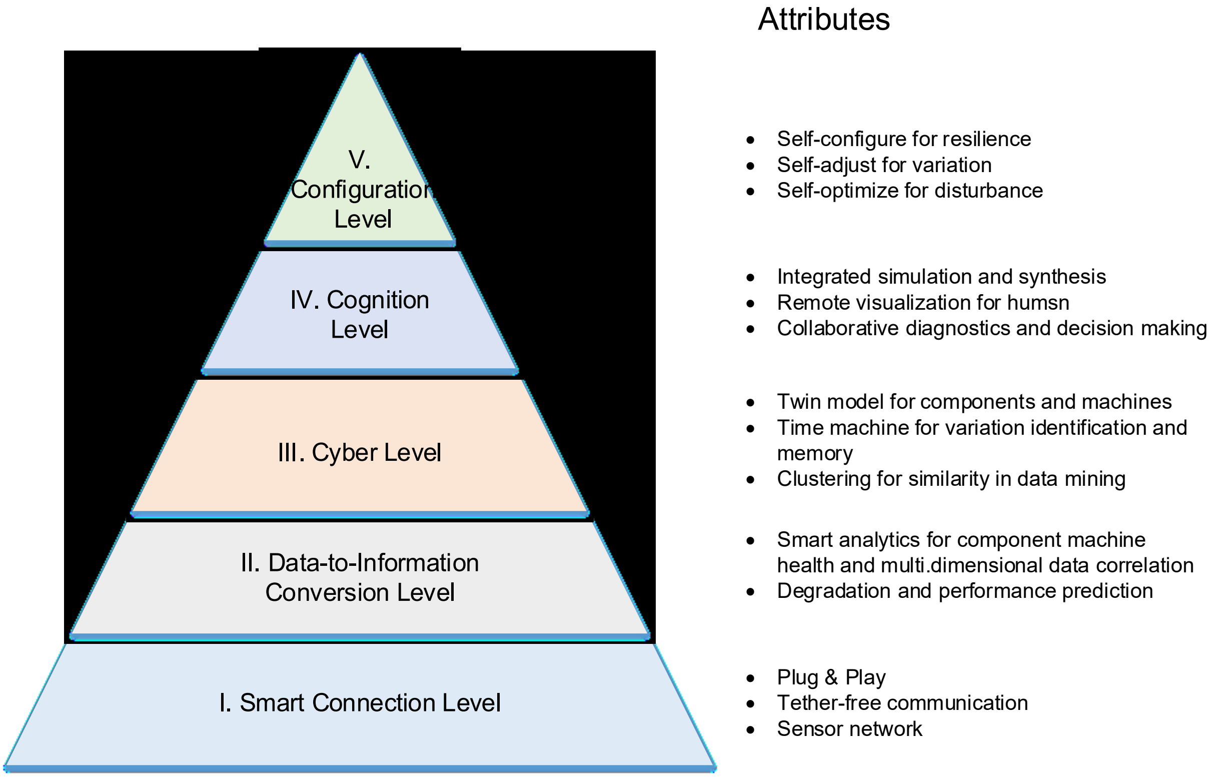

Attributes
V. Configuration Level
IV. Cognition Level
III. Cyber Level
II. Data-to-Information Conversion Level
I. Smart Connection Level
Self-configure for resilience
Self-adjust for variation
Self-optimize for disturbance
Integrated simulation and synthesis
Remote visualization for humsn
Collaborative diagnostics and decision making
Twin model for components and machines
Time machine for variation identification and memory
Clustering for similarity in data mining
Smart analytics for component machine health and multi.dimensional data correlation
Degradation and performance prediction
Plug & Play
Tether-free communication
Sensor network

Figure 6 5C architecture for implementation of Cyber-Physical System. Adapted from Lee et al. (2015)

2.2 Chemistry 4.0

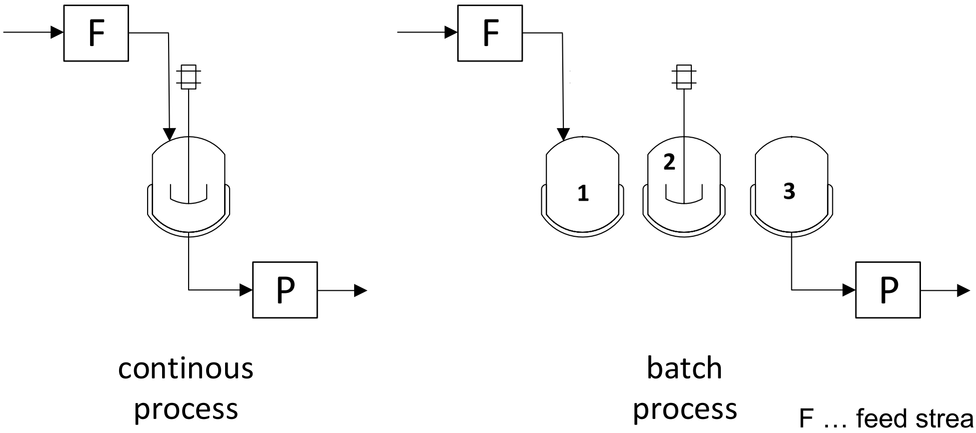
2.2.1 From Chemistry 1.0 to Chemistry 4.0

While the concept of Chemistry 4.0 is congruent with Industry 4.0, the terms Chemistry 1.0 to 3.0 do not correspond to the first three industrial revolutions. Starting in the second half of the 19th century, Chemistry 1.0, then known as the Gründerzeit, was characterized by inventors, who developed industrial scale processes. Fertilizers, synthetic dyes, soaps and pharmaceuticals were the main products. Raw materials were coal and oils and fats derived from animals and plants. After the second world war, Chemistry 2.0 used oil as raw material. Large scale plants were built to profit from economies of scale. Polymers, plastics and fibres were main products. In the late 20th century, pharmaceuticals and specialty chemicals complemented the product portfolios of chemical companies. Globalization, outsourcing and concentration on core businesses, as well as growing investments in environmental protection, mark this period of Chemistry 3.0. Next evolution – Chemistry 4.0 – will be influenced by digitalization and sustainability (Verband der chemischen Industrie e.V., 2016).

In their paper on key industry 4.0 applications in the chemical sector, van Thienen, Clinton, Mahto, and Sniderman (2016) argue that to improve productivity and reduce risks in business operations, smart manufacturing, with its core elements predictive asset management, process management and control, safety management and production control and supply chain planning, with safety management and demand forecasting are key transformations for future development in the chemical industry. Predictive asset management, often termed predictive maintenance, relies on smart equipment collecting and exchanging sensorial data and analyzing them. In a later chapter predictive maintenance is elaborated further. Process management and control will profit from readily available sensorial data, leading to improved control over batch uniformity and quality by reducing process variability. Safety management in smart manufacturing concerns the safety of all stakeholders during the product life-cycle. Production simulation is useful for training operators and helping in planning plants. Supply chain visibility tracks locations and conditions of chemicals during transport. This communication between the different stakeholders leads to improved supply chain planning and safe transport of perilous substances. Demand forecasting relying on predictive analysis along the whole supply chain help companies to plan their production capacities.

2.2.2 Process Control and chemical reactions

A chemical reaction is a process or interaction between two or more chemical compounds, the reactants, to produce one or more different chemical substances, the products. There are two types of reaction control – batch and continuous process control. In a continuous production, raw materials are charged constantly. The following reaction and separation of reaction products is also performed in a continuous manner. Typically, continuous process control is used in high volume productions such as refineries. Advantages associated with continuous production are reduction of waste, inventory and transportation costs as well as increased productivity and stability. Often the requirements on the products do not allow the use of continuous processing. In these cases, chemical batch processing is used – a discontinuous, charge-wise production method. Characteristics attributed to batch processing are smaller quantities, higher selectivity and high value specialty chemicals.



F … feed stream

Figure 7 Continuous and Batch-Processing

P … product stream

As can be seen in Figure 7, in continous processing, the feed stream F is charged simultaneously, while the product stream P is discharged from the process. In batch processing the stream Feed F is charged before the start of the reaction (1), then processed (2) and discharged at the the of processing (3). In batch processing, essentially all relevant reactors are started and stopped frequently (i.e. in a cycle-mode) for charging, processing for a specified period of time and shutting down and draining (discharging). In most cases, the equipment must be cleaned before the cycle is restarted. This study restricts itself to the batch process.

In most reactions, not only the main product, but also side products can be found. In a hypothetical reaction, compound A, which is contaminated with compound X, reacts with compound B. Also, the product C and compound X react with B to a lesser degree. Depending on the exact reaction conditions an almost pure product C or almost pure byproduct 1 can be produced as well as mixtures of product C and byproduct 1, with differing impurities of byproduct 2. These reactions can be formally described as follows:

$$A + B \ \rightarrow Product\ C$$

$$A + C \ \rightarrow ByProduct\ 1$$

$$X + B \ \rightarrow ByProduct\ 2$$

Reaction condition which influence the reaction control are temperatures, concentrations, purities of the used materials, available equipment and handling routines. Small deviations from the established processing routines can well result in charges with high impurities, lower reaction turnover, unsuitable for selling or worse, resulting in circumstances with potential disastrous environmental outcomes, like explosions, fire or contamination with toxic substances. By carefully selecting reaction conditions and monitoring them closely, it is possible to limit impurities and avoid financial losses or disasters.

2.2.3 Control Structures

Historically chemical products varied in their specifications from batch to batch and had to be blended for delivery to reach a consistent degree of purity, resulting in additional costs. Nowadays customers expect products delivered on time, with nearly identical specifications over all shipments. These market driven requirements result in a difficult production environment. Process control systems which can produce the required product quality, while minimizing costs are the focus of research. Engell (2006) argues that “profitable agile operation calls for a new look on the integration of process control with process operations”. Tippett and Bao (2015) describe process control networks as “two interacting networks: a process network interacting via mass and energy flows, and a controller network interacting via information flows”.

In his widely recognized article “Control structure design for complete chemical plants”, Sigur Skogestad describes a control system divided into separate layers and their corresponding time scales. His main achievement is the introduction of hierarchical layers, incorporating self-optimizing controls. He claims that the “main issue with self-optimizing controls is not to find the optimal setpoints, but rather to find the right variables to keep constant. A loss results when we keep a constant setpoint rather than reoptimizing when a disturbance occurs” Skogestad (2004) Figure 8 shows ich control hierarchy. The regulatory layers main purpose is stabilization of the production flows in as far as locally controllable disturbances are concerned. On the supervisory control layer, output is controlled by adjusting the setpoint of the regulatory layer. The purpose of the local optimization layer is to “identify active constraints and compute optimal setpoints for controlled variables” (Skogestad, 2004).

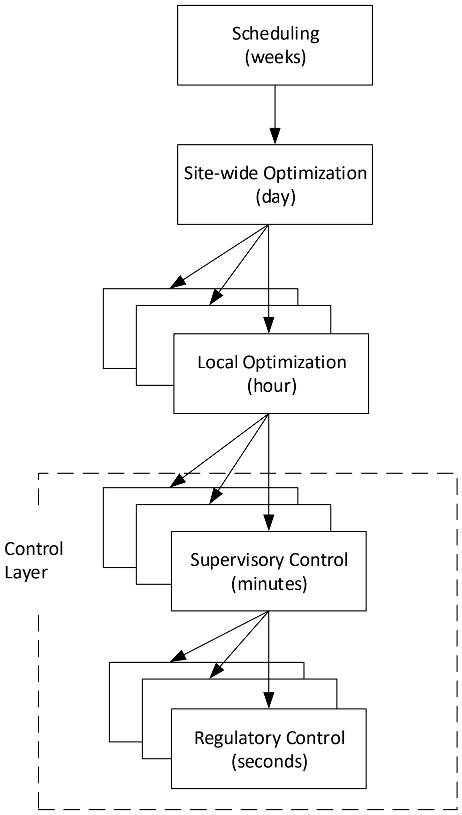

Scheduling (weeks)
Site-wide Optimization (day)
Local Optimization (hour)
Control Layer
Supervisory Control (minutes)
Regulatory Control (seconds)

Figure 8 Typical Control Hierarchy in Chemical Plants

Skogestad proclaims that the complexity of the regulatory layer should be low. Engell (2006) remarks that “ … from a process engineering point of view, the purpose of automatic feedback control (and that of manual control) is not primarily to keep some variables at their setpoints as well as possible or to nicely track setpoint changes but to operate the plant such that the net return is maximized in the presence of disturbances.” Supervisory control on the other hand can be quite complex. Skogestad (2004).

2.3 Digitalization Maturity Level

To differentiate between alternative stages of digitalization and the resulting implications for chemical plants, maturity models can be useful for categorization. Michael Kohlegger, Ronald Maier, Stefan Thalmann (2009) argue that maturity models show facets of reality, useful for classifications. These models normally incorporate dimension and level axis. Levels are attributed to stages or degrees of maturity, dimensions are associated to capabilities. Gökalp, Sener, and Eren (2017) examine different approaches to maturity models for industry 4.0 and propose a maturity model using an approach based on Software Process Improvement and Capability Determination SPICE (ISO/IEC 15504). Their model was adapted for this research.

2.3.1 Levels – Capability Dimensions

The transformation from analog production to smart manufacturing happens in stages. For each aspect dimension, capabilities are assessed. This study adopts levels proposed by Porter and Heppelmann (2015). Levels follow a sequence starting from no adaption to autonomy. A higher-level is built upon lower levels. Table 2 describes these levels in relation to the aspects as seen in 2.3.2

Table 2 Maturity Model - Capability Dimensions

Capability level	Label	Description of Capability level
Level 1	No adaption	There is no implementation
Level 2	Monitoring	Can monitor and observe itself and environment and report in real-time
Level 3	Control	Controlled by software, remotely or embedded.
Level 4	Optimization	Operations are optimized by algorithms and bigdata. Predictive Maintenance is incorporated.
Level 5	Autonomy	Autonomous operation, self-coordination and self-diagnosis enabled.

2.3.2 Aspect Dimension

The aspect dimensions are taken from the maturity model proposed by Gökalp et al. (2017) Table 3 describes the Aspects dimensions used in this thesis.

Table 3 Maturity Model - Aspect Dimensions

Aspect	Description of Aspect
Asset Management:	IT-resources and services of the organization, networked systems, security issues in regard to IT Systems
Data Governance:	Data collection, data analysis, big data allowing real-time decisions on operations
Process Transformation	Transformation of core processes i.e. planning, production, sales, distribution. Horizontal and vertical integration of electronic processes.

2.4 Maintenance

Maintenance of a plant plays a vital role in the long-term behavior of the complex system chemical factory. Lee, Ghaffari, and Elmeligy (2011) state that “Modern engineering systems and manufacturing processes are becoming increasingly complex, and are operating in highly dynamic environments. Thus, sustaining the reliability of such systems is becoming a more complex and challenging requirement.” The critical importance of maintenance is described by Popovic, Vasic, Rakicevic, and Vorotovic (2012): “In an industrial plant, the level of maintenance provided to individual equipment is directly related to the availability that is expected from it. Thus, it is hoped that the most critical equipment will not fail or, at least, that any failure will be rapidly detected and corrected in the minimum time possible.” The element maintenance and strategic and operational processes are connected via a feedback loop (Jokinen, Ylén, & Jouni, 2011). Figure 9 depicts this relation between maintenance, equipment degradation and production. Figure 10 depicts a causal diagram argument for the effects of loop monitoring, showing that continuous loop monitoring can result in higher availability and lower maintenance costs.

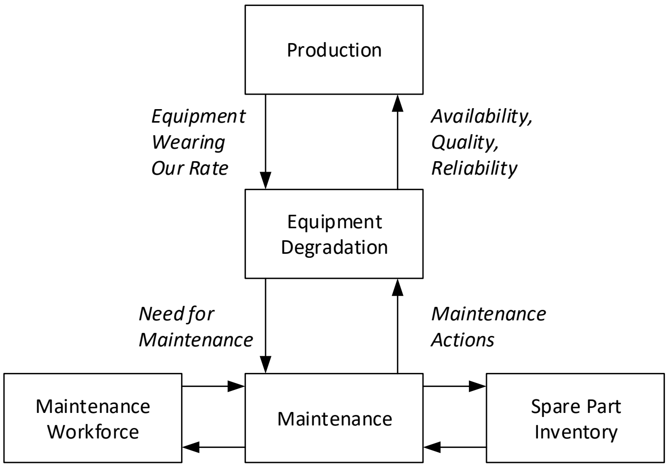


Figure 9 Maintenance model (Jokinen et al., 2011)

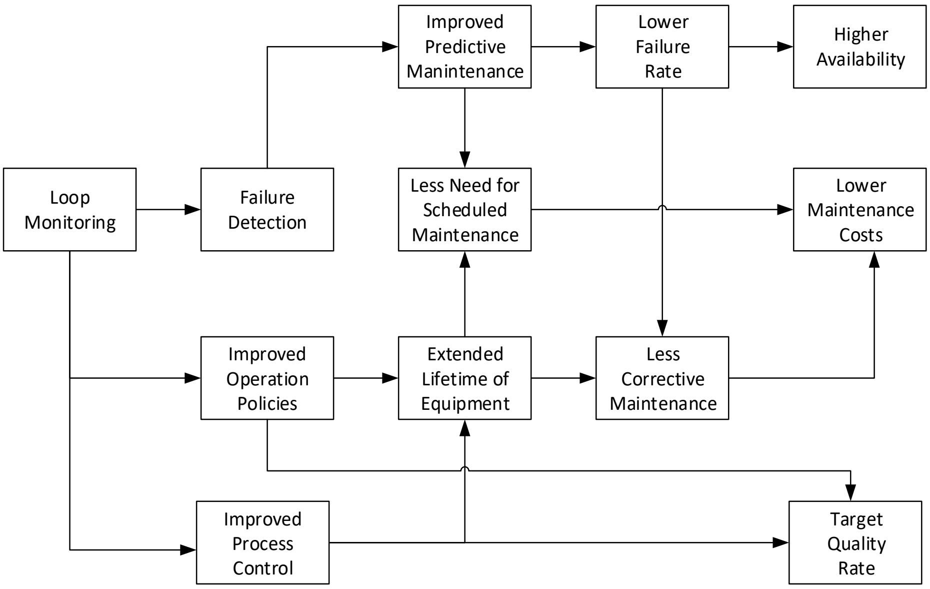

Improved Predictive Manintenance
Lower Failure Rate
Higher Availability
Loop Monitoring
Failure Detection
Less Need for Scheduled Maintenance
Lower Maintenance Costs
Improved Operation Policies
Extended Lifetime of Equipment
Less Corrective Maintenance
Improved Process Control
Target Quality Rate

Figure 10 Effects of loop monitoring service (Jokinen et al., 2011)

Failures are usually unforeseeable, so planning repairs and consequently the material and personnel used, is difficult. Failures may spread to other machinery and hamper seriously the primary operations of production. Hester, Collins, Ezell, and Horst (2016) describe " … the oldest and most common maintenance and repair strategy is fix it when it breaks. The appeal of this approach is that no analysis or planning is required."

Generally, maintenance can be divided into two categories: corrective and preventive maintenance. While corrective maintenance is done after a components failure, the goal of preventive maintenance is to avoid the breakdown of machinery. Corrective maintenance can be divided into immediate maintenance carried out immediately after the fault detection, while deferred maintenance is delayed. An additional approach besides the already mentioned, is aggressive maintenance, like total productive maintenance, focusing on design changes to equipment (Swanson, 2001). Preventive maintenance is routine maintenance intended to prevent unplanned shutdowns. It is conducted before an actual problem arises. Line check-ups and technical audits are routinely employed to prevent failures. Its goal is to maintain proactively and to minimize downtimes. Preventive maintenance can be divided into predetermined maintenance, which is carried out at predetermined intervals, condition-based maintenance, based on monitoring certain parameters, predictive maintenance resting on forecasts of degradation based on analysis and opportunity maintenance, where shutdowns or other maintenance periods are used to carry out maintenance on parts not necessarily to be replaced. Predictive maintenance is one of the core concepts of industry 4.0. Using sensory measurements of its machinery, big data, control loops and analyzing services, plans for maintenance are deduced. Predictive maintenance capable of pre-empting failures, while maximizing life expectancy and minimizing shutdowns for repairs(Jokinen et al., 2011).

Figure 11 shows a classification attempt on maintenance ontology.

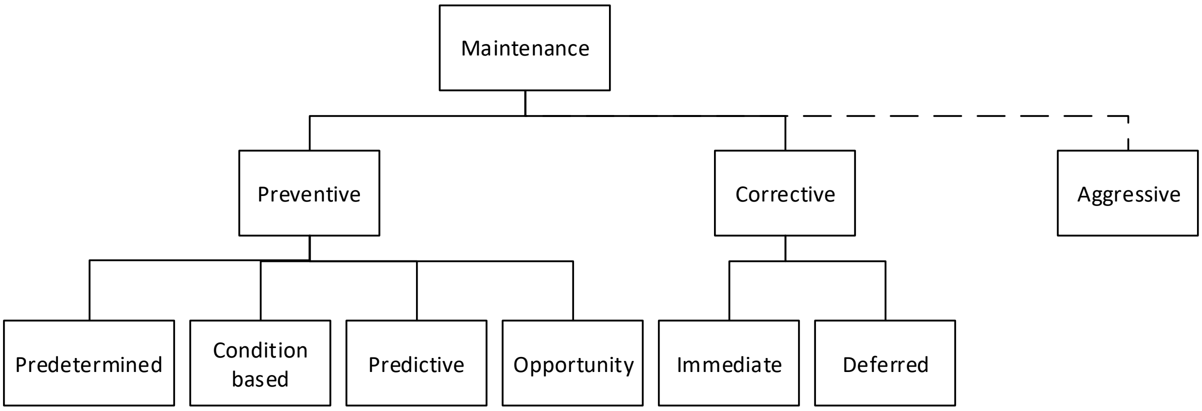


Figure 11 Maintenance Ontology (Jokinen et al., 2011)

In a study to find correlation between aggressive, preventive and corrective maintenance and the effects on product quality, equipment availability and production costs, Swanson (2001) found that while corrective maintenance had negative effects, both other strategies had positive effects. While the study focused mainly on the metal working industry, its implications should be applicable to the chemical industry. Table 4 shows the results of this survey analyzing 287 responses from plant and maintenance managers.

Table 4 Results of regression analysis of maintenance strategies on maintenance performance (Swanson, 2001)

	improvement of product quality	improvement in equipment availability	reduction in production costs
aggressive maintenance	0,253	0,136	0,236
preventive maintenance	0,194	0,212	0,183
corrective maintenance	-0,112	-0,107	-0,115

Lee et al. (2011) introduce the term engineering immune system: “The main idea is to design highly reliable systems that are: capable of surviving any disruptions without serious failures and have the capability to resist disturbances while maintaining their stability. ” It is based on autonomic computing, fault tolerant control systems and self-maintenance. Necessary qualities for autonomous computing are self-configuration, self-healing, self-optimization and self-protection, terms closely related to Industry 4.0.

3 RISK AND IT'S ASSESSMENT

As this work investigates the changing risks involved with implementation of industry 4.0, we should understand the definition of risk and which methods are currently employed to assess risk.

The ISO 31000:2009 norm "risk management guidelines on principles and implementation of risk management" serves as a guide for risk management. It is offering an overall concept for dealing with risks. The risk management process is based on the Deming PCDA (Plan Do Check Act) cycle and a typical risk assessment procedure with feedback cycles (see Figure 12).

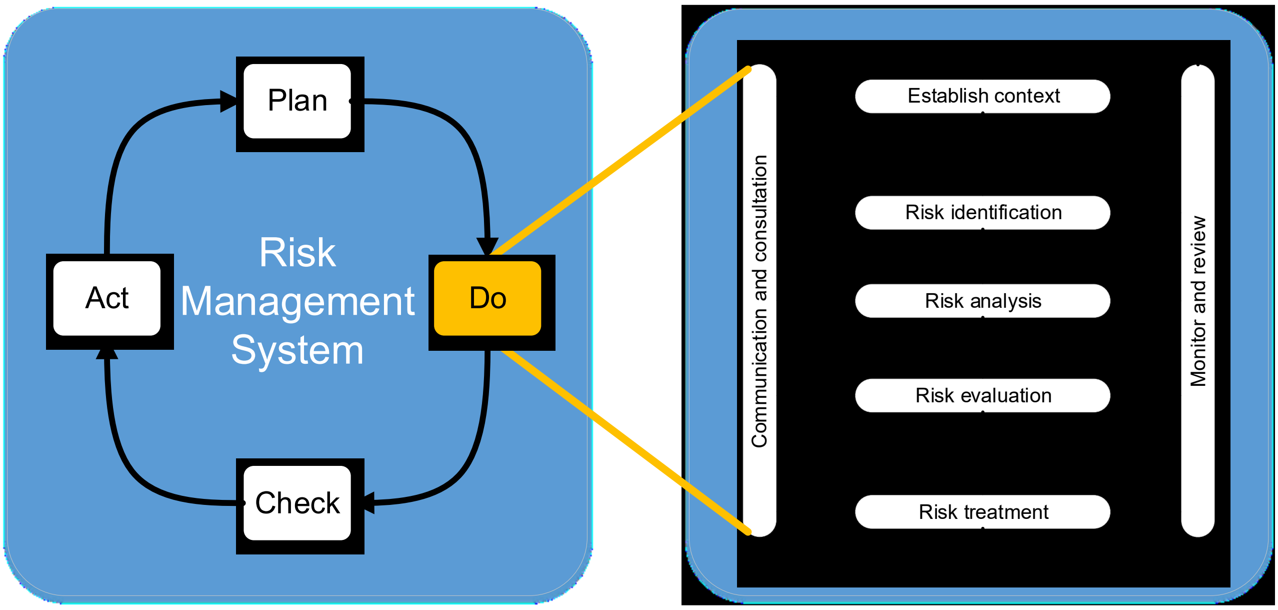


Figure 12 Risk management process (based on ISO 31000:2009)

This study follows partly the ISO 31000 risk assessment procedure as depicted in Figure 12. While the ISO 31000 is described as some improvement over previous norms, some criticism focuses on its definition of risk. Risk is no longer chance or probability of loss but is interpreted as an effect of uncertainty on objectives. To allow positive and negative consequences. In his criticism of the ISO definition Aven (2012) states "risk is the effect of uncertainty on objectives. But what does this mean? Risk relates to uncertainty, but is it the effect of uncertainty? And risk is linked to objectives, but what if objectives are not defined? Then we have no risk?"

This chapter is structured as follows: the first chapter discusses different approaches to risk, the next chapter shows some definition needed, the third chapter relates to risk assessment techniques, the fourth chapter to accident models. The next chapter deals with domino effects, in the sixth chapter dynamic risk assessment methods are discussed. The seventh chapter is dedicated to special considerations needed in in the chemical industry, followed by a chapter dedicated to IT security risks. The last chapter relates to supply chains and demands.

3.1 The meaning of risk and definitions

What does risk mean? As, depending on the context, different interpretations can be found in the literature, there seems to be no agreed upon definition of risk. Necci, Cozzani, Spadoni, and Khan (2015) explain that "When we ask - what is the risk?, we really ask three questions: What can go wrong? What is the likelihood of that happening? and what are the consequences?" Aven (2012) declares risk as "a calculable phenomenon in logic and mathematics, an objective reality in science and medicine, as a societal phenomenon in sociology and as a concept in linguistics". He notes that the definitions for risk changed over time. In the 18th century risk was only related to a potential loss. With the beginning of the 20th century risk was also associated with probability and uncertainty. In the last decades several other approaches were proposed. In his work on historical and recent trends of the risk concept, he recommends nine general risk definitions (see Table 5).

Table 5 Definition of Risks by Aven (2012)

	Risk Definition	Explanation
1	Expected value(Loss)	Risks equals the expected loss Risk equals the expected disutility
2	Probability of an undesirable event	Risk means the likelihood of a specific effect originating from a certain hazard occurring within a specified period or in specified circumstances
3	Objective uncertainty	Risk is a measurable uncertainty. The distribution of the outcome is known.
4	Uncertainty	Risk refers to uncertainty of outcome, of actions and events
5	Potential/possibility of loss	Risk is the potential for realization of unwanted, negative consequences of an event
6	Event estimated frequency (probability) x event consequence	Risk is measure of the probability and severity of adverse effects.
7	Event or consequence	Risk is a situation or event where something of human value (including humans themselves) is at stake and where the outcome is uncertain. Risk is an uncertain consequence of an event or an activity with respect to something that humans value.
8	Consequence / damage /severity of these + uncertainty	Risk is equal to the two-dimensional combination of events/consequences and associated uncertainties (will the events occur, what will be the consequences)
9	Effect of uncertainty on objectives	As defined in ISO (2009). Definition is disputed by Aven (2012) as being not precise enough.

The following definitions are based on the definitions of Rausand (2013), Aven (2012) and (Deutsches Institut für Normung e.V.; Deutsches Institut für Normung e.V.)

Event An event is an incident or a situation materializing in a particular place during a distinct interval of time.

Initiating Event An event that disturbs normal operations of a system and unopposed, may lead to undesirable outcomes.

Hazardous Event The first event in a sequence of events leading to unwanted consequences to some assets.[2]

Accident Scenario A specific sequence of events starting with an initiating event and leading to unwanted consequence.

Probability One can differentiate between several kinds of probability (see Table 6)

Table 6 Different approaches to probability

Classic Probability	$\Pr(E) = \frac{n_E}{n}$
Frequentist Probability	$\Pr(E) = \lim_{n\to\infty} \frac{n_E}{n}$ Where each experiment is repeatable under the same conditions
Bayesian Approach	$\Pr(E\|D_1) = \Pr(E) * \frac{\Pr(D_1\|E)}{\Pr(D_1)}$ Where an individual's belief on the probability of an event is calculated using the prior belief function and additional evidence D_1

Where $\Pr(E)$ is the probability of event E, $n_E$is the number of favourable outcomes, n is the total number of outcomes, $\Pr(E|D_1)$ is the posterior probability, D_1 is additional evidence.

Harm injury or damage to the health of people, or damage to property or the environment.

Frequency the number of occurrences of a repeating event per unit time.

$$\lambda_E = \lim_{t\to\infty} \frac{n_E(t)}{t}$$

λ_E ... the rate of the event E.

Asset An asset is something of value and worth to be preserved, a resource controlled by the entity as a result of past events and from which future economic benefits are expected to flow to the entity

Consequence and Harm A consequence leads to damage to assets.[3] A harm is a physical injury or damage to health or property. There exists a wide range of consequence categories,

[2] Often a hazardous event is defined as „The incident which occurs when a hazard is realized “. This study restricts itself to the view that a hazardous event is „an event that can cause harm “.

[3] Other terms for consequences are adverse effects, impacts or losses.

starting with loss of human life, business interruption losses, loss of productivity, loss of motivation, damage to material assets.

Severity The severity of a consequence can be described in categories like severe loss or major or minor damage. Often it is expressed as monetary value.

Barriers functional grouping of safeguards or controls selected to prevent a major accident or limit the consequences. Barriers can be subdivided into hardware/physical, human, administrative and management barriers. Barriers can be proactive or reactive. Proactive barriers prevent hazardous events, while reactive barriers try to stop event sequences after the hazardous event or reduce the severity of consequences.

Safety performance as risk is closely connected to uncertainty, it does not make sense to speak of risk in the past, as the element of uncertainty is removed in this case. So, safety performance is a summary of hazardous events, their frequencies and accompanying consequences in precise time frame.

Risk influencing factor a relatively stable condition influencing a risk. There can be operational risk influencing factors, organizational risk influencing factors or regulatory risk influencing factors.

Based on these nine risk categories of Aven in Table 5, Villa, Paltrinieri, Khan, and Cozzani (2016) propose a high-level overview probability-consequence diagram, with four distinct priority areas (see Figure 13).

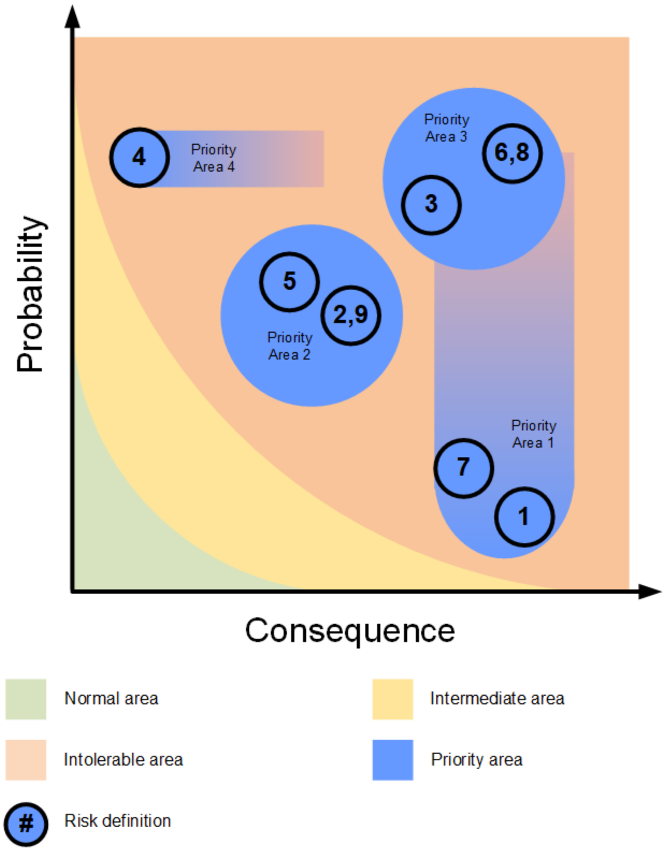


Figure 13 Risk definition and related priority areas (Villa et al., 2016)

In Figure 13 Risks are mapped to risk priority areas depending on the probability and consequences of risk event occurrence. Risk priority area 1 is characterized by reducing the amount of losses, raising the resilience and insurance against consequences, emergency management. Risk priority area 2 relates to preventative measures, emergency management and know how build up. Risk priority area 3 is concerned with risk communication, consciousness building and contingency planning. The high probability of occurrence in risk priority area 4, combined with low impacts, leads to focus on learning effects (Renn & Klinke, 2004; Villa et al., 2016).

3.2 Risk and Accident Models

Risk models help us to understand what influencing factors lead to losses of people, property, environment or quality and teach us how to build better, safer and more resilient systems. While accident models were originally employed to prevent human injuries, they are also a valuable tool to understand the impact of disruptions on business. Toft, Dell, Klockner, and Hutton (2012) describe how accident models evolved in the last century. Starting in early 20th century, simple linear models, where events act sequentially, were employed. Removing one of the causes in the sequence, prevent the sequence leading to the accident. In the second half of the 20th century complex linear models were proposed, arguing that accidents happen if latent hazard conditions meet with unsafe acts. To avoid accidents this school of thoughts recommends barriers to prevent failure propagation. Complex non-linear accidents models propose that the complexity and coupling of multiple causal factors lead to accidents, which can only be examined by investigating the interaction and combination of these factors. Figure 14 shows the emergence of these three different approaches in the past.

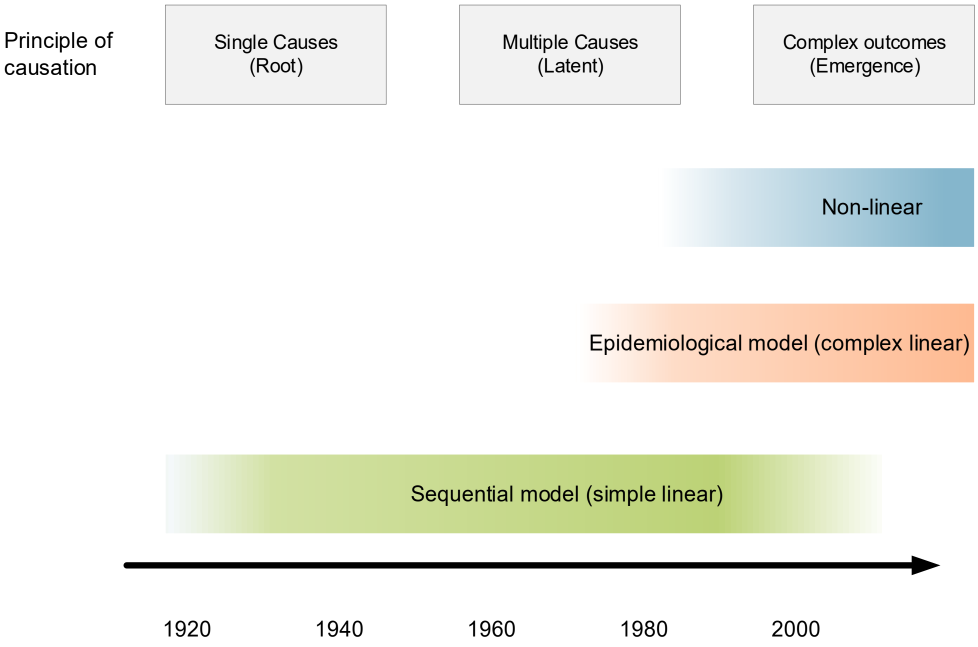

Principle of causation
Single Causes (Root)
Multiple Causes (Latent)
Complex outcomes (Emergence)
Non-linear
Epidemiological model (complex linear)
Sequential model (simple linear)
1920
1940
1960
1980
2000

Figure 14 Summary of a history of accident modelling, Toft et al. (2012)

One drawback of this classification is, that some accident models do not fit into these three categories.

3.2.1 Linear accident models

For simple systems, we are able to understand how things work in terms of cause-effect relations. Heinrich’s Domino model, published in 1931, says that accidents are caused by a chain of events, each event triggering the next one until the accident happens. He proposed five dominoes, social environment and ancestry, fault of person, unsafe act or condition, accident and injury. If one of the dominoes, for example “unsafe condition” is removed, the chain propagation is stopped. To reduce the numbers and severity of accidents, Heinrich advocates engineering efforts, education and training of workers and enforcement of rules and regulations (Heinrich, 1931).

The Loss causation model of Bird, Germain, and Clark (2014) is also based on a chain of events see Figure 15. Usually one starts with the last event – the loss – and propagates step by step backwards, until the steps which led to the loss are identified and the cause is described. The model argues that lack of management control lead to the existence of basic causes like limited training. These basic causes lead in turn to immediate causes, such as unprofessional handling of machines. In the presence of energy or substance, substandard practices and conditions will lead to incidents in an manufacturing environment, resulting in losses (Bird et al., 2014; Storbakken, 2002).

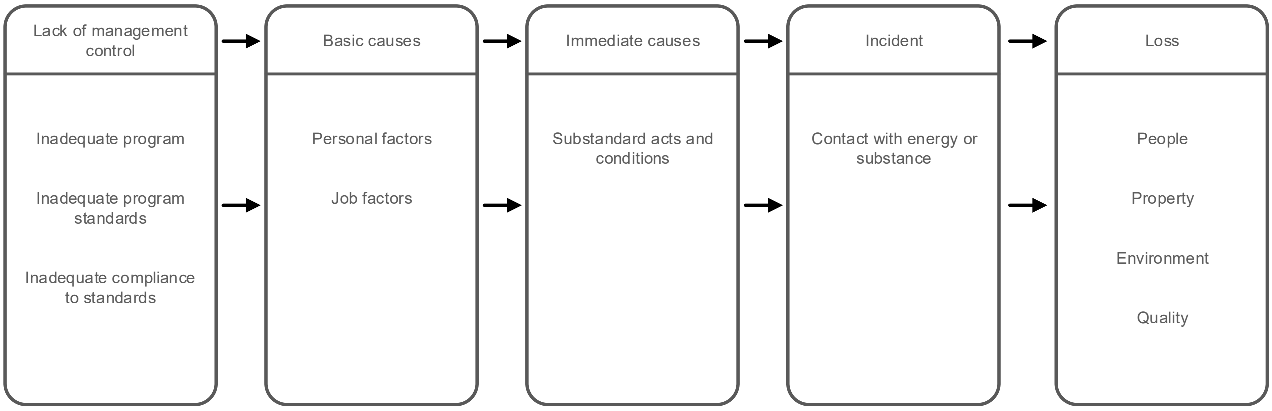

Lack of management control
Basic causes
Immediate causes
Incident
Loss
Inadequate program
Inadequate program standards
Inadequate compliance to standards
Personal factors
Job factors
Substandard acts and conditions
Contact with energy or substance
People
Property
Environment
Quality

Figure 15 Loss causation model (Toft et al., 2012)

Another event causation and sequencing model is the fault tree analysis FTA. As a top-down approach one starts with the undesired top-event and constructs a fault tree. Hardware and software as well as human failures are combined using logic gates. One advantage of the FTA is that by using statistical methods, the probability of the top event can be calculated. Typical metrics used for calculation are failure rates and repair rates (Gryna, Chua, & DeFeo, 2007; Rausand, 2013). In Figure 16 a FTA is done. The top event – a fire breaks out - is only started under the following conditions: a) a spark exists or an employee is smoking, b) the ensuing ignition is near gas and there is a leakage of flammable gas.

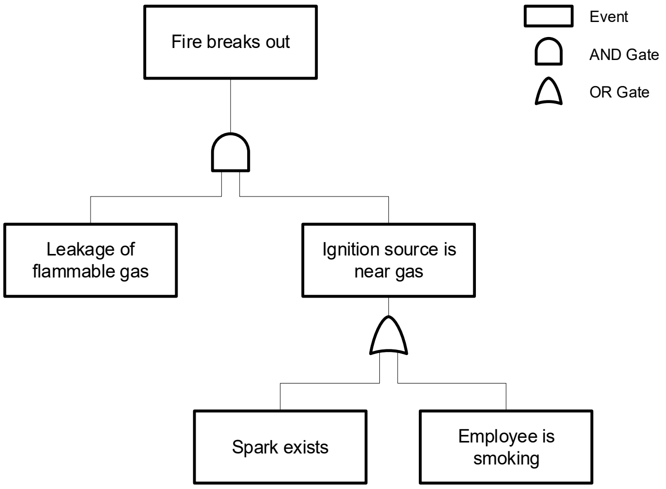


Figure 16 Fault tree analysis

The Failure Modes and Effect Analysis (FMEA) is most suitable for components with well-known failure modes (Qureshi, 2008). The FMEA links potential errors with its causes and its consequences. These cause-effect chains are prioritized by calculating a risk priority number RPN.

$$RPN = Severity\ x\ Occurrence\ x\ Detection$$

One criticism of FMEA is that it cannot take into account multiple or common failure causes. Also its static nature prohibits the consideration of real time data (Qureshi, 2008). Qureshi also argues that, FTA and FMEA, designed as tools for component failures, are not suitable for analysis of sociotechnical systems because they do not take into account non-technical or complex interactions between the system's elements.

The sequential timed events plotting (STEP) method starts with the system in a normal state. A start events disturbs the system and leads to a propagation of events (see Figure 17). Actors can be persons, equipment or substances like halon. They change or control the system. If the actors cannot impede the event chain, it will lead to the undesired end event state, where assets are harmed (Rausand, 2013).

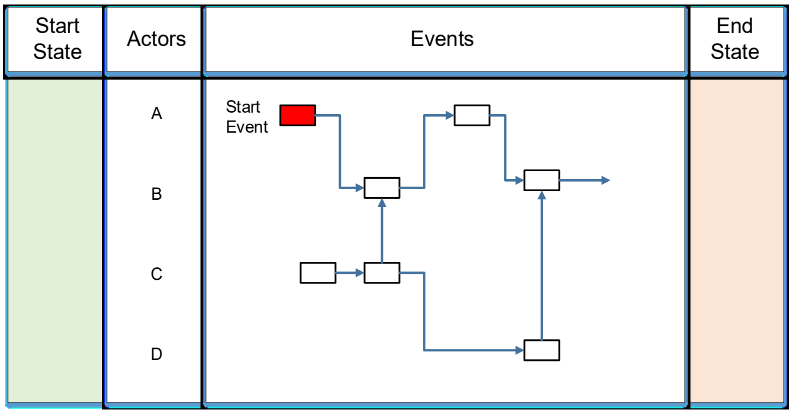


Figure 17 STEP diagram (Rausand, 2013)

Hazard and Operability Study (HAZOP) is a standard tool for risk evaluation the chemical industry, is used to systematically identify errors and operability problems. In expert discussions, the impact of potential deviations for the system, users and environment are investigated (Hyatt, 2004).

Bow-Tie Risk Analysis is another, visually easy to understand, way to construct an accident model. It combines fault end event tree methodologies using a barrier-based approach. At the center of Figure 18 is the hazardous event, it asks the following three questions: a) what can cause the hazardous event? b) What events or consequences could result? And c) which proactive and reactive barriers should be implemented to control the process?

Left of the top event, threats and preventive barriers to reduce the probability of top event occurrence can be found, while on the right side mitigation procedures and barriers try to weaken the impact of the top event, leading to possible consequences.

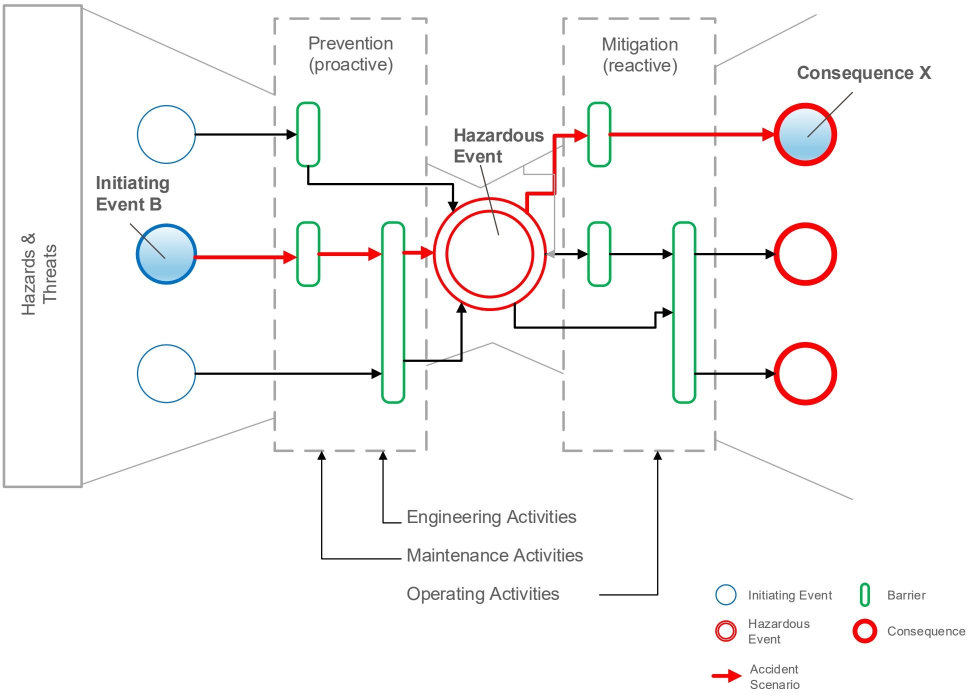


Figure 18 Bow Tie diagram

3.2.2 Complex linear models

The linear accident models focused on identifying the root causes to eliminate or prevent accidents. As the society became increasingly dynamic, Rasmussen (1997) posed the question whether these simple linear accident models were adequate for systems stressed with technological change and aggressive competition. He proposes a system oriented approach combining elements from several disciplines with control theory approaches. Rasmussen argues that in complex socio-technical systems, not every state or condition can be foreseen. He thinks that the safety of such a system is constrained by the unacceptable workload, economic failure and boundary of functionally acceptable performance (safety procedures and regulations). Acting on this system are forces, like pressure on efficiency or campaigns for safety, changing the behavior of the workforce over time (Figure 19). Rasmussen explains that due to management pressure for efficiency and the human trend for least effort, leads the behavior to the boundary of acceptable risk. Actors in the system make decisions, but do not observe or take into account the interaction their decisions have with one's form other actors in the system (Rasmussen, 1997).

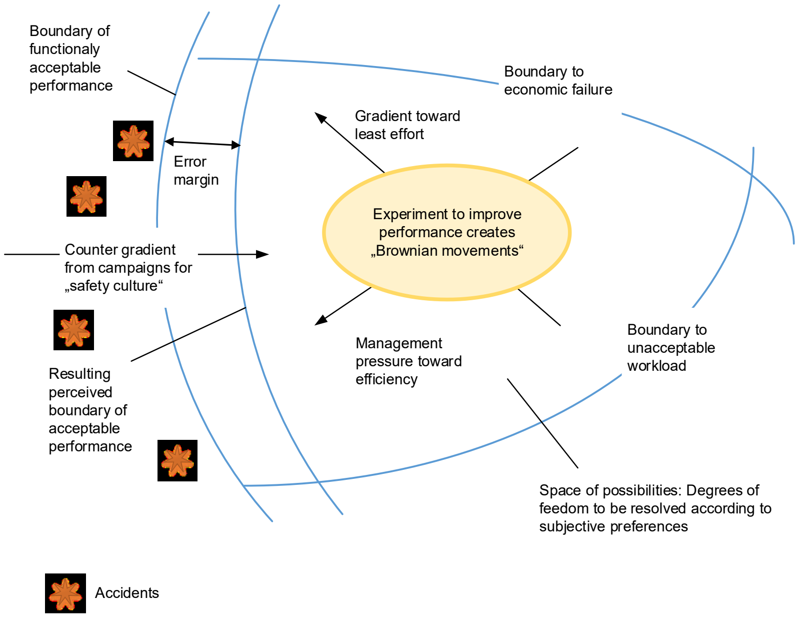

Boundary of functionaly acceptable performance
Error margin
Boundary to economic failure
Gradient toward least effort
Experiment to improve performance creates „Brownian movements"
Counter gradient from campaigns for „safety culture"
Management pressure toward efficiency
Boundary to unacceptable workload
Resulting perceived boundary of acceptable performance
Space of possibilities: Degrees of feedom to be resolved according to subjective preferences
Accidents

Figure 19 Boundaries of safe operation (Rasmussen, 1997)

Reason's Swiss Cheese Model states that an accident can only happen if the causal sequence of an accident is permitted by holes in barriers or defenses (resembling swiss cheese slices). He investigates organizational safety and how barriers can be compromised. Latent conditions like company culture combined with trigger events and active failures (violations of process guidelines) lead to accidents. He differentiates between active errors "where the effect is felt immediately" and latent conditions "dormant in the system largely undetected until they combine with other factors to breach system defenses" see Figure 20 (Reason, 2009).

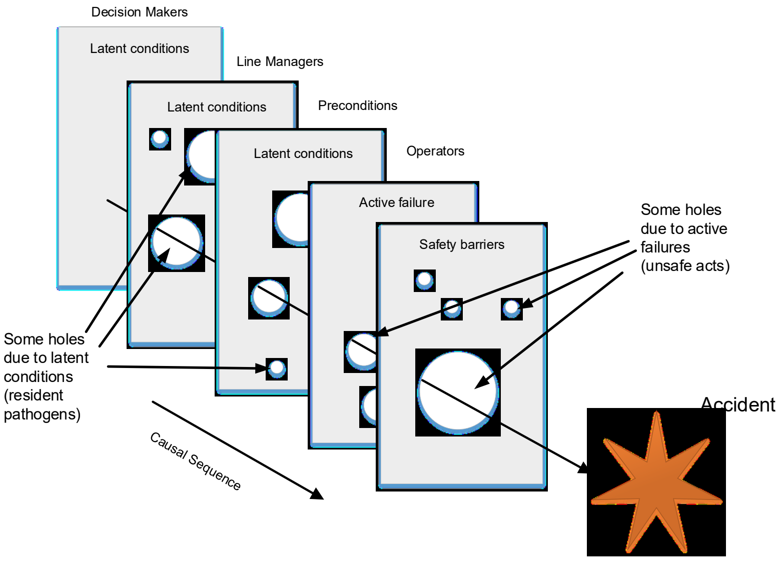


Figure 20 Swiss Cheese Model (Reason, 2009)

Under ideal conditions, no holes are present, so no accident should be possible. Defenses may degrade or be removed intentionally like in Chernobyl. Holes in the defenses do not lead automatically to accidents, only if holes line up along the causal sequence. The Swiss Cheese Model was extended to include event chains leading to holes in barrier layers. This adaption allows Reason's model to include cause paths of failures into the model (Besnard & Baxter, 2003).

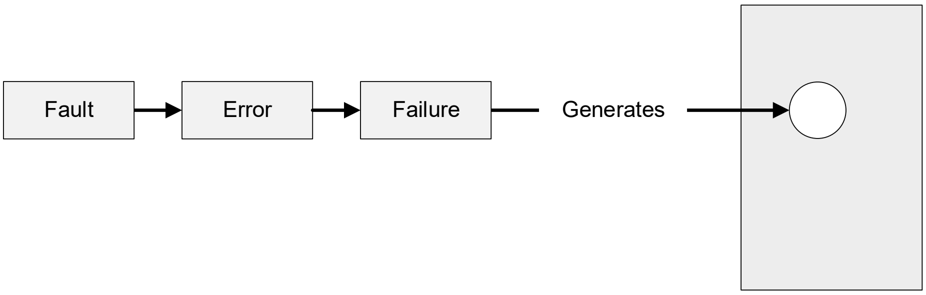


Figure 21 Event Chain generating a hole in a barrier layer (Besnard & Baxter, 2003)

3.2.3 Complex non-linear models

The linear and the complex linear models rely on analytical reduction. This limits their usage in situations where components interact, systemic factors, complexity and indirect and no-linear interactions predominate, factors often attributed to modern socio-technical systems. Another drawback is that they consider systems as static, while in reality, the need to improve efficiency and productivity shifts the system towards greater risk over time. For complex systems there are numerous ways for events and conditions to combine, therefore a lot of risks remain unknown.

In his normal accident theory, Perrow (1984) researched accidents in complex systems and found that complex interactions and tight coupling resulted in higher accident rates. He argues that:

> *"A complex system is composed of many components that interact with each other in linear and complex manners. Linear interactions are those that are expected in production or maintenance sequences, and those that are quite visible even if unplanned (during design), while complex (nonlinear) interactions are those of unfamiliar sequences, unplanned and unexpected sequences, and either not visible or not immediately comprehensible. Two or more discrete failures can interact in unexpected ways which designers could not predict, and operators cannot comprehend or control without exhaustive modelling or test."*

Feedback loops change the way elements of a system react. They can make identification of underlying problems difficult, as they hide symptoms due their inherent nature of positive or negative feedback. Tight coupling between elements of a system mean, that an event in one element effects interacting elements without delay. Rausand (2013) states that " Tightly coupled systems are characterized by the absence of natural buffers and will therefore have little or no slack." Loosely coupled elements have time to react, are more lenient against disturbances. Perrow categorized several sociotechnical systems along these two axes and identified chemical plants as complex systems with tight coupling (see Figure 22). To function properly, tight coupling needs centralized authority, in contrast complex systems require autonomous decision making. These conflicting requirements for tight coupled, complex systems lead to accidents (Perrow, 1984).

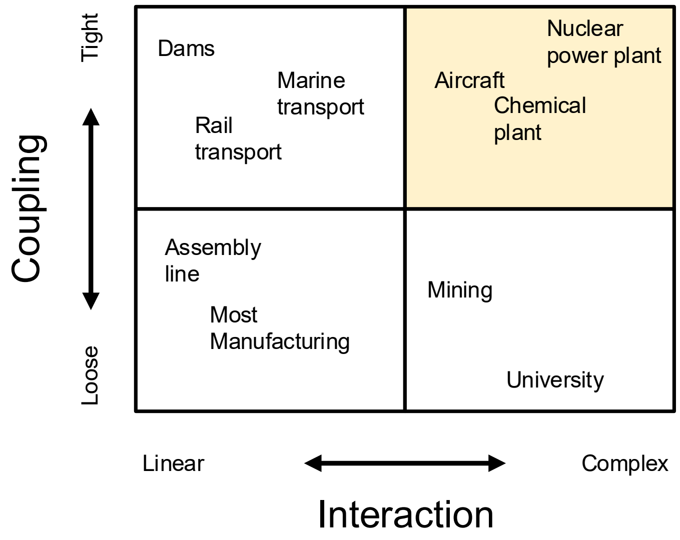


Figure 22 Interactions and Couplings in systems (Perrow, 1984)

The normal accident theory has been heavily criticized as Perrow concluded that some technologies, being not controllable, should be abandoned. Hopkins (1999) claims that it can be applied only on a small number of accidents, that is lacking exact criteria for measuring complexity and coupling and that decision making authority in reality can be both centralized and autonomous, as organizations with high central authority under normal conditions, tend to shift authority to lower levels under pressure.

A new view on risk assessment is the emphasis of system resilience, the ability to compensate or adjust to disturbances or continuous stress. Hollnagel's Functional Resonance Analysis Method (FRAM) uses resilience concepts to explain emerging behaviors of complex systems. Hollnagel states that outcomes are defined more by relations than by factors, performance variability has a higher influence than failure probability. Often failures can be attributed to combinations of performance variabilities of everyday performance. (E.Hollnagl & E.Rigaud, 2006; Hollnagel, 2003, 2006; Hollnagel, Leonhardt, Licu, Shorrock, & S.; Praetorius, Hollnagel, & Dahlman, 2015; Rigaud, Hollnagel, & Pieri, 2008) According to Slifkin and Newell (1998) variability of performance can serve as a measure of success in realizing task goal and they also state that "The characteristics of performance, whether produced by an individual or by different individuals, are never exactly the same, even under the same task conditions." In his article on the performance variability dilemma Matson and Prusak (2003) emphasize the distinction between processes and practices: "while a process outlines how tasks are to be organized, practice refers to the way those tasks are understood and actually performed. And practice is rarely based on narrow definitions that show how to complete a job from A to Z; more often, it stems from stories, principles, heuristics (rules of thumb) and expertise that emerge over time and combine to create a basis for action."

The fundamentals of Hollnagel’s theory are based on four principles:

- The principle of equivalence of failure and success
  One insight of resilience engineering is the realization that “individuals and organisations must adjust to the current conditions in everything they do. Because information, resources and time always are finite, the adjustments will always be approximate “ (Hollnagel, 2006). Performance variability is the cause for successful work and also the reason why things occasionally go wrong. There are no causes that result in failure only.
- The principle of approximate adjustments
  As stated above, performance variability is inevitable as resources as time or information or manpower are limited and uncertain. This lack of resources leads to efficiency–thoroughness-trade-offs[4], where either actions are poorly prepared or in the case of meticulous planning, too little time is left to carry out the action.
- The principle of emergence
  While everyday performance variability is seldom the cause of accidents, the combination of performance variability of multiple functions can lead to emergent, unexpected results.
- The principle of functional resonance
  While „stochastic resonance is the enhanced sensitivity of a device to a weak signal that occurs when random noise is added to the mix. Functional resonance is the detectable signal that emerges from the unintended interaction of the normal variabilities of many signals.”

The basic element of the model is a characteristic function, not a system structure or physical unit. A function may be an engineering function relating to processes of a technological system, or a human function, describing necessary task for people to achieve goals. Figure 23 depicts such an archetypal function. Each function can be connected to other functions through up to six characteristic relationships. (Hollnagel, Hounsgaard, & Colligan, 2014) see Figure 24.

[4] Efficiency and thoroughness are goals which are impossible to maximize at the same time. An increase in thoroughness leads to a decrease in efficiency, while raising efficiency will be accompanied by a decrease in thoroughness. Humans try to reach an optimal balance between these poles. Each individual balance is affected by subjective and personal feelings, culture and social or organizational pressure.

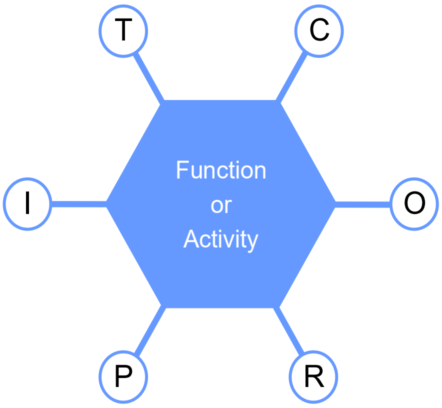


Figure 23 FRAM 6 aspects to a function (Hollnagel, 2003)

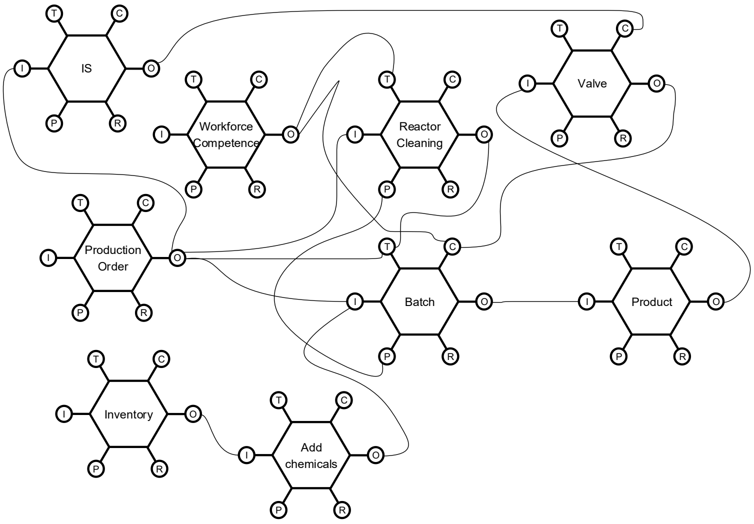


Figure 24 FRAM links

- Inputs (I) are typically that which is used or transformed by the function (energy, matter, information). Other purposes of inputs are the activation of the function and the link to upstream functions.
- Time (T) is a particular resource, usually a time window for the function to be carried out. Time can also be regarded as a control for sequencing functions. Also, time could be interpreted as a precondition. Due to this ternary point of view, Hollnagel created a time
- Controls (C) are controlling elements, supervising and regulating the function. Plans, guidelines or active functions like monitoring or tuning.
- Outputs (O) are the results of the function (energy, matter or information) and provide the link to downstream functions.
- Resources (R) are necessary resources, like manpower, energy, competences or procedures, to create the output. Hollnagel describes two types of resources - normal resources, consumed by the function and execution conditions available while the function is carried out. Typical normal resources would be solvents in a chemical setting, while execution conditions could be competence or a solid, non-degrading catalyst.

- Preconditions (P) are system conditions which must be met before the function is carried out. Can be considered as binary variables.

Functions can be divided into foreground functions (all aspects should be defined) and background function (only necessary aspects are defined). The idea behind this model is to create a system representation, showing how the system works to accomplish its goals and how the variability of functions affect performance. FRAM modeling does not result in a model showing an actual sequence of events.

For each defined aspect two separate characteristics for the output - precision and time - are evaluated according to Table 7. (Patriarca, Di Gravio, & Costantino, 2017). Different characteristics could also be introduced.

Table 7 Output characterisation for function (Patriarca, Di Gravio et al., 2017)

		Temporal characteristic		
		Too early	On time	Too late
Precision characteristic	Precise	A: output to downstream is too early, but precise	B: output to downstream is on time and precise	C: output to downstream is too late, but precise
	Appropriate	D: output to downstream is too early, but appropriate	E: output to downstream is on time and appropriate	F: output to downstream is too late, but appropriate
	Imprecise	G: output to downstream is too early and imprecise	H: output to downstream is on time, but imprecise	I: output to downstream is too late and imprecise

Each defined aspect is to be valued for its dampening or increasing effect on the variability. This can be done in a linguistic or numerical representation. So the variability of a function can be defined by the function variability itself and the output variability characteristics of the upstream functions specified by their connection type.

According to Patriarca, Di Gravio et al., the variability of the upstream output j OV_j can be defined as the product of the upstream output score in terms of timing and precision.

$$OV_j = V_j^T * V_j^P$$

$$CV_{ij} = OV_j * a_{ij}^T * a_{ij}^P$$

Where V_j^T represents the upstream output j score in terms of timing, V_j^P represents the upstream output j score in terms of precision, a_{ij}^T represents the amplifying factor for the upstream output j and the downstream function i in terms of timing, a_{ij}^{P} represents the amplifying factor for the upstream output j and the downstream function i in terms of precision.

3.3 Risks related to the chemical industry

The chemical industry is a system of high complexity, dealing with a multitude of partly dangerous materials, difficult operating procedures and complex equipment. The interaction in this system combined with human operators often leads to process deviations. In this environment process deviations are dangerous as they can lead to fatal accidents (Kletz, 2001). Menon, Praveensal, and Madhu (2015) examined job stress and its sources in the chemical process industry, which result in accidents and sickness. Modern chemical factories are even more subjected to risks, as to maximize profits, processes are conducted unter extreme conditions or need extreme flexibility (Zhao, Bhushan, & Venkatasubramanian, 2005). An accident in a chemical factory may well lead to loss of lives in the thousands. The Bhopal disaster is recognized as the worst industrial disaster in history (Kletz, 2001). More than 25.000 people died, over half a million people were injured.

3.4 Risks related to IT security

As digitalization of production networks increases, the need for improved cybersecurity is evident. Stuxnet and flame crippled Iranian centrifuges for separating nuclear material. These attack vectors targeted programmable logic controllers, allowing control of machinery on factory assembly lines (Piggin, 2011). In 2014, hackers got access to the office software of a steel company in Germany. Using this as starting point, they gained control of the production management software and consequently almost complete control over the factory's systems. The human computer interfaces were destroyed, emergency procedures were intercepted, resulting in physical destruction of a blast furnace. (Lee, Assante, & Conway, 2014).Ahlan and Arshad (2012) state that the more businesses depend on IT, the more they are subjugated to IT risks. Hackers and intruders and administrators and soft- and hardware vendors are in a constant battle, with an inherent advantage to the attacker. Gerace and Cavusoglu (2009) argue that "Today most security incidents are caused by flaws in software, called vulnerabilities. It is estimated that there are as many as 20 flaws per thousand lines of software code" and "… the sophistication of attack tools has also advanced over time. Using the interconnected nature of the Internet and automated attack tools, attackers exploit software vulnerabilities at an alarming rate to cause serious damage to organizations."

Ilie-Zudor, Kemény, and Preuveneers (2016) categorize threat to networked production systems into three categories.

- Human decisions and social engineering – over 90% of cyberattacks begin with some sort of social engineering as humans are recognized as the weakest link in the cyber defence chain.

- Intercepting and injecting information – getting access to or modifying confidential information such as trade secrets, intellectual property, strategies and customer information. Due to the connectivity of industry 4.0, access at this layer allows also control of physical systems.
- Aggregation and inference attacks – aggregation means that information is collected to get an overview of the whole system, while inference means using the aggregated information to attack the system.

In his paper, Tzezana (2017) analysed potential methods for crimes and attributed likelihood factors to attack methods. The most likely attack vectors were (in increasing order): An inside man, mass attacks by hacking groups, botnets, social engineering and Distributed-Denial-of-Service DDOS attacks.

Not all IT risk are related to attackers. As early as 1982, Kletz (1982) wrote in his article about human problems with computer control: “Computers do not create new sorts of errors. They merely provide new and easier opportunities for making the old errors.” He identified four categories of failure incidents and added in a later paper three additional causes of failures (Kletz, 1991).

- Hardware faults – hardware and equipment attached to computers are not always working as intended.
- Software failures - McConnell (2009) estimated that well-written code contains one bug per 1000 lines of code.
- Treating the computer as a black box – not knowing what instructions the software send to the computer, leads to insufficient behaviour and different conditions. Kletz (1991) mentions an accident, where due to ending of summertime, when an operator changed the time of the computer and the computer shut down the factory.
- Misjudging the way operators will respond to the computer – the human-machine interface, often overloaded with information, invites for operator errors.
- Entering wrong data – wrong data can lead to false quantities of chemicals added to the batch. An aircraft crash was the result of entering 270° instead of 207° into the navigation system (Kletz, 1991)
- Failure to tell operators of changes in data or programs lead to unintended consequences.
- Unauthorized Interference with Hardware or Software – overriding software or hardware settings by users in good will, result in altered behaviour of the computer system.

4 RESEARCH DESIGN AND METHODOLOGY

A methodical approach was used for this thesis. This study was divided into several phases. The first phase consisted of a literature survey on topics relevant. The results of this literature survey for Industry 4.0 and Chemistry 4.0 were described in chapter 2, the results centered around risk and its management in chapter 3. The results of this survey were then used in the second phase for constructing the base of a multiple case study, i.e. three fictional chemical plants representing three different levels of digitalization maturity.

4.1 Case Study

As, at the time this thesis was written, no Chemistry 4.0 plant was realized and to make comparisons between chemical plants of different digitalization levels feasible, this study uses three fictional chemical plants, differing in their degree of digitalization maturity in a multiple case study.[5] The maturity levels, presented in chapter 2.3 were used to clearly distinguish between the three plants.

- Plant A - the analog plant - can be considered as a plant typically around 1960.
- Plant B - the IT-centralized plant - with central IT-based control, is a plant typically found in the year 1980.
- Plant C - the Chemistry 4.0 plant - describes what a plant might look like in the future.

To distinguish between these plants and to establish their capabilities, the maturity level model described in chapter 2.3 is applied.

- All capability levels for plant A are set at capability level 1.
- In plant B monitoring and controlling of assets and data are realized, but no process transformation has been realized.
- Plant C describes a hypothetical plant were all aspects are fulfilled to the autonomy level.

The average maturity level can be calculated by:

$$Digitalization\ Maturity\ Level = \frac{\sum capability\ levels}{n_{capability\ levels}}$$

This results in plant A having a digitalization maturity level of 1, plant B having a digitalization maturity level of 3, and plant C having a digitalization maturity level of 5 (see Table 8) .In *Figure 25* the capability levels for each aspect for each plant are shown. Then for all plants process

[5] The companies and events depicted in this Case Study are fictitious. Any similarity to any event, corporation, organization and person living or dead is merely coincidental.

maps were constructed and in conjunction with the maturity level model, the boundaries of the investigated system were drawn.

Table 8 Digitalization Maturity Level of Plants

Plant	Digitalization Maturity Level
A	1
B	3
C	5

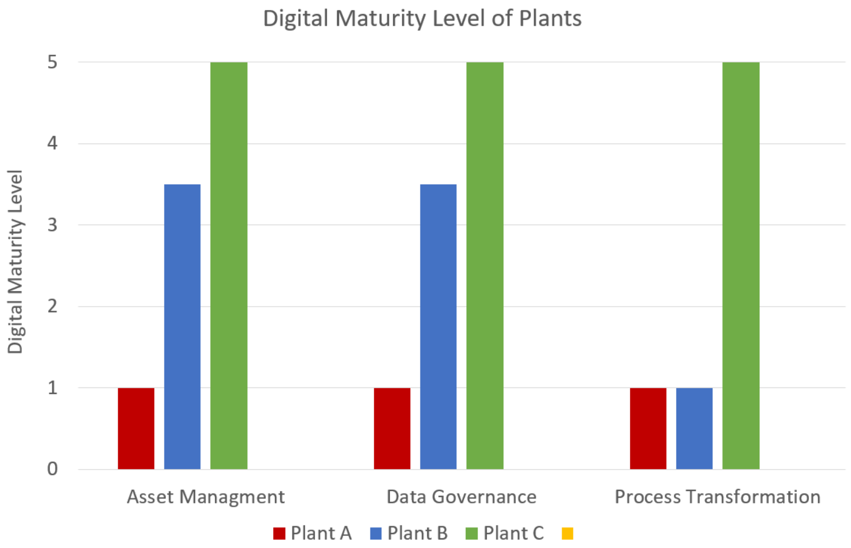


Figure 25 Digital Maturity Level of Case Study Plants

All plants consist of several batch reactors, in all plants the same reaction is carried out. Each reactor system consists of a reactor, a temperature controlling system and an emergency cooling system. The reaction is controlled by the temperature controlling system. At start, the reaction mixture is heated to a certain temperature level, later on the temperature of the reaction mixture is controlled in order to absorb the heat generated by the reaction. In case the reaction is considered to be reaching runaway conditions, a safety system - the emergency cooling system - is activated, in which case the reaction temperature is lowered to 20°C. Chemical workers and operators control the cooling system and the emergency cooling system. The temperature control system and the emergency cooling system are controlled by operators in a control room. Temperature sensors and alarms complete the system. Alarm 1 is set to 90 ± 2 °C, Alarm 2 is set to 105 ± 2°C. This setting is described in the literature and is used as a base for the centralized IT based control plant (Karanki, Dang, MacMillan, & Podofillini, 2018).

4.1.1 Chemical reaction

The system under analysis describes a plant where in a batch reactor an adiabatic consecutive reaction of two steps is carried out. A and B react to C, the desired product, and in a second step

C reacts with A to the unwanted by-product D. Both reactions are exothermic, the distinguish in their reaction rates. The reaction rate of the second step is less than the first one.

$$A + B \ \rightarrow C$$

$$A + C \ \rightarrow D$$

The system under examination is described in the literature (Arpornwichanop et al., 2002, 2002; Arpornwichanop, Kittisupakorn, & Mujtaba, 2005; Karanki et al., 2018; Podofillini & Dang, 2012; Podofillini, Sudret, Stojadinović, Zio, & Kröger, 2015).

Both reactants (A and B) and a solvent are loaded into a batch reactor. The stirrer is switched on. The reaction mixture is heated up slowly to its temperature setpoint of 71 ± 2 °C, where the reaction starts. When the temperature of the reaction mixture reaches 71 ± 2 °C the temperature control system starts in such a way, that the cooling liquids mass flow and temperature remain constant under normal reaction conditions. If the temperature of the reaction mixture exceeds 90 ± 2 °C, within 70 ± 2 °minutes of operation, alarm 1 is triggered. The crew then adjusts the cooling temperature of the mass flow of the cooling liquid to of 40 ± 2 °C to improve the heat transfer from the batch reactor to the cooling liquid. If the temperature of the reaction mixture exceeds 105 ± 1°C however, alarm 2 is triggered. The operators then activate the emergency cooling system, which enables the maximum equipment related heat transfer to cool down the reactor content to 20 ± 3°C. Deviations in the process parameters of unforeseeable equipment failures may lead to extreme temperature rises, reaching unsafe conditions. If temperature exceeds 150 ± 3°C, the released reaction heat will be higher than the maximum possible heat transfer of the reaction mixture to the cooling liquid. Consequently the reaction in the batch reactor will be out of control, a run-away reaction occurs.

In their simulation, Karanki et al. (2018) found that “extreme deviations in initial conditions induce very fast reactor dynamics leading to uncontrolled runaway conditions. In such a scenario, reactor temperature reaches 105 °C even if safety functions (ECS and operator changing TCS set point) intervene”. The exact nominal and deviation process parameters can be found in (Karanki et al., 2018).Karanki et al. (2018) express their belief that the higher the temperature, the higher the mental stress acting on the operators, thus raising failure probability.

4.1.2 Plant A - pre-digital chemical plant

In the analog chemical plant, there is no IT and no control room. The chemical worker in the near vicinity of the reactor, monitoring the temperature in case of an alarm, adjusts manually the temperature of the cooling system or activates the emergency cooling system using two point (on, off) controllers. This system represents the plant with lowest complexity. Primitive temperature control is achieved by using temperature indicating thermometers and hand valves. with a threaded spindle and rotary magnet. As mentioned above, there is no IT department and no IT services are provided. Persons, departments and outside stakeholders communicate via oral or written communication. Conversations over phone lines are possible. Maintenance is primarily done when inspections indicate equipment deterioration. Figure 26 shows the process map of plant A, the processes marked with red border are used in the FRAM model, the process marked with black border are outside the scope of the investigated system. Essentially all production relevant processes, excluding the supply chain, are per definition part of the described system.

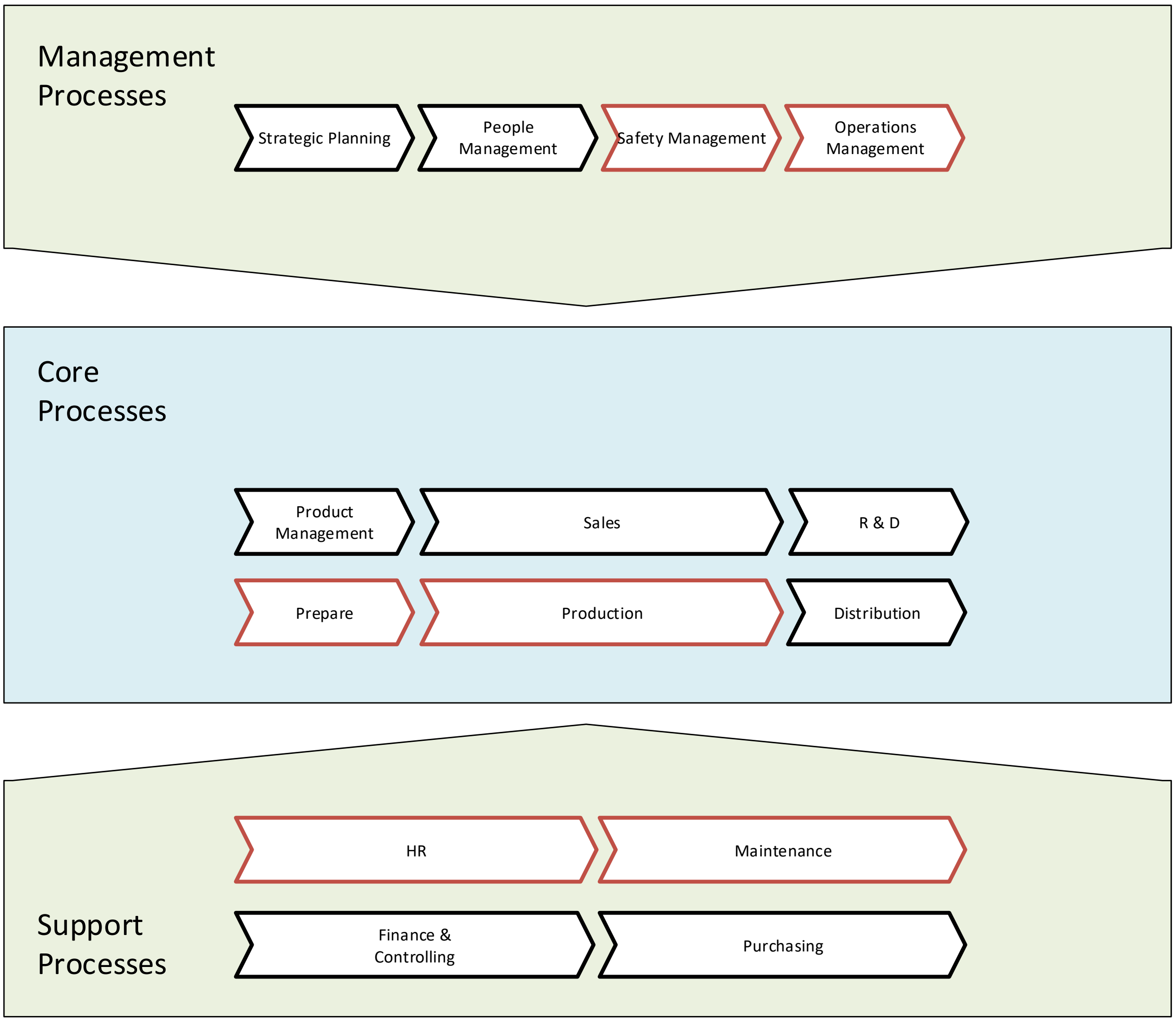


Figure 26 Process map of plant A - analog plant

Figure 29Figure 29 shows a simplified schematic of this type of plant.

4.1.3 Plant B - IT centralized chemical plant

In centralized control plants, the process control system monitors and controls the local plant. It regulates or changes physical measurement values like flows, temperatures, amounts, following certain, even time dependent, recipes for a batch reaction.

In case of alarm 2 – temperature exceeding 105 ± 1°C -the control system should automatically start the emergency cooling system. In case the emergency cooling system is not started automatically, the operator needs to start it manually. The centralized IT control structure uses point-to-point communication and introduces a single point of failure. Failure or malfunction in one sensor can lead to severe disturbances of operations. Applications, as ERP software or control software, are specifically written for its purposes. As reliability data is available, maintenance relies upon preventive maintenance. As in plant A, inspections are an integral part of maintenance. *Figure 27* shows the process map of plant B, the processes marked with red border are used in the FRAM model, the process marked with black border are outside the scope of the investigated system. In comparison with plant A, the safety management process was substituted by risk management processes. Quality improvement process and IT support processes were introduced.

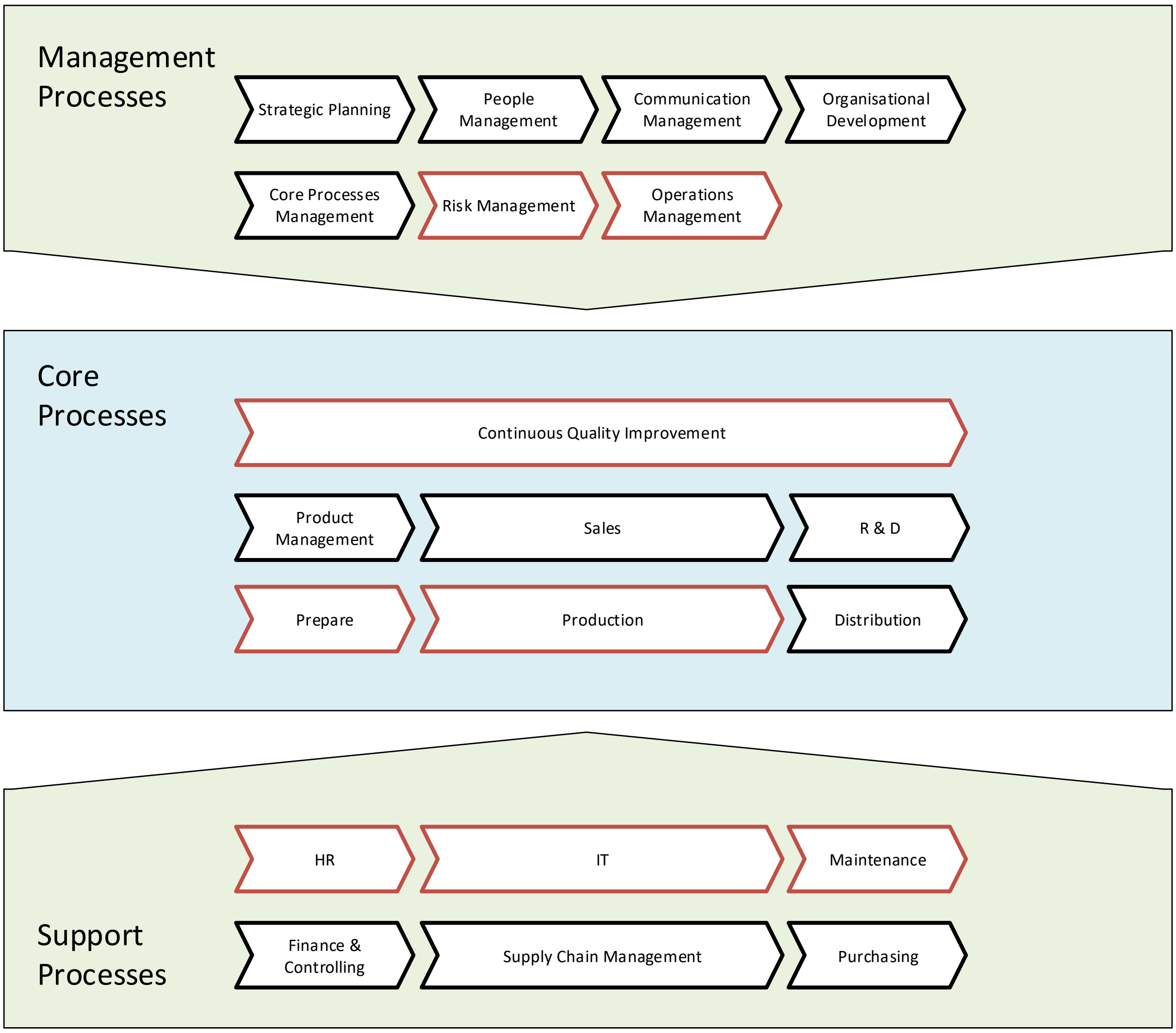


Figure 27 Process map of plant B - centralized control plant

Figure 30 shows a simplified schematic of this type of plant.

4.1.4 Plant C - Chemistry 4.0 plant

In the Chemistry 4.0 plant, multiple controllers supervise the process and control the cooling system independently. Human operators in a control room supervise the system. In case of reaching alarm 1, the low-level controllers or the high-level controllers or the operators adjust the temperature of the cooling system. If alarm 2 is triggered, the controllers activate the emergency cooling system. In case the emergency cooling system is not started automatically, the operator needs to start it manually. The IT control structure is interwoven with the control network and represents a coordinated distributed control network relying on point-to-point supplemented by networked, synchronous and asynchronous communication. All controllers communicate with each other or via higher level controllers and can act independently or conjoined. Figure 31 shows the process map of plant C, the processes marked with red border are used in the FRAM model, the process marked with black border are outside the scope of the investigated system. In comparison with plant B, the processes inside the investigated system do not change.

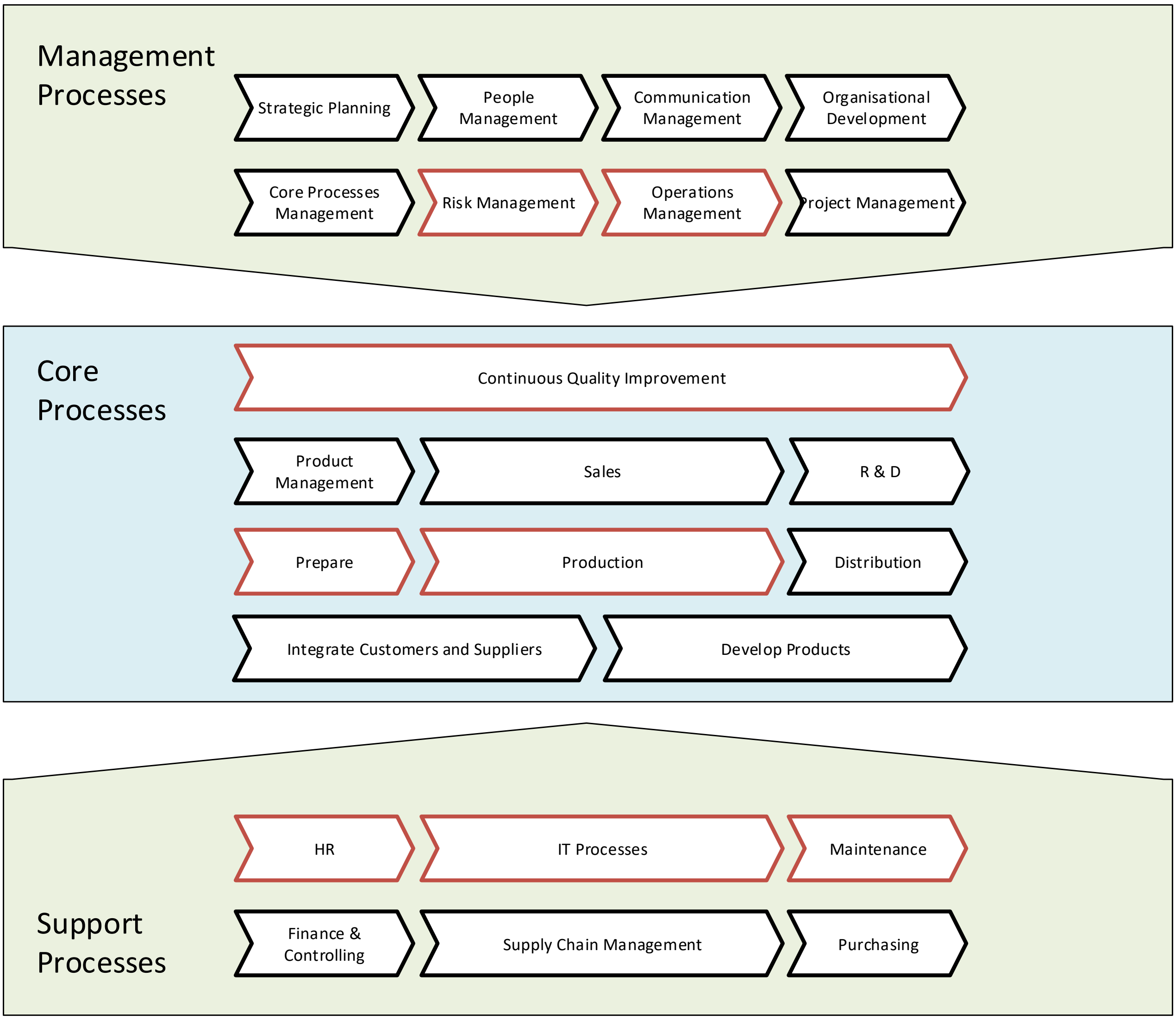


Figure 28 Process map of plant C – Chemistry 4.0 plant

Figure 31 shows a simplified schematic of this type of plant.

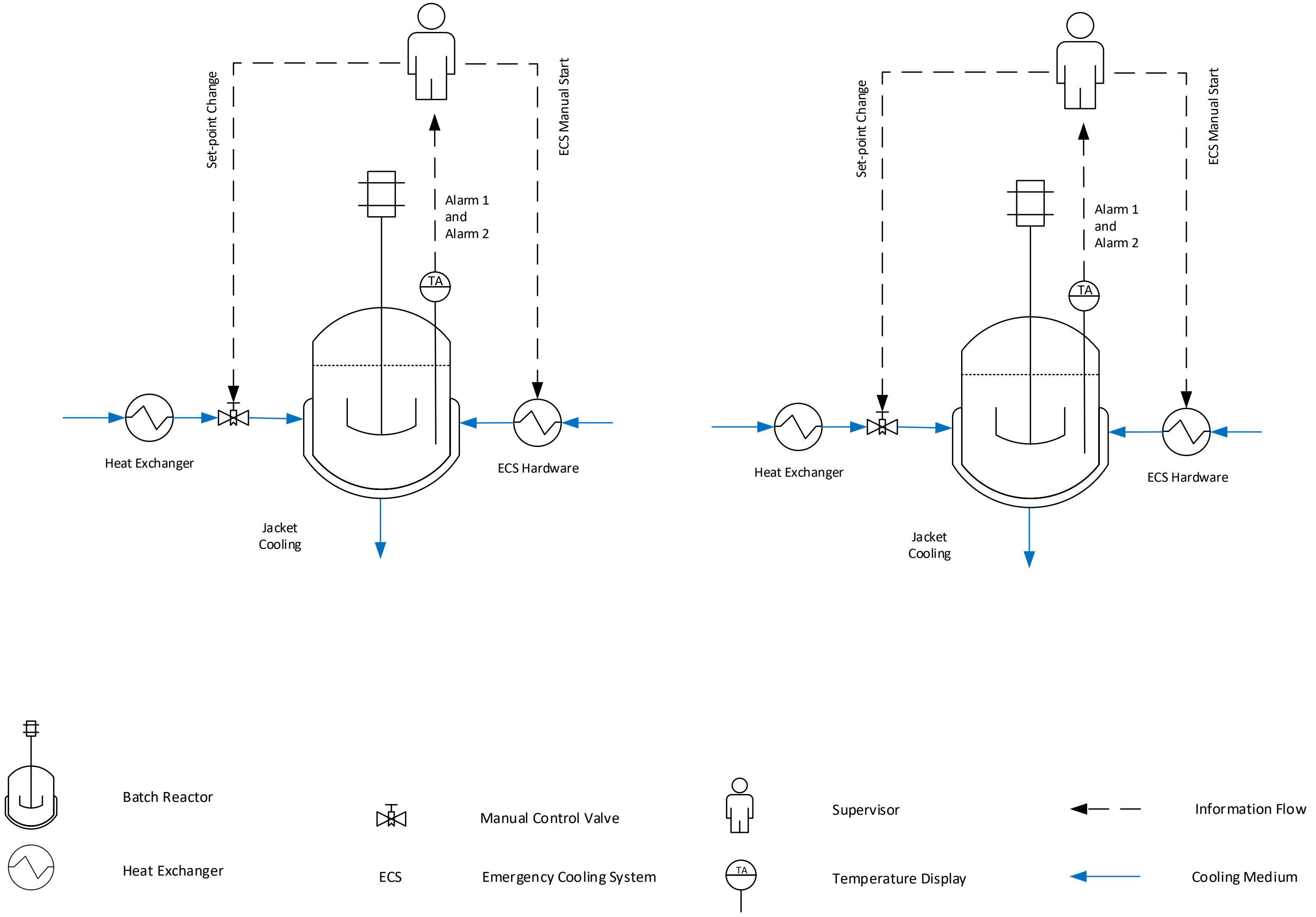


Figure 29 Simplified schematic plant A - the analog plant

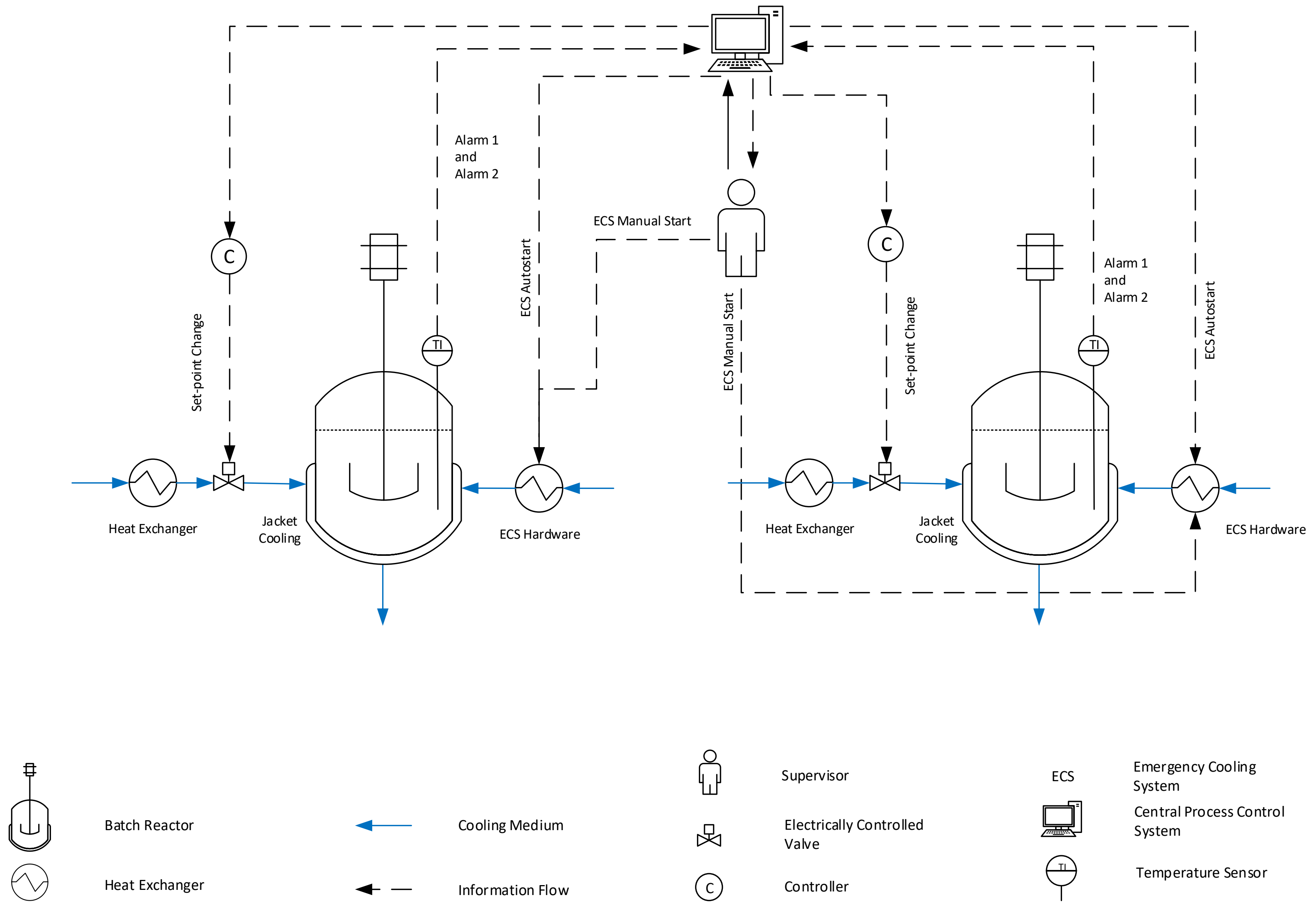


Figure 30 Simplified schematic of plant B with centralized IT control

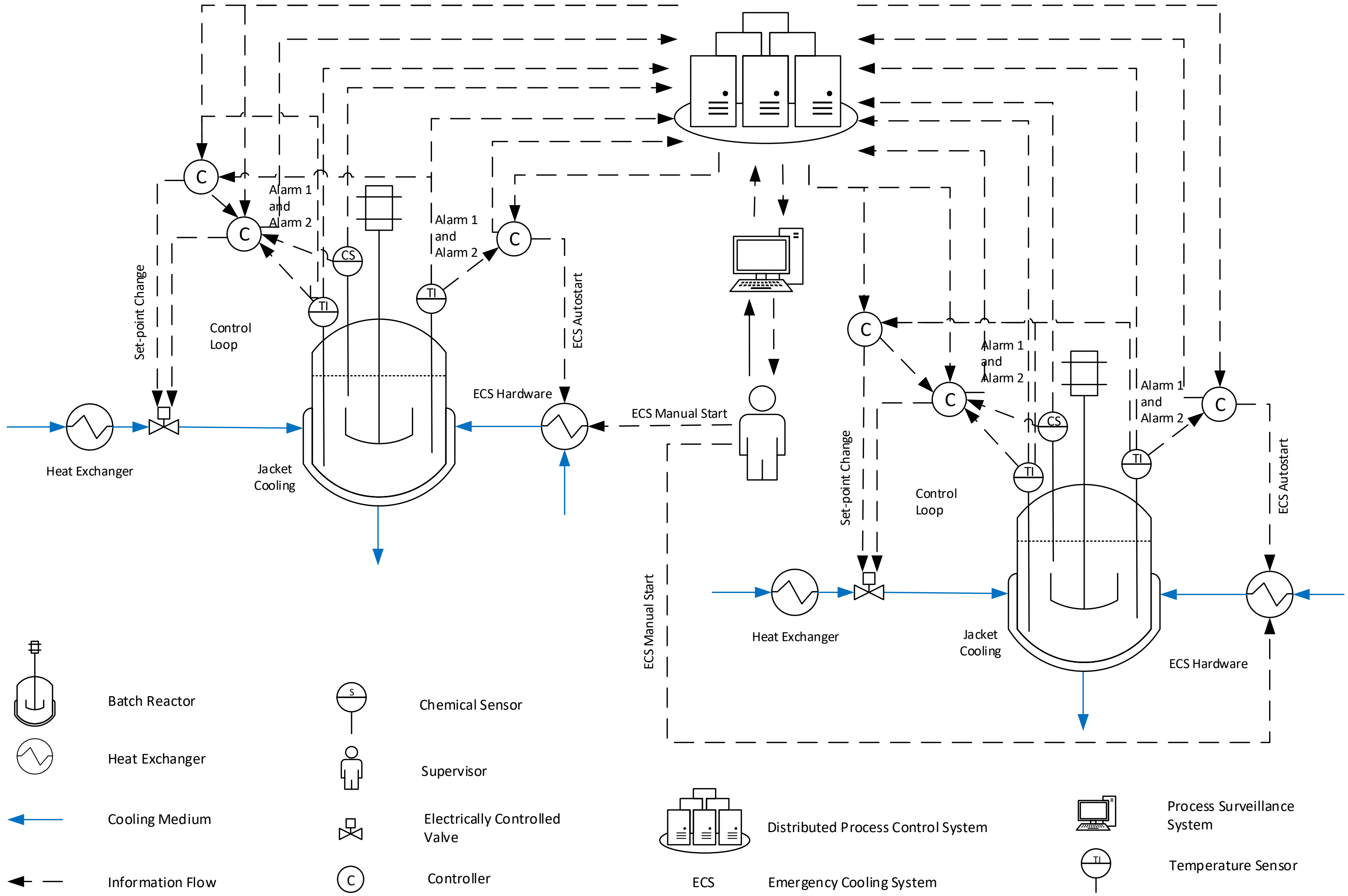


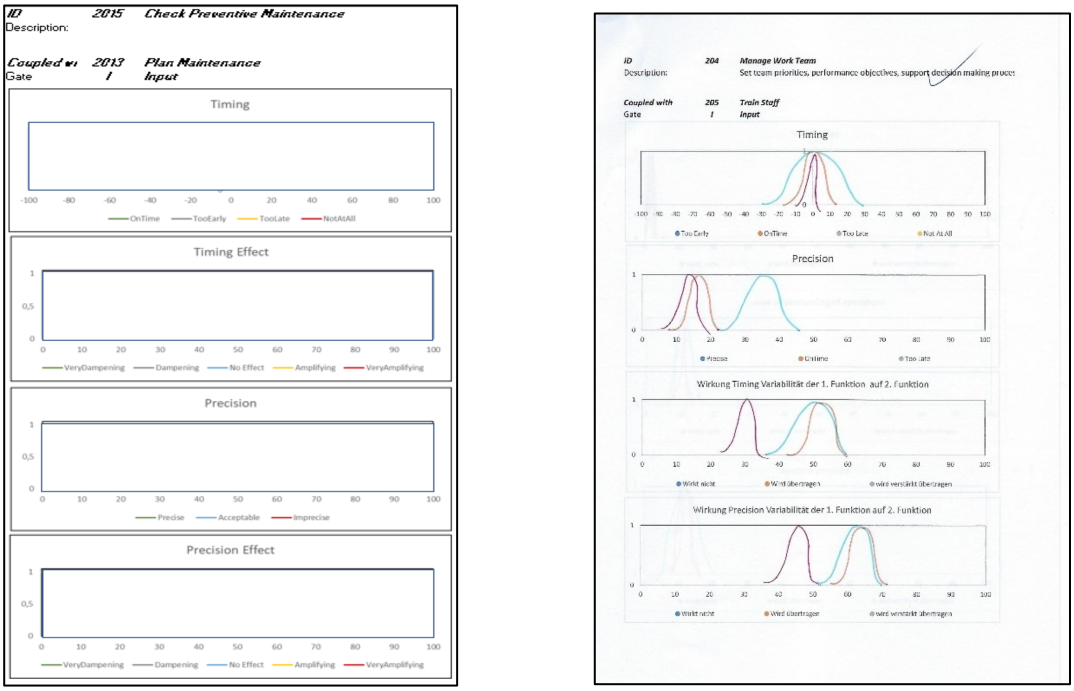
Figure 31 Simplified schematic plant C - chemistry 4.0 plant

4.2 Interviews

An expert is a person who has special knowledge related to his profession. The selection of experts took place based on three criteria. The experts had to have background in at least one of the disciplines in chemistry, plant operations or IT operations and knowledge about the topic. Based on these criteria three experts were selected and used in interviews to verify the FRAM model for the different plants and to give their estimates on performance variabilities of the FRAM functions.

One expert has over 40 years' experience with chemical plants, with positions ranging from technikum manager, to manager responsible for complete plants. One expert has over 17 years' experience in the IT department of an automotive company. Among his responsibilities is the management of IT hardware infrastructure and the IT service landscape of the company's manufacturing execution system. One expert is responsible for security aspects in the IT department of an automotive company. His work experience is six years.

These experts verified the FRAM models of plant A, B and C as shown in chapter 4.4.1. Then each expert gave his estimation for output timing and precision variability of the basic function for each coupling and what effect these timing and precision variabilities have on the performance variability in form of distributions. With these values the model is instantiated. For each of the disturbances the experts gave their estimation of the disturbance effect on performance variability, also in the form of distributions. With these values the effect of disturbances on the system chemical plant can be simulated. These interviews were conducted for all chemical plants studied in this research. Figure 32 shows one example for the interview forms for the coupling of FRAM functions and one filled out sample.



ID 2015 Check Preventive Maintenance
Description:

Coupled wi 2013 Plan Maintenance
Gate I Input

ID 204 Manage Work Team
Description: Set team priorities, performance objectives, support decision making proce:

Coupled with 205 Train Staff
Gate I Input

Figure 32 Sample of interview form

4.3 Fault Tree Analysis FTA

As discussed in chapter 3.2 the limitations of FTA in complex systems is evident. For this reason, the Fault tree analysis is only carried out for one top event, namely a runaway reaction caused by deviations of process variables. This FTA for a runaway reaction was chosen, because this model is described in literature for setups similar to plant A and plant B. For each type of plant an FTA is made. The response variable for the fault tree analysis is probability - the extent to which the top event of the fault tree, or system failure condition is likely to happen given the reliability data. The event tree leading to the top event, based on the descriptions of chapter 4.1.1 is shown in Figure 33. A process deviation may lead directly to an uncontrollable top event, alternatively the failure of some barriers may also result in a runaway reaction.

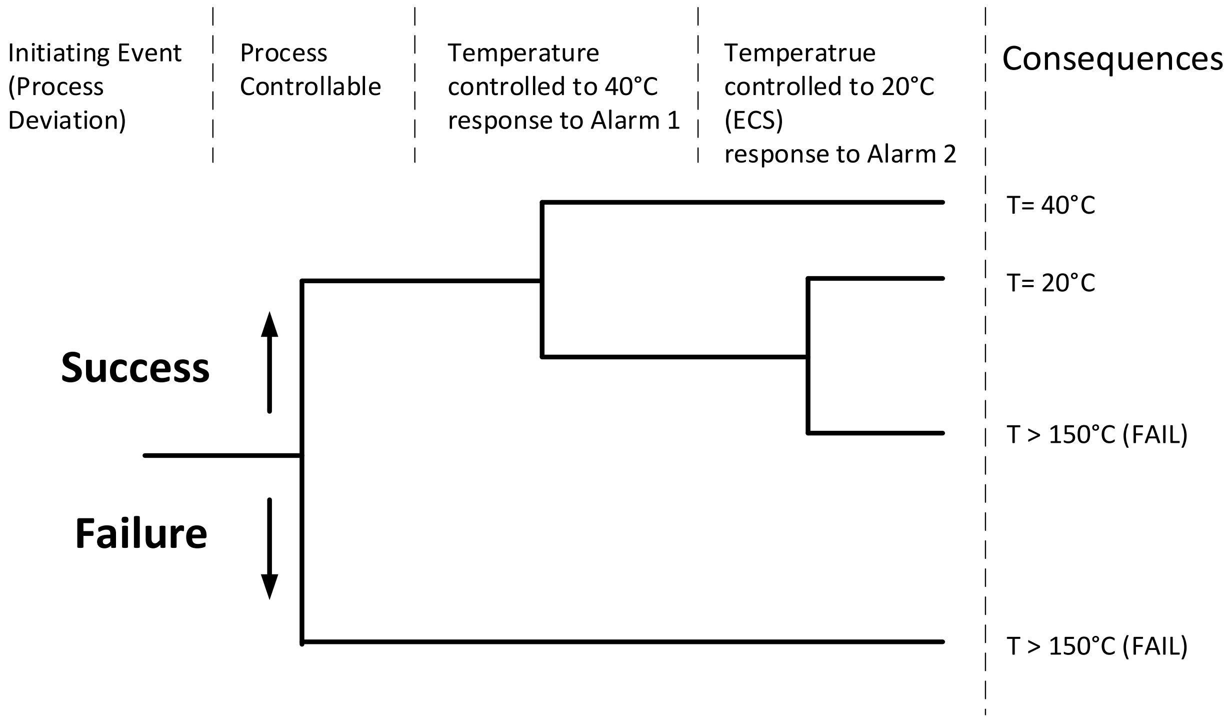

Initiating Event (Process Deviation)
Process Controllable
Temperature controlled to 40°C response to Alarm 1
Temperatrue controlled to 20°C (ECS) response to Alarm 2
Consequences
T= 40°C
T= 20°C
T > 150°C (FAIL)
T > 150°C (FAIL)
Success
Failure

Figure 33 Event tree for deviation in process parameters

For this study, a constant failure model is assumed, where specified event unavailabilities and failure frequencies that do not vary with time. The data used for FTA analysis were used as reported in the literature. Not reported values were supplied by the interviewees. Table 9 shows the data used in the FTA and its sources.

Table 9 FTA Unavailabilities – Literature Sources

Plant	Node	Unavailability	Literature Source
A	Activation Conditions for Alarm 1 bypassed	q=0,1	Podofillini and Dang (2012)
A	ECS fails to run	q=2,5E-06	Podofillini and Dang (2012)
A	Failure Heat Exchanger	q=0,01	Podofillini and Dang (2012)
A	Failure of Alarm 2	q=0,01	Podofillini and Dang (2012)
A	Failure of Operator to diagnose	q=0,01	Podofillini and Dang (2012)
A	Failure of Operator to diagnose	q=0,25	Podofillini and Dang (2012)

Plant	Node	Unavailability	Literature Source
A	Failure of Operator to execute	q=0,001	Podofillini and Dang (2012)
A	Failure of Operator to execute	q=0,001	Podofillini and Dang (2012)
A	Failure of Temperatur Sensors	q=0,01	Kletz (2001)
A	Failure Valve	q=0,0001	Kletz (2001)
A	No Cooling Medium	q=0,01	Podofillini and Dang (2012)
B	Activation Conditions for Alarm 1 bypassed	q=0,1	Podofillini and Dang (2012)
B	Control System Fail	q=0,001	Karanki et al. (2018)
B	Control System fails to respond to Alarm 1	q=0,001	Karanki et al. (2018)
B	Control System fails to start automatically	q=0,01	Karanki et al. (2018)
B	Controller Fail	q=0,001	Karanki et al. (2018)
B	ECS fails to run	q=2,5E-06	Podofillini and Dang (2012)
B	Failure Heat Exchanger	q=0,01	Podofillini and Dang (2012)
B	Failure of Alarm 2	q=0,01	Podofillini and Dang (2012)
B	Failure of Operator to diagnose	q=0,01	Podofillini and Dang (2012)
B	Failure of Operator to diagnose	q=0,25	Podofillini and Dang (2012)
B	Failure of Operator to execute	q=0,001	Podofillini and Dang (2012)
B	Failure of Operator to execute	q=0,001	Podofillini and Dang (2012)
B	Failure of Temperatur Sensor	q=0,01	Kletz (2001)
B	Failure Valve	q=0,0001	Kletz (2001)Expert Estimate
B	No Cooling Medium	q=0,01	Podofillini and Dang (2012)
C	Activation Conditions for Alarm 1 bypassed	q=0,1	Podofillini and Dang (2012)
C	Control System Fail	q=0,001	Karanki et al. (2018)
C	Control System fails to respond to Alarm 1	q=0,001	Karanki et al. (2018)
C	Control System fails to start automatically	q=0,01	Karanki et al. (2018)
C	Controller Fail	q=0,001	Karanki et al. (2018)
C	Controller fail to start ECS	q=1E-05	Karanki et al. (2018)
C	ECS fails to run	q=2,5E-06	Podofillini and Dang (2012)
C	Failure Heat Exchanger	q=0,01	Podofillini and Dang (2012)
C	Failure of Alarm 2	q=0,01	Podofillini and Dang (2012)
C	Failure of Operator to diagnose	q=0,01	Podofillini and Dang (2012)
C	Failure of Operator to diagnose	q=0,25	Podofillini and Dang (2012)
C	Failure of Operator to execute	q=0,001	Podofillini and Dang (2012)
C	Failure of Operator to execute	q=0,001	Podofillini and Dang (2012)
C	Failure of Temperatur Sensors	q=0,0001	Kletz (2001)
C	Failure Valve	q=0,0001	Kletz (2001)
C	High, Low Controllers fails to respond to Alarm 1	q=1E-06	Expert Estimate
C	No Cooling Medium	q=0,01	Podofillini and Dang (2012)

The FTA calculations were conducted using TopEvent FTA 2017 Version1.2.2 from Reliotech S.A.S de C.V.

4.4 FRAM Analysis

FRAM investigates the interactions between different system functions and not simple probability of failures. It analyses the whole system, giving a model, describing performance variability of commonplace operations. It shows critical coupling paths between functions, allowing to introduce barriers or mitigating actions in critical areas, to decrease performance variability. The system behavior in case of disturbance is also investigated.

After defining the boundaries of the investigated system (see chapter 4.1), three FRAM models were developed using a hierarchical approach. Then the developed FRAM models were verified and validated by domain experts who have a good understanding of how the model should work. In a new approach, a hybrid Fuzzy-Logic-FRAM Simulation Model is developed. Based on a hierarchical FRAM model, data from the interviews are used as input to the simulation.

The program was written in C# in Visual Studio 2017 Professional, Data were stored and analyzed in SQL Server 2016 SP1. Visualizations were done by using Excel 365 ProPlus 1806. All these programs are provided by Microsoft Inc. Additional analysis was done in R-Studio Version 1.1.453.

4.4.1 Hierachical FRAM model

The model for this study uses an hierarchical approach as proposed by Patriarca, Bergström, and Di Gravio (2017) and similar to Rasmussen (1997). The hierarchical approach identifies key agents and uses a top-down description of the system. In this way it is possible to go into details where necessary and to describe superficially where it is sufficient. Key agents can be departments, companies or persons. The four abstraction hierarchical layers as defined by Patriarca, Bergström et al. (2017) can be found in Table 10.

Table 10 Meaning of the four abstraction levels (Patriarca, Bergström et al., 2017)

Abstraction Level	**Characteristics of the Function proposed with respect to the agent**
Functional Purpose (FP)	The ultimate functions that the agent should accomplish
Generalized Function (GF)	Purpose-related functions of the agent to achieve the functional purpose
Physical Function (PF)	Functions necessary to implement GF-level function, identified from the related technological components.
Physical and Technological Form (PTF)	Functions describing components and devices of the system in terms of layout, functioning and form.

To identify relevant stakeholders in the operation of a chemical facility, a stakeholder analysis was conducted. Input from different domain experts were used to prioritize the stakeholders. This analysis was used to narrow down the number of relevant stakeholders. Defining the boundaries of the investigated system, only three agents – the IT department, operations and the chemical worker / operator from the top right quadrant were used in this study (see Figure 34).

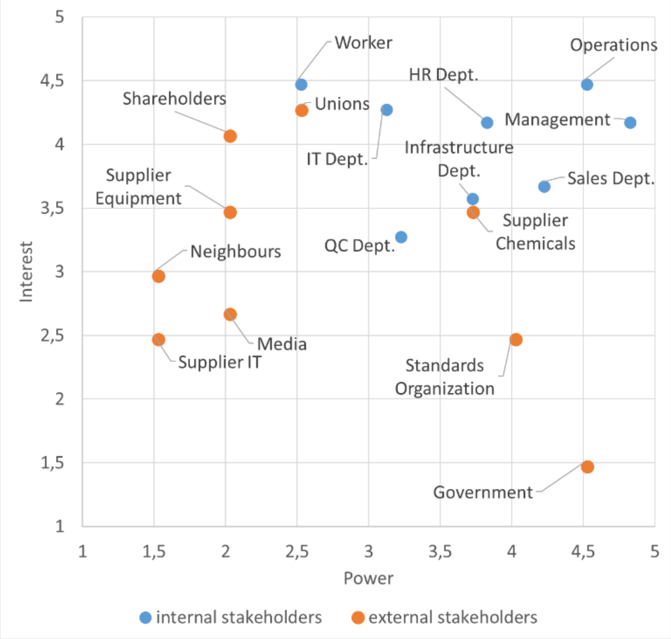


Figure 34 Stakeholder analysis

One advantage of the hierarchical approach is that it is not necessary to investigate all agents in complete depth (see Table 11).

Table 11 Hierarchical Model - Analyzation levels

Agency Abstraction	Operations	IT Dept.	Worker
Functional Purpose	analyzed	analyzed	analyzed
Generalized Function	analyzed	analyzed	analyzed
Physical function	analyzed	analyzed	analyzed
Physical and Technological Form	Not analyzed	analyzed	analyzed

After setting the boundaries of the system, FRAM models for the three plants were developed. Only compact views of all FRAM models are presented in this thesis. All plans are included as PDFs on the CD and in printed-out form attached to this master thesis book.

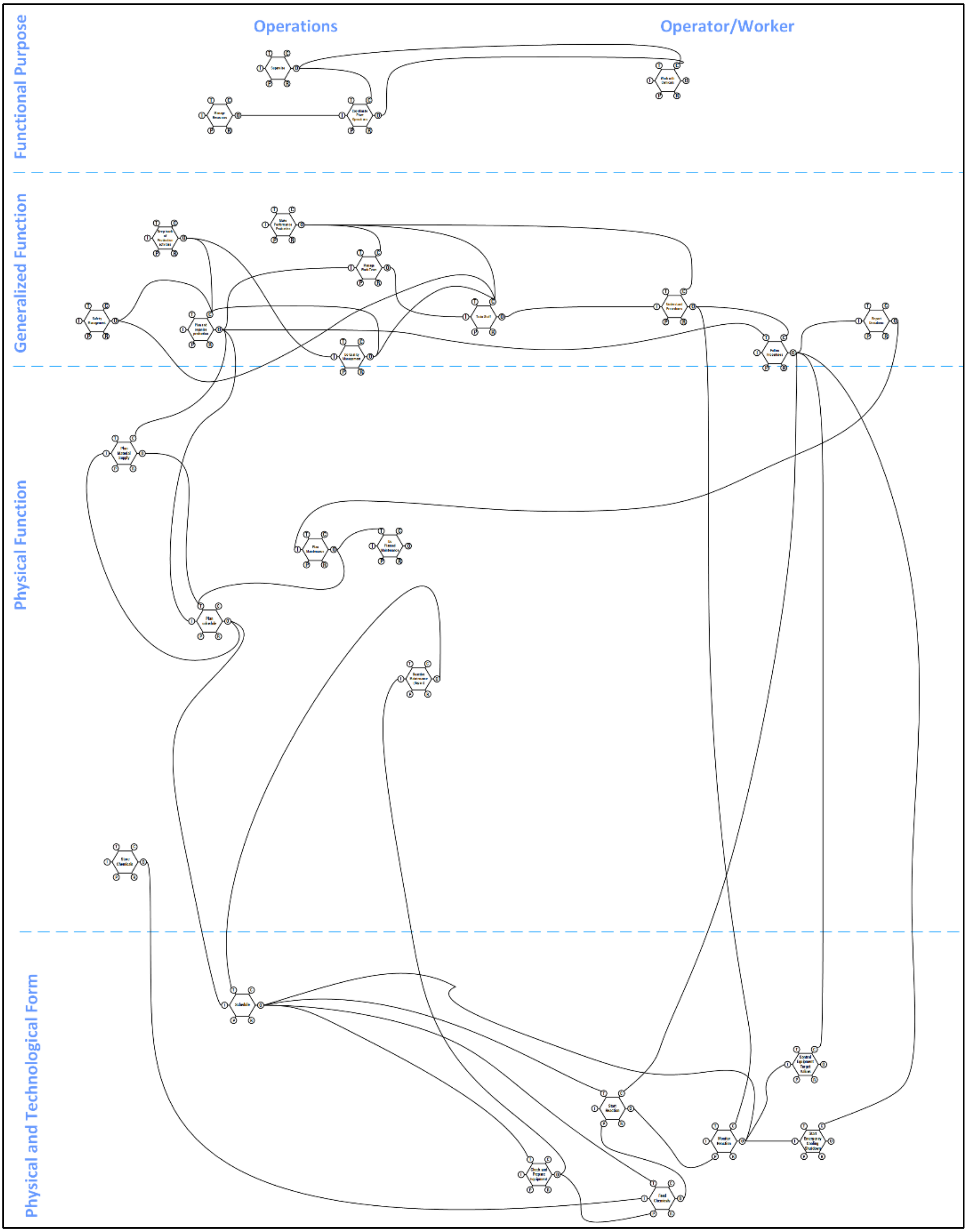


Figure 35 FRAM Model Plant A

Figure 35 shows the FRAM model for plant A, the functions and couplings relevant for IT Services are missing as defined following the digitalization maturity model. Maintenance functions are only related to repair. Control systems are missing.

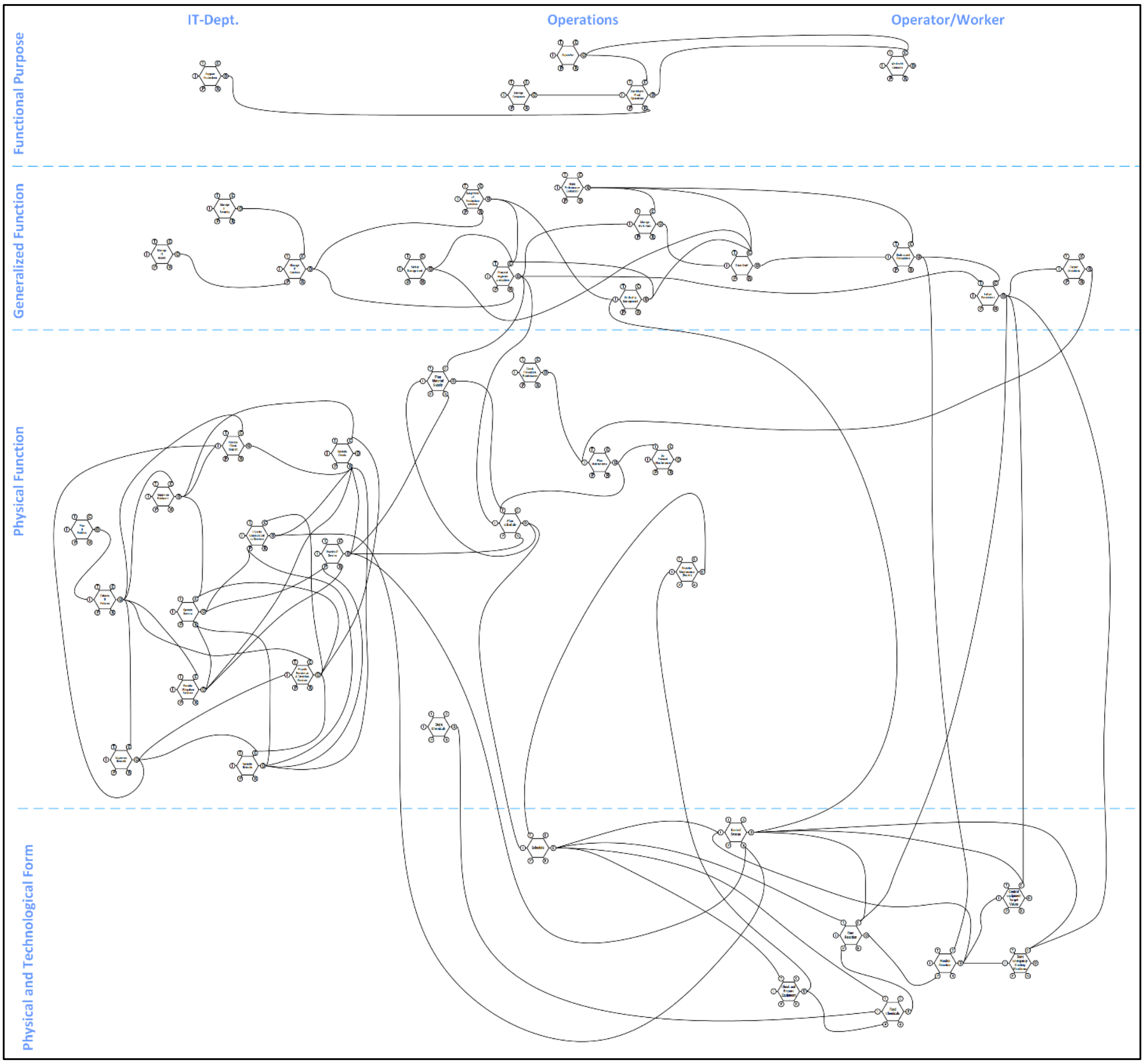


Figure 36 FRAM Model of Plant B

Figure 36 shows the FRAM model for plant B, the functions and couplings relevant for IT Services are included. Maintenance functions are related to repair and preventive maintenance. The control and planning systems depend on Services provided by the IT department. Figure 37shows the FRAM model for plant C, this model is similar to the one of plant B. The main difference is the inclusion of functions related to predictive maintenance.

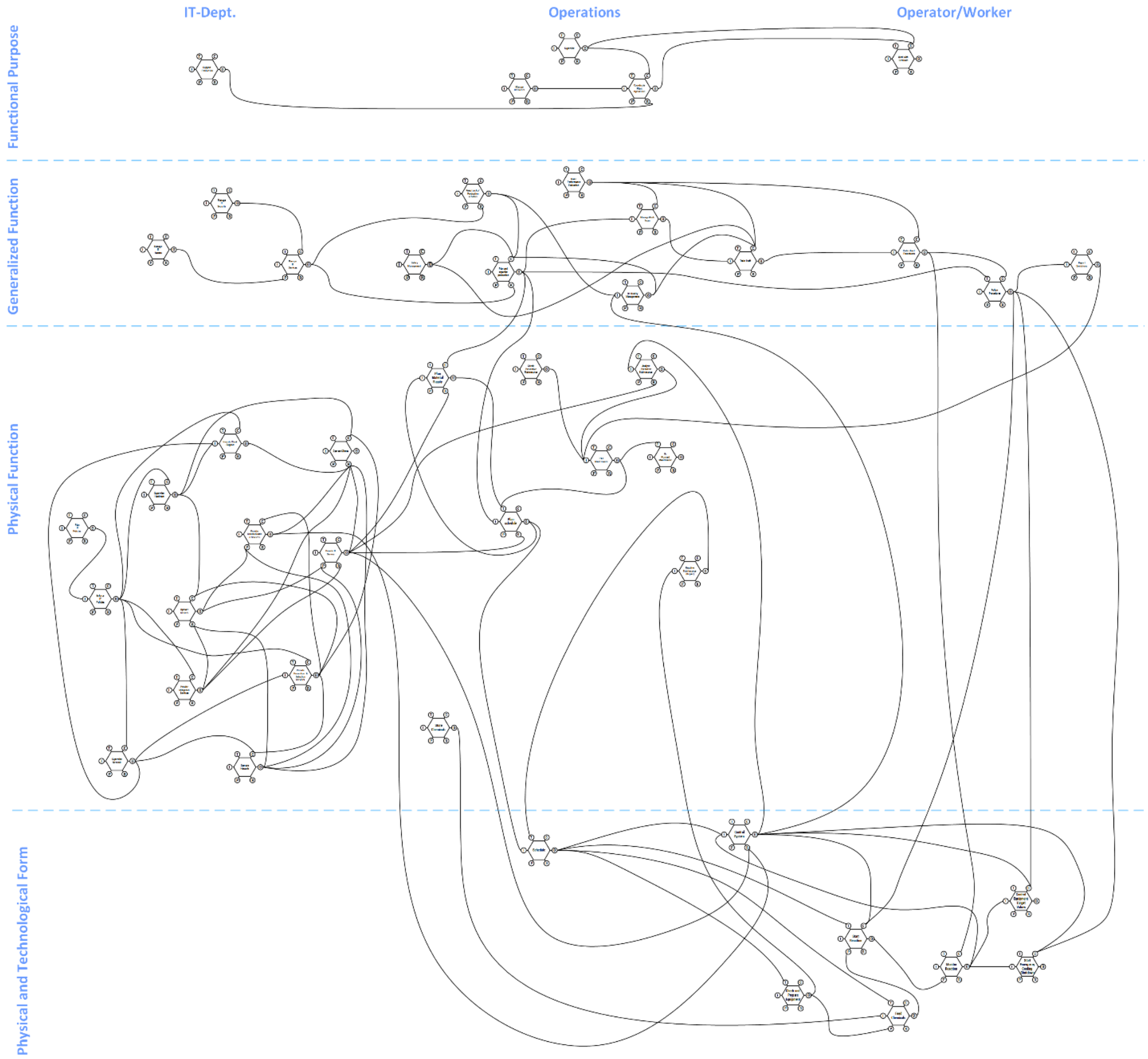


Figure 37 FRAM Model of Plant C

Plant A has fewer functions and couplings due to its analog nature. Table 12 shows the number of functions and couplings for all plants. It can be seen that digitalization leads to more functions and connections, increasing the complexity of the system. The identified couplings for each plant can be seen in Table 13.

Table 12 Number of Functions and Couplings for all plants

Plant	FRAM Functions	FRAM Couplings
A	26	49
B	45	85
C	47	87

Table 13 FRAM Couplings for Plants A , B and C

Plant	FRAMName OUT	FRAMName IN	GATE_IN	ID FRAM Coupling
A	Support Production	Coordinate Plant Operations	P	181
A	Manage Resources	Coordinate Plant Operations	I	182
A	Supervise	Coordinate Plant Operations	C	183
A	Supervise	Work with Chemicals	C	184
A	Coordinate Plant Operations	Work with Chemicals	C	185
A	Keep track of production activities	Plan and organize Production	C	190
A	Keep track of production activities	Make Performance Evaluation	I	191
A	Keep track of production activities	Do Quality Management	I	192
A	Keep track of production activities	Schedule	I	193
A	Safety Management	Plan and organize Production	C	194
A	Safety Management	Train Staff	C	195
A	Plan and organize Production	Manage Work Team	I	196
A	Plan and organize Production	Follow Procedures	T	197
A	Plan and organize Production	Plan Material Supply	C	198
A	Plan and organize Production	Plan Schedule	I	199
A	Make Performance Evaluation	Manage Work Team	C	200
A	Make Performance Evaluation	Train Staff	C	201
A	Make Performance Evaluation	Understand procedures	C	202
A	Manage Work Team	Train Staff	I	203
A	Manage Work Team	Follow Procedures	T	204
A	Train Staff	Understand procedures	I	205
A	Train Staff	Follow Procedures	I	206
A	Understand procedures	Follow Procedures	C	207
A	Understand procedures	Monitor Reaction	C	208
A	Follow Procedures	Report Deviations	I	209
A	Follow Procedures	Start Reaction	C	210
A	Follow Procedures	Start Emergency Cooling Shutdown	C	211
A	Plan Material Supply	Plan Schedule	T	244
A	Plan Schedule	Plan Material Supply	I	245
A	Plan Schedule	Schedule	I	246
A	Schedule	Check & Prepare Equipment	T	247
A	Schedule	Feed Chemicals	T	248
A	Schedule	Start Reaction	T	249
A	Store Chemicals	Feed Chemicals	I	251
A	Check & Prepare Equipment	Feed Chemicals	P	252
A	Feed Chemicals	Start Reaction	P	253
A	Start Reaction	Monitor Reaction	P	254
A	Monitor Reaction	Start Emergency Cooling Shutdown	I	255
A	Monitor Reaction	Control Equipment Target Values	C	257
A	Reactive Maintenance (Repair)	Schedule	T	263

Plant	FRAMName OUT	FRAMName IN	GATE_IN	ID FRAM Coupling
A	Plan Maintenance	Plan Schedule	C	264
A	Plan Maintenance	Do planned maintenance	T	265
B	Support Production	Coordinate Plant Operations	P	94
B	Manage Resources	Coordinate Plant Operations	I	95
B	Supervise	Coordinate Plant Operations	C	96
B	Supervise	Work with Chemicals	C	97
B	Coordinate Plant Operations	Work with Chemicals	C	98
B	Manage IT Assets	Manage IT Services	P	99
B	Manage IT Security	Manage IT Services	C	100
B	Manage IT Services	Keep track of production activities	R	101
B	Manage IT Services	Plan and organize Production	R	102
B	Keep track of production activities	Plan and organize Production	C	103
B	Keep track of production activities	Make Performance Evaluation	I	104
B	Keep track of production activities	Do Quality Management	I	105
B	Keep track of production activities	Schedule	I	106
B	Safety Management	Plan and organize Production	C	107
B	Safety Management	Train Staff	C	108
B	Plan and organize Production	Manage Work Team	I	109
B	Plan and organize Production	Follow Procedures	T	110
B	Plan and organize Production	Plan Material Supply	C	111
B	Plan and organize Production	Plan Schedule	I	112
B	Make Performance Evaluation	Manage Work Team	C	113
B	Make Performance Evaluation	Train Staff	C	114
B	Make Performance Evaluation	Understand procedures	C	115
B	Manage Work Team	Train Staff	I	116
B	Manage Work Team	Follow Procedures	T	117
B	Train Staff	Understand procedures	I	118
B	Train Staff	Follow Procedures	I	119
B	Understand procedures	Follow Procedures	C	120
B	Understand procedures	Monitor Reaction	C	121
B	Follow Procedures	Report Deviations	I	122
B	Follow Procedures	Start Reaction	C	123
B	Follow Procedures	Start Emergency Cooling Shutdown	C	124
B	Plan IT Policies	Enforce IT Policies	I	125
B	Enforce IT Policies	Supervise Hardware	C	126
B	Enforce IT Policies	Provide Mitigation Services	C	127
B	Enforce IT Policies	Supervise Network	C	128
B	Enforce IT Policies	Provide Client Support	C	129
B	Enforce IT Policies	Provide Prevention & Detections Services	C	130
B	Supervise Hardware	Operate Servers	C	131
B	Supervise Hardware	Provide Client Support	I	132
B	Supervise Hardware	Operate Clients	C	133

Plant	FRAMName OUT	FRAMName IN	GATE_IN	ID FRAM Coupling
B	Operate Servers	Provide Communication Services	P	134
B	Operate Servers	Provide IT Services	P	135
B	Provide Mitigation Services	Operate Servers	R	136
B	Provide Mitigation Services	Operate Clients	R	137
B	Provide Mitigation Services	Provide IT Services	R	138
B	Supervise Network	Provide Client Support	I	139
B	Supervise Network	Provide Prevention & Detections Services	I	140
B	Supervise Network	Operate Network	C	141
B	Provide Client Support	Operate Clients	R	142
B	Provide Communication Services	Operate Clients	R	143
B	Provide Communication Services	Control System	R	144
B	Provide IT Services	Operate Clients	R	145
B	Provide IT Services	Plan Material Supply	R	146
B	Provide IT Services	Plan Schedule	R	147
B	Provide Prevention & Detections Services	Operate Servers	C	149
B	Provide Prevention & Detections Services	Provide Client Support	C	150
B	Provide Prevention & Detections Services	Operate Clients	C	151
B	Provide Prevention & Detections Services	Operate Network	C	152
B	Operate Network	Operate Servers	R	153
B	Operate Network	Provide Communication Services	R	154
B	Operate Network	Operate Clients	R	155
B	Operate Network	Provide IT Services	R	156
B	Plan Material Supply	Plan Schedule	T	157
B	Plan Schedule	Plan Material Supply	I	158
B	Plan Schedule	Schedule	I	159
B	Schedule	Check & Prepare Equipment	T	160
B	Schedule	Feed Chemicals	T	161
B	Schedule	Start Reaction	T	162
B	Schedule	Control System	I	163
B	Store Chemicals	Feed Chemicals	I	164
B	Check & Prepare Equipment	Feed Chemicals	P	165
B	Feed Chemicals	Start Reaction	P	166
B	Start Reaction	Monitor Reaction	P	167
B	Monitor Reaction	Start Emergency Cooling Shutdown	I	168
B	Monitor Reaction	Control System	I	169
B	Monitor Reaction	Control Equipment Target Values	C	170
B	Control System	Do Quality Management	I	171
B	Control System	Start Reaction	C	172
B	Control System	Start Emergency Cooling Shutdown	C	173
B	Control System	Control Equipment Target Values	C	174

Plant	FRAMName OUT	FRAMName IN	GATE_IN	ID FRAM Coupling
B	Reactive Maintenance (Repair)	Schedule	T	176
B	Plan Maintenance	Plan Schedule	C	177
B	Plan Maintenance	Do planned maintenance	T	178
C	Support Production	Coordinate Plant Operations	P	7
C	Manage Resources	Coordinate Plant Operations	I	8
C	Supervise	Coordinate Plant Operations	C	9
C	Supervise	Work with Chemicals	C	10
C	Coordinate Plant Operations	Work with Chemicals	C	11
C	Manage IT Assets	Manage IT Services	P	12
C	Manage IT Security	Manage IT Services	C	13
C	Manage IT Services	Keep track of production activities	R	14
C	Manage IT Services	Plan and organize Production	R	15
C	Keep track of production activities	Plan and organize Production	C	16
C	Keep track of production activities	Make Performance Evaluation	I	17
C	Keep track of production activities	Do Quality Management	I	18
C	Keep track of production activities	Schedule	I	19
C	Safety Management	Plan and organize Production	C	20
C	Safety Management	Train Staff	C	21
C	Plan and organize Production	Manage Work Team	I	22
C	Plan and organize Production	Follow Procedures	T	23
C	Plan and organize Production	Plan Material Supply	C	24
C	Plan and organize Production	Plan Schedule	I	25
C	Make Performance Evaluation	Manage Work Team	C	26
C	Make Performance Evaluation	Train Staff	C	27
C	Make Performance Evaluation	Understand procedures	C	28
C	Manage Work Team	Train Staff	I	29
C	Manage Work Team	Follow Procedures	T	30
C	Train Staff	Understand procedures	I	31
C	Train Staff	Follow Procedures	I	32
C	Understand procedures	Follow Procedures	C	33
C	Understand procedures	Monitor Reaction	C	34
C	Follow Procedures	Report Deviations	I	35
C	Follow Procedures	Start Reaction	C	36
C	Follow Procedures	Start Emergency Cooling Shutdown	C	37
C	Plan IT Policies	Enforce IT Policies	I	38
C	Enforce IT Policies	Supervise Hardware	C	39
C	Enforce IT Policies	Provide Mitigation Services	C	40
C	Enforce IT Policies	Supervise Network	C	41
C	Enforce IT Policies	Provide Client Support	C	42
C	Enforce IT Policies	Provide Prevention & Detections Services	C	43
C	Supervise Hardware	Operate Servers	C	44
C	Supervise Hardware	Provide Client Support	I	45

Plant	FRAMName OUT	FRAMName IN	GATE_IN	ID FRAM Coupling
C	Supervise Hardware	Operate Clients	C	46
C	Operate Servers	Provide Communication Services	P	47
C	Operate Servers	Provide IT Services	P	48
C	Provide Mitigation Services	Operate Servers	R	49
C	Provide Mitigation Services	Operate Clients	R	50
C	Provide Mitigation Services	Provide IT Services	R	51
C	Supervise Network	Provide Client Support	I	52
C	Supervise Network	Provide Prevention & Detections Services	I	53
C	Supervise Network	Operate Network	C	54
C	Provide Client Support	Operate Clients	R	55
C	Provide Communication Services	Operate Clients	R	56
C	Provide Communication Services	Control System	R	57
C	Provide IT Services	Operate Clients	R	58
C	Provide IT Services	Plan Material Supply	R	59
C	Provide IT Services	Plan Schedule	R	60
C	Provide IT Services	Analyse predicitive Maintenance	R	61
C	Provide Prevention & Detections Services	Operate Servers	C	62
C	Provide Prevention & Detections Services	Provide Client Support	C	63
C	Provide Prevention & Detections Services	Operate Clients	C	64
C	Provide Prevention & Detections Services	Operate Network	C	65
C	Operate Network	Operate Servers	R	66
C	Operate Network	Provide Communication Services	R	67
C	Operate Network	Operate Clients	R	68
C	Operate Network	Provide IT Services	R	69
C	Plan Material Supply	Plan Schedule	T	70
C	Plan Schedule	Plan Material Supply	I	71
C	Plan Schedule	Schedule	I	72
C	Schedule	Check & Prepare Equipment	T	73
C	Schedule	Feed Chemicals	T	74
C	Schedule	Start Reaction	T	75
C	Schedule	Control System	I	76
C	Store Chemicals	Feed Chemicals	I	77
C	Check & Prepare Equipment	Feed Chemicals	P	78
C	Feed Chemicals	Start Reaction	P	79
C	Start Reaction	Monitor Reaction	P	80
C	Monitor Reaction	Start Emergency Cooling Shutdown	I	81
C	Monitor Reaction	Control System	I	82
C	Monitor Reaction	Control Equipment Target Values	C	83
C	Control System	Do Quality Management	I	84
C	Control System	Start Reaction	C	85

Plant	FRAMName OUT	FRAMName IN	GATE_IN	ID FRAM Coupling
C	Control System	Start Emergency Cooling Shutdown	C	86
C	Control System	Control Equipment Target Values	C	87
C	Control System	Analyse predicitive Maintenance	I	88
C	Reactive Maintenance (Repair)	Schedule	T	89
C	Plan Maintenance	Plan Schedule	C	90
C	Plan Maintenance	Do planned maintenance	T	91
C	Analyse predicitive Maintenance	Plan Maintenance	I	92
C	Check Preventive Maintenance	Plan Maintenance	I	93

4.4.2 Datasets

The data gathered by the interviews and used in the FRAM analysis/simulation, are stored on the attached CD. An inclusion in this written thesis is not feasible, as more than 3.1 million result sets were generated.

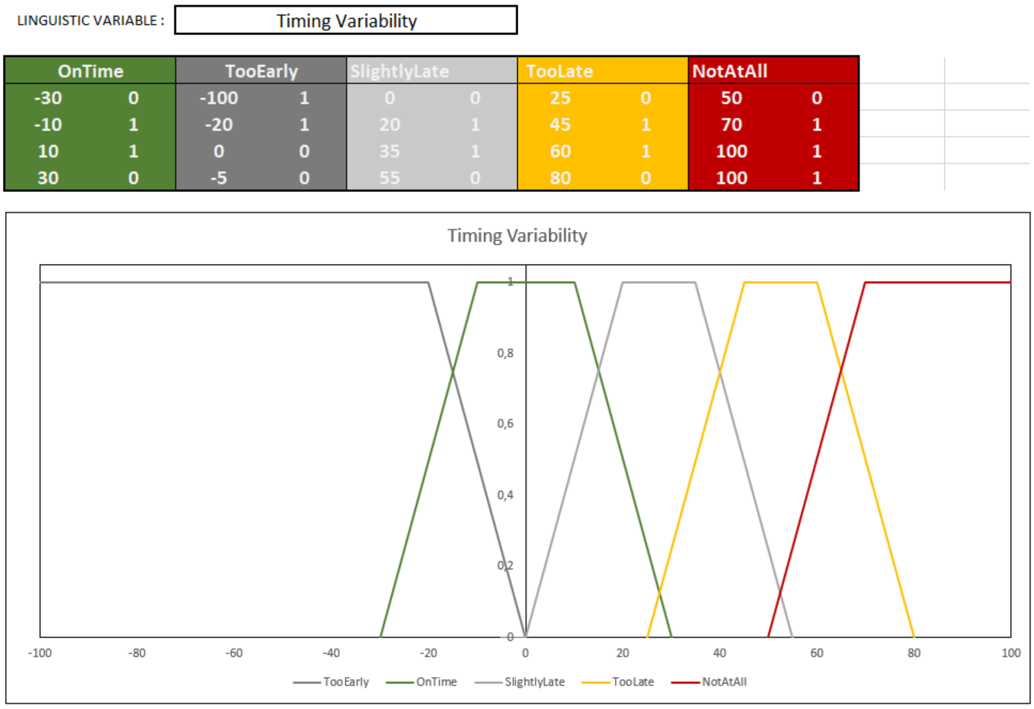
4.5 Fuzzy Set Theory and Fuzzy Logic

Zadeh (1965) introduced fuzzy sets to represent data and information maintaining non-statistical uncertainties. The strength of fuzzy logic lies in the combination of a mathematical approach and uncertainties associated with human cognitive processes, such as thinking and reasoning. The exact description of fuzzy logic can be found elsewhere . (Abul-Haggag & Barakat, 2013 Vol 3; Bandemer & Gottwald, 1995; Dutta, Boruah, & Ali, 2011; Isermann, 1998; Zadeh, 1965; Zadeh, 2008; Zukin & Young, 2010).

In the following chapters used linguistic variables, inference rules and the hierarchical fuzzy logic system are described.

4.5.1 Fuzzy Sets

Timing Variability is described with the linguistic variables on time, too early, slightly late, too late or not at all. The scale for timing variability starts at -100 and reaches up to +100. Figure 38 shows the fuzzy set used for timing variability.

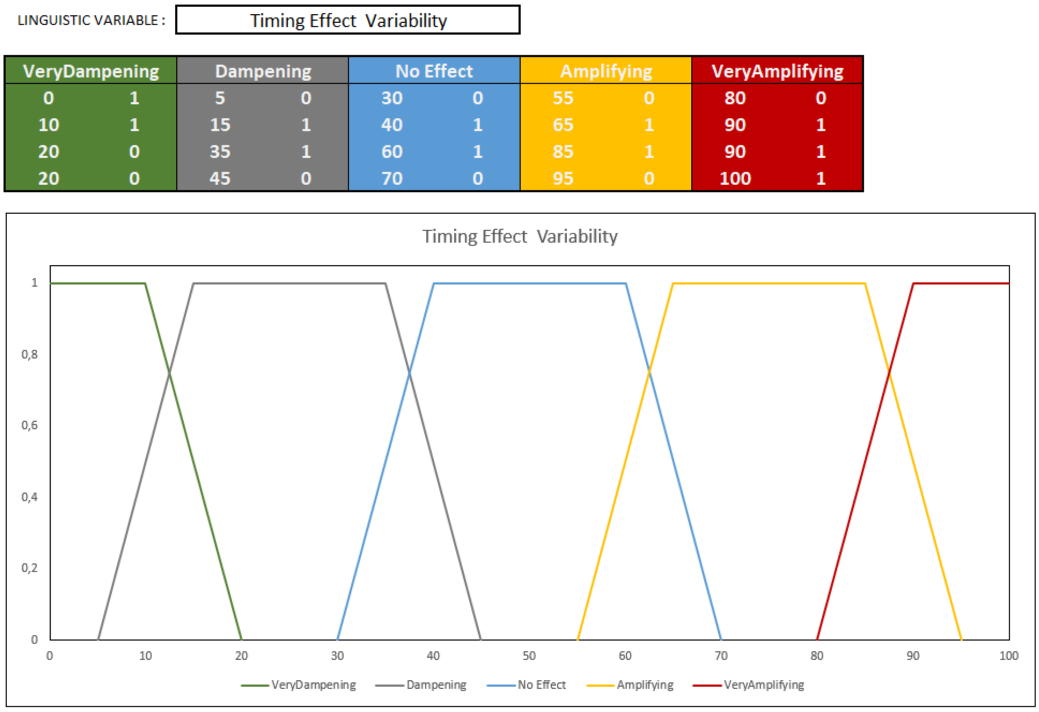


LINGUISTIC VARIABLE : Timing Variability

OnTime		TooEarly		SlightlyLate		TooLate		NotAtAll	
-30	0	-100	1	0	0	25	0	50	0
-10	1	-20	1	20	1	45	1	70	1
10	1	0	0	35	1	60	1	100	1
30	0	-5	0	55	0	80	0	100	1

Figure 38 Fuzzy Set Timing Variability

Timing effect is described with the linguistic variables very dampening, dampening, no effect, amplifying or very amplifying. The scale for timing variability starts at 0 and reaches up to 100. Figure 39 shows the fuzzy set used for timing effect variability.

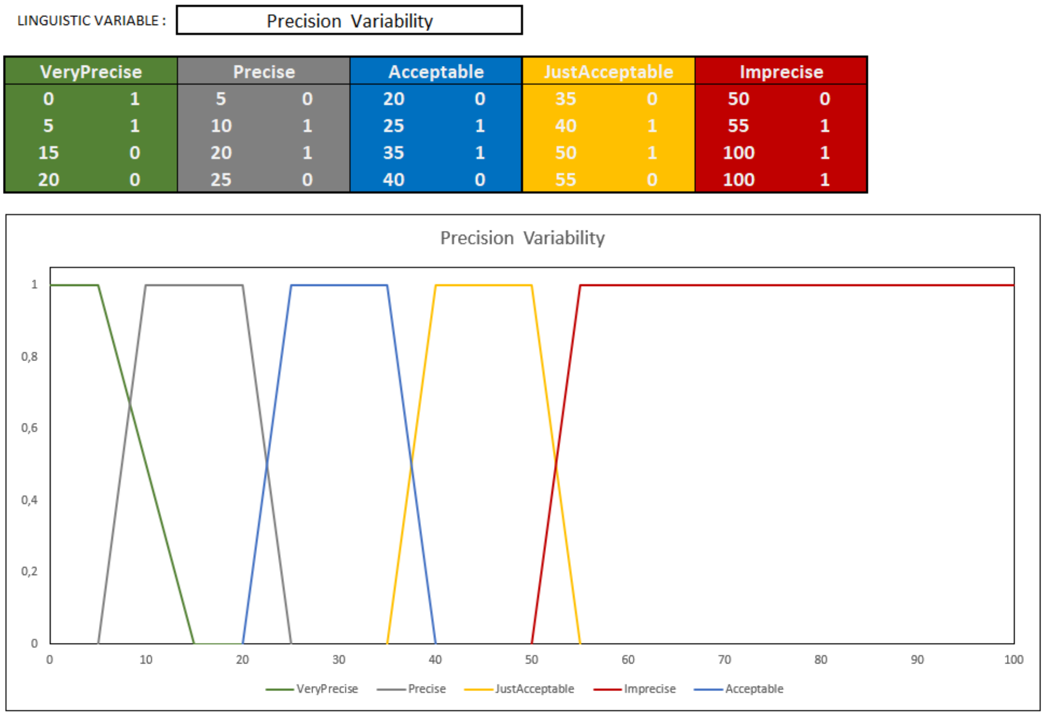


LINGUISTIC VARIABLE : Timing Effect Variability

VeryDampening		Dampening		No Effect		Amplifying		VeryAmplifying	
0	1	5	0	30	0	55	0	80	0
10	1	15	1	40	1	65	1	90	1
20	0	35	1	60	1	85	1	90	1
20	0	45	0	70	0	95	0	100	1

Figure 39 Fuzzy Set Timing Effect

Precision Variability is described with the linguistic variables precise, acceptable, just acceptable and imprecise. The scale for timing variability starts at 0 and reaches up to 100. Figure 40 shows the fuzzy set used for precision variability.

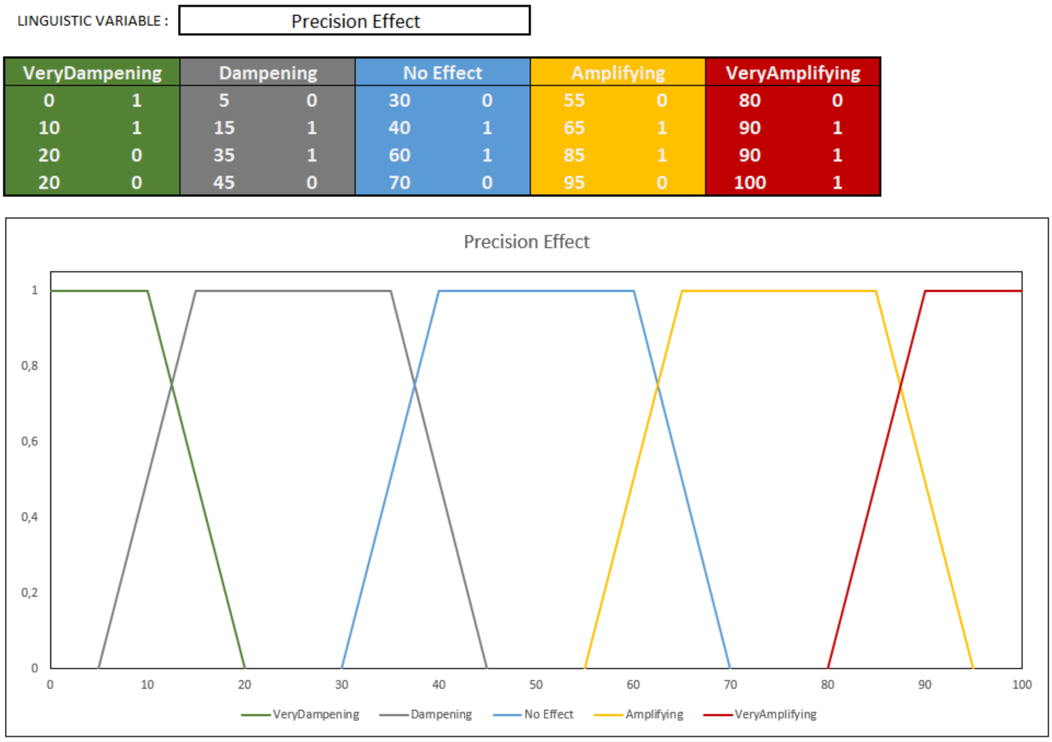


LINGUISTIC VARIABLE : Precision Variability

VeryPrecise		Precise		Acceptable		JustAcceptable		Imprecise	
0	1	5	0	20	0	35	0	50	0
5	1	10	1	25	1	40	1	55	1
15	0	20	1	35	1	50	1	100	1
20	0	25	0	40	0	55	0	100	1

Figure 40 Fuzzy Set Precision Variability

Precision effect is described with the linguistic variables very dampening, dampening, no effect, amplifying or very amplifying. The scale for precision variability starts at 0 and reaches up to 100. Figure 41 shows the fuzzy set used for precision effect variability.

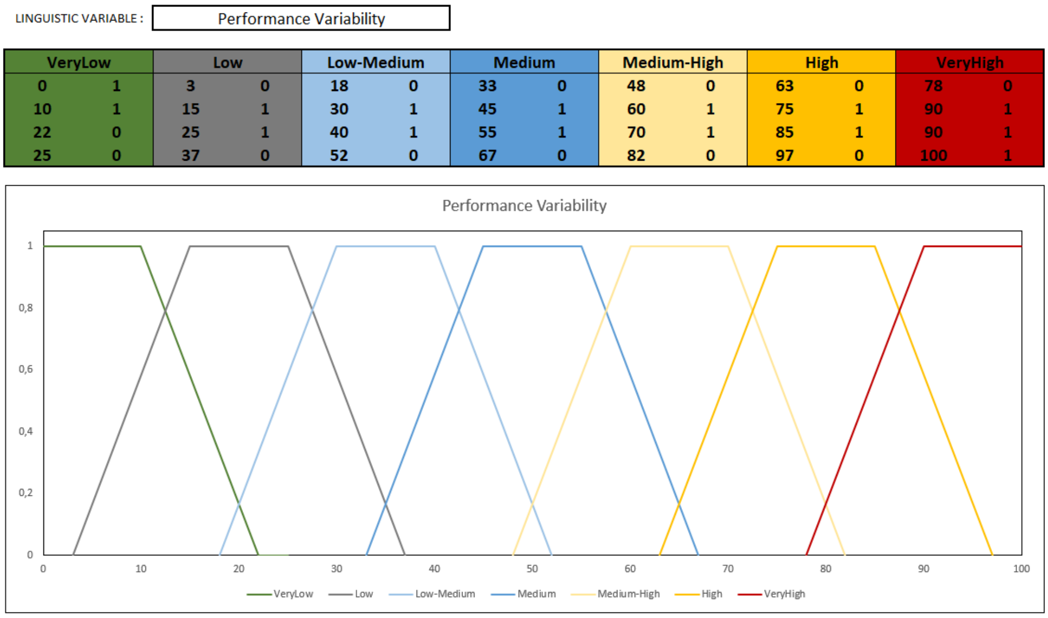


LINGUISTIC VARIABLE : Precision Effect

VeryDampening		Dampening		No Effect		Amplifying		VeryAmplifying	
0	1	5	0	30	0	55	0	80	0
10	1	15	1	40	1	65	1	90	1
20	0	35	1	60	1	85	1	90	1
20	0	45	0	70	0	95	0	100	1

Figure 41 Fuzzy Set Precision Effect

Performance variability is described with the linguistic variables very low, low, low-medium, medium, medium-high, high or very high. The scale for performance variability starts at 0 and reaches up to 100. shows the fuzzy Figure 42 set used for performance variability.

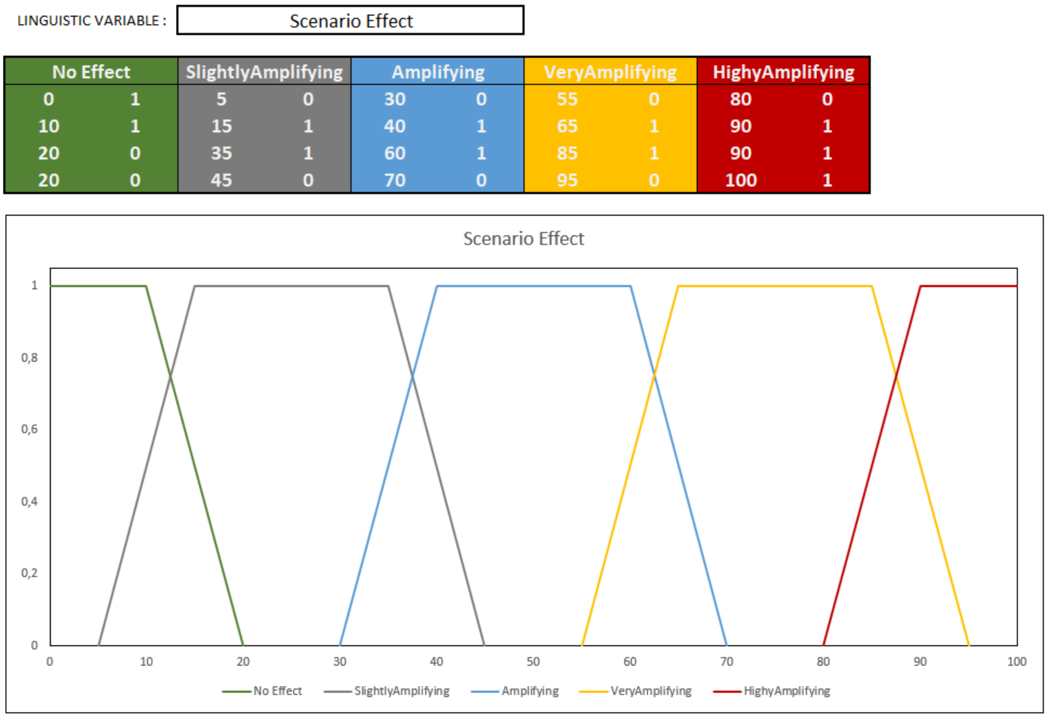


LINGUISTIC VARIABLE : Performance Variability

VeryLow		Low		Low-Medium		Medium		Medium-High		High		VeryHigh	
0	1	3	0	18	0	33	0	48	0	63	0	78	0
10	1	15	1	30	1	45	1	60	1	75	1	90	1
22	0	25	1	40	1	55	1	70	1	85	1	90	1
25	0	37	0	52	0	67	0	82	0	97	0	100	1

Figure 42 Fuzzy Set Performance Variability

The scenario effect is described with the linguistic variables very dampening, dampening, no effect, amplifying or very amplifying. The scale for scenario variability starts at 0 and reaches up to 100. Figure 43 shows the fuzzy set used for scenario effect variability.



LINGUISTIC VARIABLE : Scenario Effect

No Effect		SlightlyAmplifying		Amplifying		VeryAmplifying		HighyAmplifying	
0	1	5	0	30	0	55	0	80	0
10	1	15	1	40	1	65	1	90	1
20	0	35	1	60	1	85	1	90	1
20	0	45	0	70	0	95	0	100	1

Figure 43 Fuzzy Set Scenario Effect

4.5.2 Inference Rules

Semantic descriptions, so called fuzzy logic proposition or if-then propositions are used to map fuzzy sets to other fuzzy sets. For example:

$IF\ (TimingVariability\ IS\ OnTime) AND\ (TimingEffect\ IS\ Amplifying)$
$THEN\ TimingVariation\ IS\ Medium$

or

$IF\ (PerformanceVariability\ IS\ \mathrm{Low}) AND\ (ScenarioEffect\ IS\ Amplifying)$
$THEN\ ScenarioPerformanceVariability\ IS\ Medium$

Several of these rules are then combined into one ruleset. One disadvantages of a direct ruleset where all possible combinations are joined is the high number of rules necessary to describe the system. In this research the number of rules can be calculated as:

$$\sum rules\ = n_{TimingVariability} * n_{TimingEffect}\ * n_{PrecisionVariability} * n_{PrecisionEffect}\ *\ n_{ScenarioEffect}$$

$$\sum rules\ = 5 * 5 * 5 * 5 * 5 = 3125$$

where $n_{fuzzy\ set}$ denotes the number of linguistic variables in the corresponding fuzzy set.

One way to avoid this high number of rules is to introduce a hierarchical fuzzy system (Šindelář, 2005). In his critique on fuzzy systems Šindelář states: „A rule explosion is a fundamental limitation of fuzzy systems because the number of rules increases exponentially as the number of input variables increases.” He describes hierarchical fuzzy sets as a viable alternative, to reduce complexity and improve transparency of the system. Figure 44 shows the different construction of fuzzy systems. In a large fuzzy system all inputs are mapped to the fuzzy system, in a hierarchical design. The system is decomposed into smaller fuzzy system.

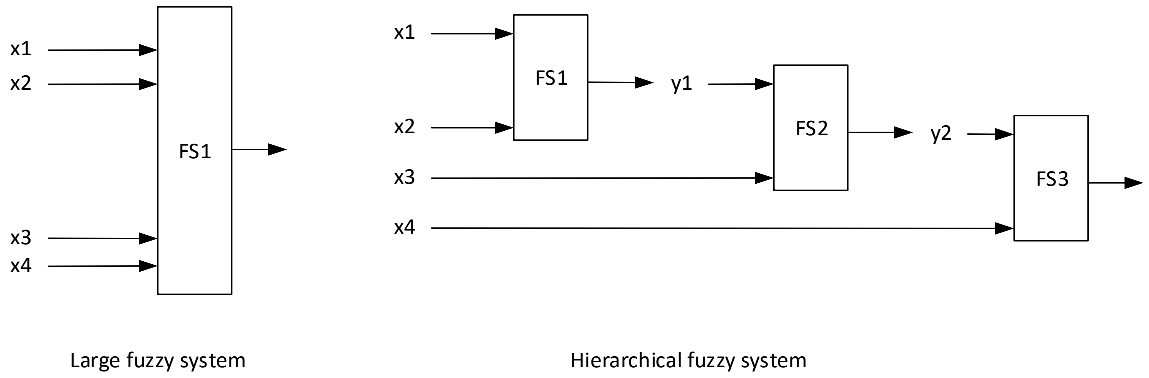
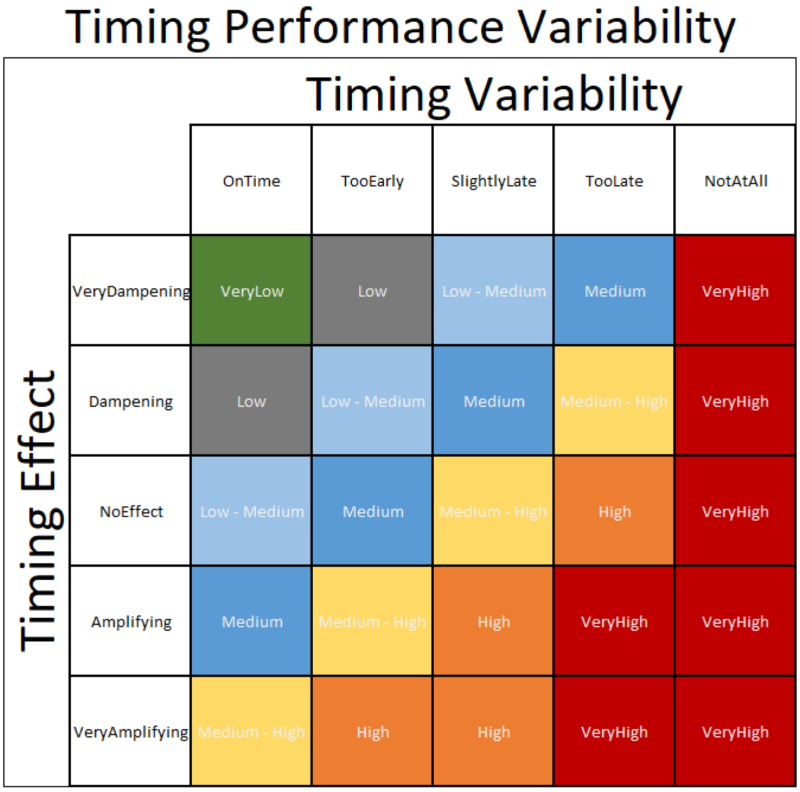


Figure 44 Large and hierarchical fuzzy system (Šindelář, 2005)

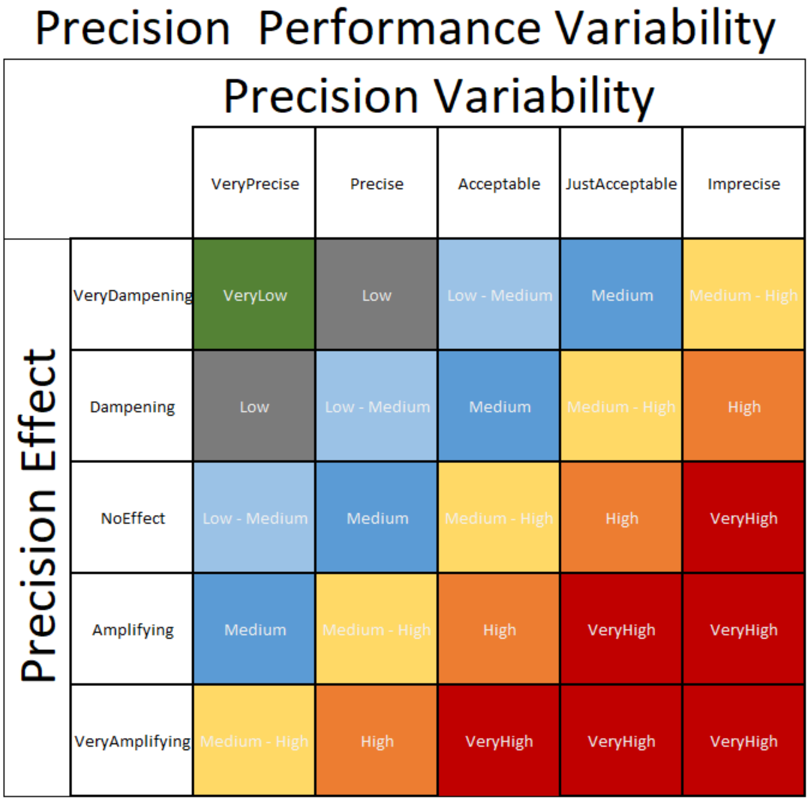
By using a hierarchical fuzzy logic system as depicted in Figure 49, the number of rules can be reduced to 134. The ruleset matrix for combining timing variability with timing effect is shown in Figure 45. The ruleset matrix for combining precision variability with precisioneffect is shown in Figure 46. The ruleset matrix for combining timing performance variability with precision performance variability is shown in Figure 47. The ruleset matrix for combining performance variability with scenario effect is shown in Figure 48.



Timing Performance Variability

		Timing Variability				
		OnTime	TooEarly	SlightlyLate	TooLate	NotAtAll
Timing Effect	VeryDampening	VeryLow	Low	Low - Medium	Medium	VeryHigh
	Dampening	Low	Low - Medium	Medium	Medium - High	VeryHigh
	NoEffect	Low - Medium	Medium	Medium - High	High	VeryHigh
	Amplifying	Medium	Medium - High	High	VeryHigh	VeryHigh
	VeryAmplifying	Medium - High	High	High	VeryHigh	VeryHigh

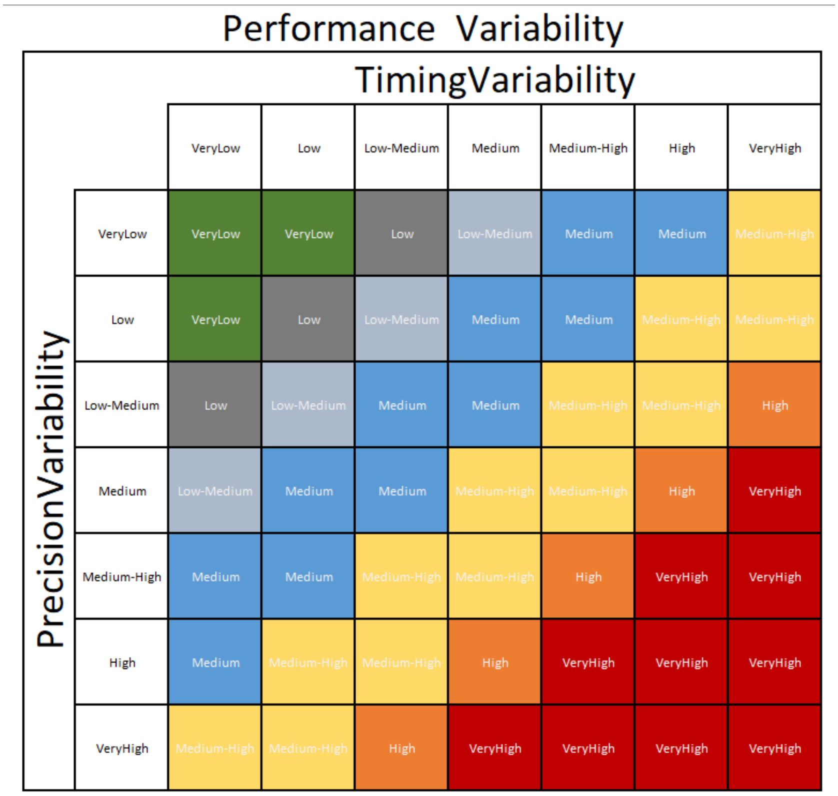
Figure 45 Ruleset Timing Perfomance Variability



Precision Performance Variability

		Precision Variability				
		VeryPrecise	Precise	Acceptable	JustAcceptable	Imprecise
Precision Effect	VeryDampening	VeryLow	Low	Low - Medium	Medium	Medium - High
	Dampening	Low	Low - Medium	Medium	Medium - High	High
	NoEffect	Low - Medium	Medium	Medium - High	High	VeryHigh
	Amplifying	Medium	Medium - High	High	VeryHigh	VeryHigh
	VeryAmplifying	Medium - High	High	VeryHigh	VeryHigh	VeryHigh

Figure 46 Ruleset Precision Perfomance Variability



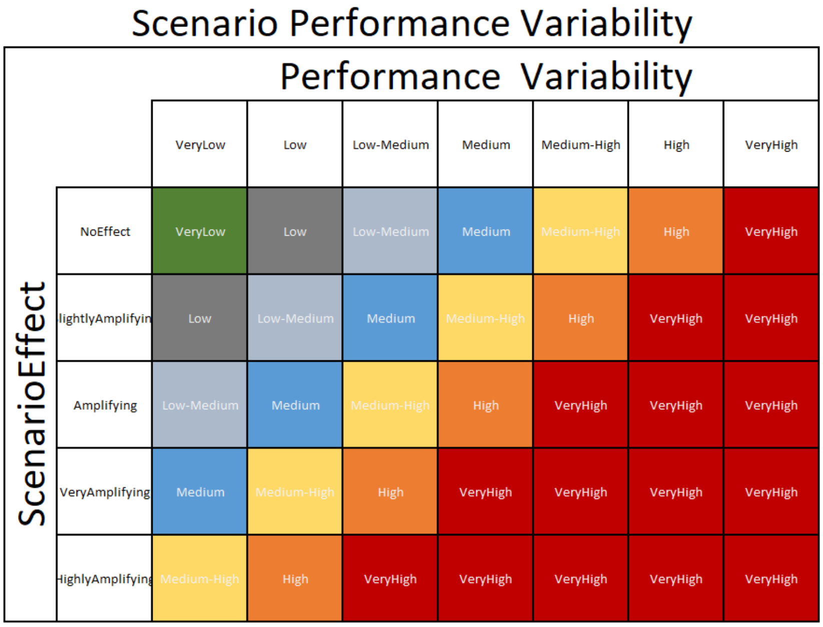
Performance Variability

TimingVariability

PrecisionVariability

	VeryLow	Low	Low-Medium	Medium	Medium-High	High	VeryHigh
VeryLow	VeryLow	VeryLow	Low	Low-Medium	Medium	Medium	Medium-High
Low	VeryLow	Low	Low-Medium	Medium	Medium	Medium-High	Medium-High
Low-Medium	Low	Low-Medium	Medium	Medium	Medium-High	Medium-High	High
Medium	Low-Medium	Medium	Medium	Medium-High	Medium-High	High	VeryHigh
Medium-High	Medium	Medium	Medium-High	Medium-High	High	VeryHigh	VeryHigh
High	Medium	Medium-High	Medium-High	High	VeryHigh	VeryHigh	VeryHigh
VeryHigh	Medium-High	Medium-High	High	VeryHigh	VeryHigh	VeryHigh	VeryHigh

Figure 47 Ruleset Perfomance Variability



Scenario Performance Variability

Performance Variability

ScenarioEffect

	VeryLow	Low	Low-Medium	Medium	Medium-High	High	VeryHigh
NoEffect	VeryLow	Low	Low-Medium	Medium	Medium-High	High	VeryHigh
lightlyAmplifyin	Low	Low-Medium	Medium	Medium-High	High	VeryHigh	VeryHigh
Amplifying	Low-Medium	Medium	Medium-High	High	VeryHigh	VeryHigh	VeryHigh
VeryAmplifying	Medium	Medium-High	High	VeryHigh	VeryHigh	VeryHigh	VeryHigh
HighlyAmplifying	Medium-High	High	VeryHigh	VeryHigh	VeryHigh	VeryHigh	VeryHigh

Figure 48 Ruleset Scenario Perfomance Variability

4.5.3 Defuzzification

Several methods for defuzzification are described in the literature. This research uses the centroid method, where the center of gravity of the membership function is mapped to a crisp number.

4.5.4 Complete Hierarchical Fuzzy Logic System

The complete fuzzy hierarchical inference system to simulate the one function of the instantiated system and the impact of disturbances is shown in Figure 49. Timing and timing effect variabilities are mapped via ruleset A to timing performance variability, precision and precision effect variability to precision performance variability using ruleset B. The timing and precision performance variabilities are mapped via ruleset C to the performance variability. Scenarios are coupled with the instantiated performance variability using ruleset D to give a scenario performance variability for each function.

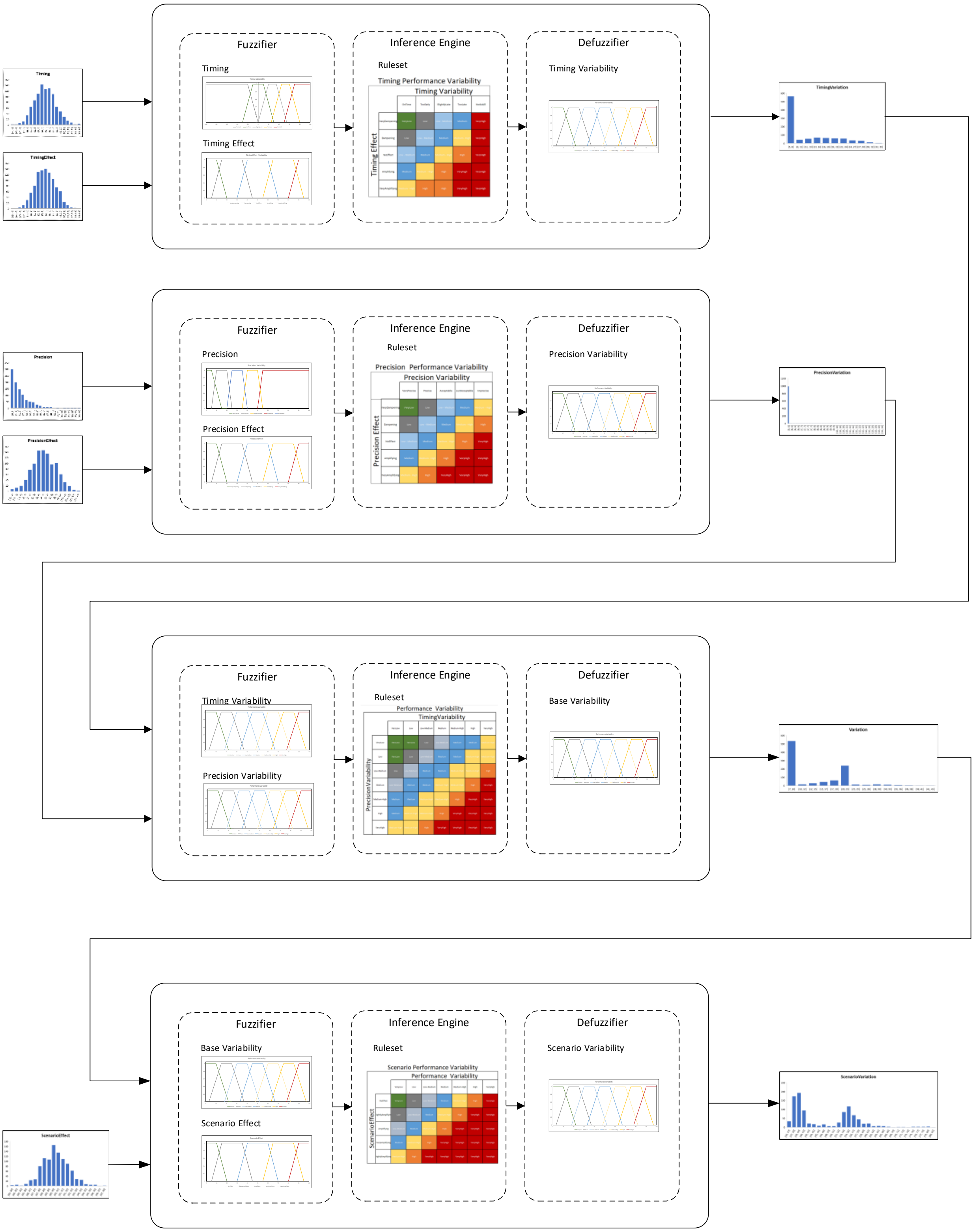
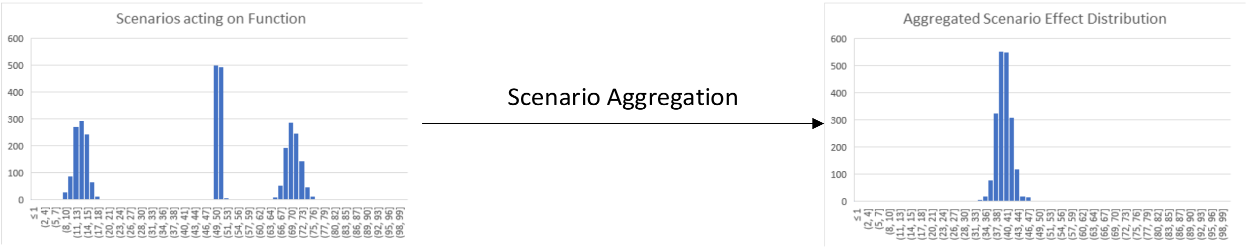


Figure 49 Fuzzy Hierarchical Inference System

4.6 Scenarios

An accident scenario can be considered as characterization of a predicted situation. Actions, events and developments are combined to create a potential scenario. Basic events can be aggregated to result in different scenarios. Each scenario is evaluated for its effect on the performance variability of each output function (see chapters 4.5.1 and 4.5.2. for the scenario effect fuzzy set and scenario effect ruleset). Scenarios can be combined or aggregated to new scenarios encompassing their information. A formula to aggregate scenarios was developed and used in a Monte Carlo style for the distribution generation of the new aggregated scenario.



$$Effect_{cumulative} = Mean + \ Deviation * Deviation\ Factor$$

$$Effect_{cumulative} = \frac{\sum_{i=1}^{n} Effect}{n} + \frac{\sum_{i=1}^{n}(Effect - 50)}{n} * (1 - \frac{1}{50} * \left|\sum_{i=1}^{n} Effect - 50\right|)$$

Several scenarios are used in this thesis. All scenarios were verified by the experts as plausible and having a possible effect on the system. Table 14 describes 8 base scenarios and 5 aggregated scenarios.

Table 14 Scenarios used in the simulation

Scenario Name	Scenario Description
Change of Shift	That time during the working day, when one group of operators or employees arrives for work and another group prepares to leave. Communication lapses can lead to high risk situations as key pieces of information are missing.
Update Software	Updating and upgrading IT systems, due to performance, safety or security issues is a necessity, as every piece of hardware and software, will need to be updated at some point of time (Venezia, 2012). “From a purely logistical point of view, there are only three possible outcomes to a firmware or software update: • Everything goes as planned. Bugs are fixed or new functionality is added, and everything proceeds normally. • There's no noticeable difference in operation or administration aside from a version number ticking upward.

	• You've just turned a working system into a brick.”
Weak understanding of process	Weak understanding of the chemical process can easily lead to misinterpretation of data relating to process variables (Kletz, 1982, 1991).
Deadline pressure	Time deadline pressure occurs when at a specific point in time for task completion is specified and it is difficult to complete the required work by the deadline. Besnard and Hollnagel (2014) argues that that as deadline pressure increases, performance declines because important cues are ignored.
Deviation of process variables	Chemical plants are complex systems and use several dynamic process variables for their operation. Rapidly changing conditions due to small deviations in process state variables pose a challenging problem in process industries.
DDOS Attack	There are several types of Distributed Denial of Service (DDOS) attacks. While some are targeted directly on server infrastructure, others use weaknesses in applications or communication protocols. Goal of the attack is to deny authorized users access to IT services.
Valve Condition Deterioration	This is maintenance related scenario. Caused by corrosion or blocking, a deteriorating valve might induce a serious accident scenario.
Deviation from operating procedures	Risks are introduced by taking intentionally deviations from the rules or procedures. Short-cuts or non-compliance with procedures usually result from an intention to get the job done despite the consequences.
Mix 1	Aggregation of Scenarios Change of Shift and Update Software
Mix 2	Aggregation of Scenarios Update Software, Weak Understanding of Process And DDOS Attack
Mix 3	Aggregation of Scenarios Weak Understanding Process, Deviation of Process and Valve Condition Deterioration
Mix 4	Aggregation of Scenarios Update Software and Deadline Pressure
Mix 5	Aggregation of Scenarios Change of Shift and Update Software

4.7 Model Data Base Design

The database model used in this thesis uses five tables. In FRAMCFG, the name of the FRAM function and its description are stored, scenarios names and descriptions are stored in FRAMScenarioCFG, Couplings between functions are stored in FRAMCouplings, used distributions associated with the couplings are stored with their distribution parameter description in FRAMDistribution. The results are stored in table FRAMResults (see Figure 50)

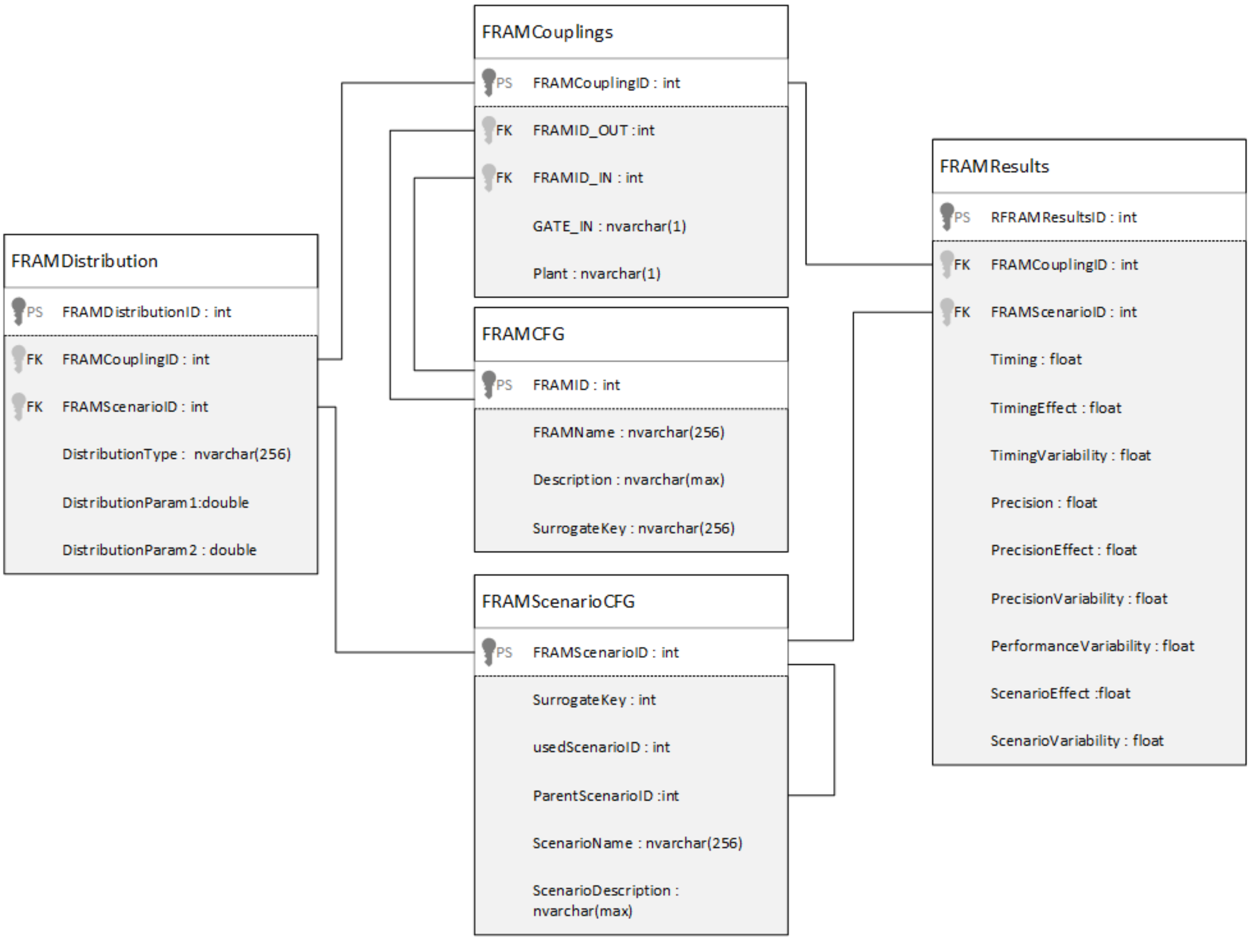


Figure 50 UML Database Diagram of Model

4.8 Explanatory and Response Variables

As explanatory variables, this thesis uses the following variables:

- Digital maturity level of a chemical plant, as defined in chapter 4.1 ranging from “analog” (1) to “chemistry 4.0” (5)
- Timing, as defined in chapter 4.5.1 ranging from “too early” (-100) to “not at all” (+100)
- Timing effect, as defined in chapter 4.5.1 ranging from “highly dampening” (0) to “highly amplifying” (+100)
- Precision, as defined in chapter 4.5.1 ranging from “very precise” (0) to “imprecise” (+100)
- Precision effect, as defined in chapter 4.5.1 ranging from “highly dampening” (0) to “highly amplifying” (+100)
- Scenario effect, as defined in chapter 4.5.1 ranging from “no effect” (0) to “highly amplifying” (+100)

As response variables the following variables were chosen:

- Probability of top event for FTA analysis probability - the extent to which the top event of the fault tree, or system failure condition is likely to happen.
- Performance variability for a FRAM function coupling, as defined in chapter 4.5.1 ranging from “very low” (0) to “very high” (+100)
- Aggregated performance variability for the plant, as defined in chapter 4.5.1 ranging from “very low” (0) to “very high” (+100)
- The number of critical couplings
- The Kolmogorov-Smirnov Effect D as described in the next chapter.
- Percentage Critical, the area under the distribution function for values higher than the threshold defined critical, as defined below, ranging from 0 to 1

To identify critical couplings, a performance variabilities threshold was defined and set to 82. A situation was defined as critical if the timing variability was slightly late and amplifying and precision variability was just acceptable and neutral. Taking into account other combinations the threshold was set to 82. The analysis recognizes a coupling as critical if the cumulative distribution of the coupling higher than 82, exceed 5%. As measure *percentCritical* is introduced:

$$percentCritical = \frac{\int_{82}^{100} PerformanceVariability}{\int_{0}^{100} PerformanceVariability}$$

setting the area under the distribution function with values higher than the threshold value into relation to the whole area. Essentially it gives the fraction of the distribution over the threshold. In Figure 51 the red und blue distributions are deemed critical, because the fraction of the distribution over the threshold is over 5%, with the red distribution having a much higher criticality (close to 1) as the blue distribution (close to 0.1). The green distribution is not critical.

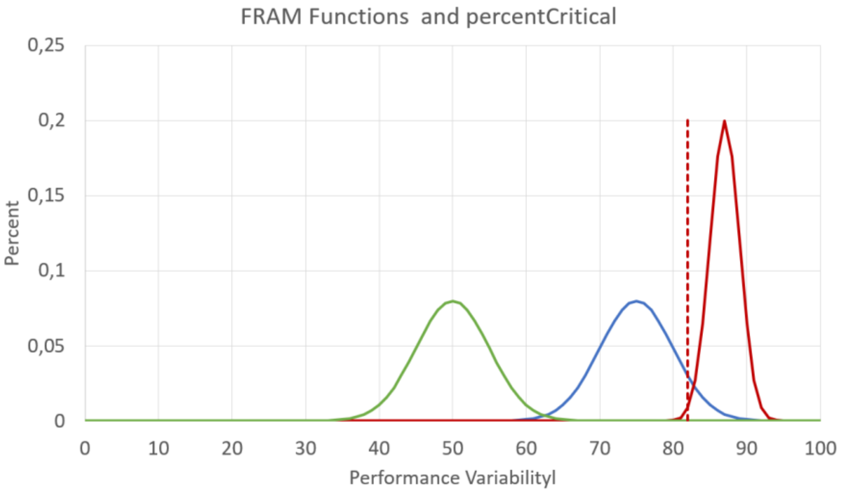
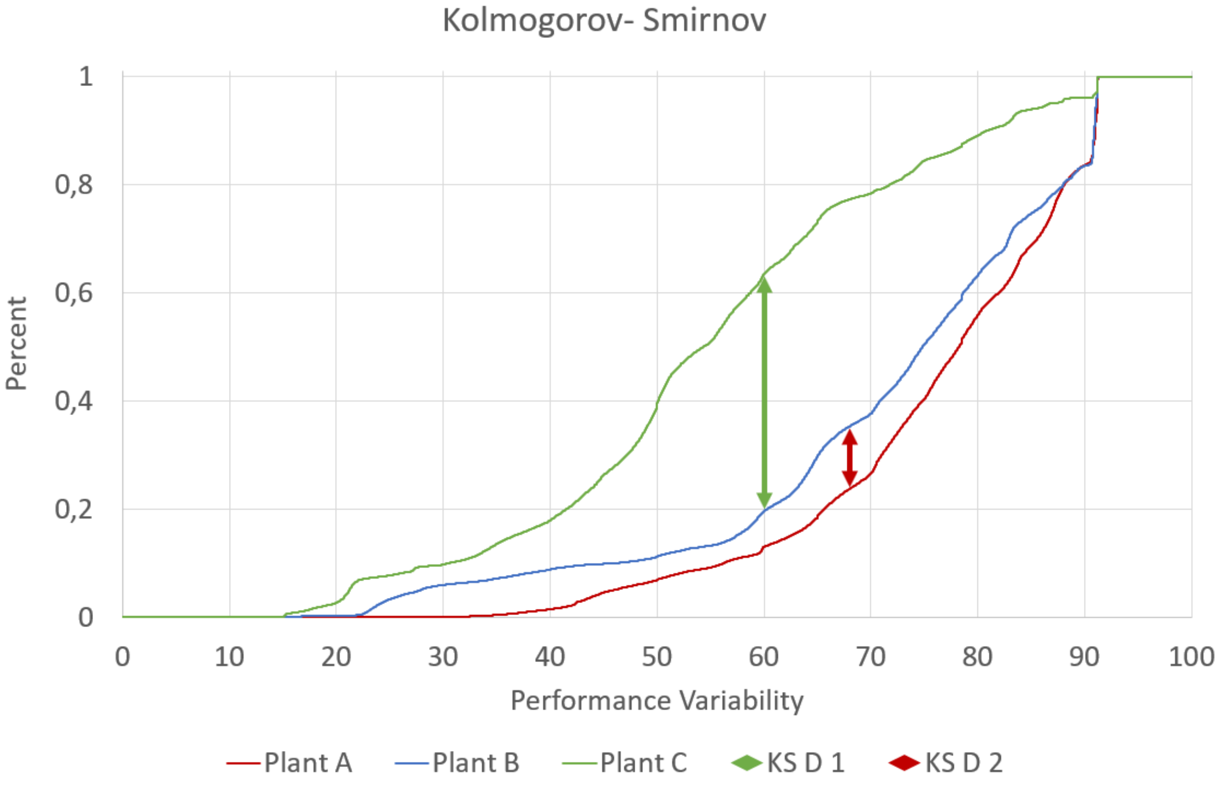


Figure 51 Distribution Functions and percentCritical

4.9 Data Analytic Plan

For comparing two or more empirical distributions, usual performed test like student-t test are failing because they compare one distribution with the normal distribution. For this reason, the Kolmogorov Smirnow test was used in this thesis. One additional advantage of the Kolmogorov Smirnow test is that it provides a certain measure of effect – the greatest distance between the cumulative distribution functions – D. A p-value < 0.05 means that the two-number series do not belong to the same distribution.



Box plots and cumulative distribution functions are used for comparison of plant A, B and C. Pearson product-moment correlation was used to identify correlation between two variables.

5 RESULTS AND ANALYSIS

In this chapter the results of the study are presented and discussed. In the first section the results of the FTA analysis are presented and discussed. In the following sections the results of FRAM analysis are discussed.

5.1 Fault tree analysis of runaway reaction caused by chemical process deviations

The fault trees were modelling and calculated using TopEvent FTA Express 2017. The calculation results for the probability of failure in case of deviations in process parameters are shown in Table 18.

5.1.1 Results for plant A

In plant A (see Figure 52) possible failures center around operator mishandling situations, and failure of cooling system and the emergency cooling system. Table 15 shows the resulting minimal cut set for plant A, showing that the most likely failure combination leading to the top event are “activation conditions for alarming are bypassed” and “operator does not diagnose emergency situation”.

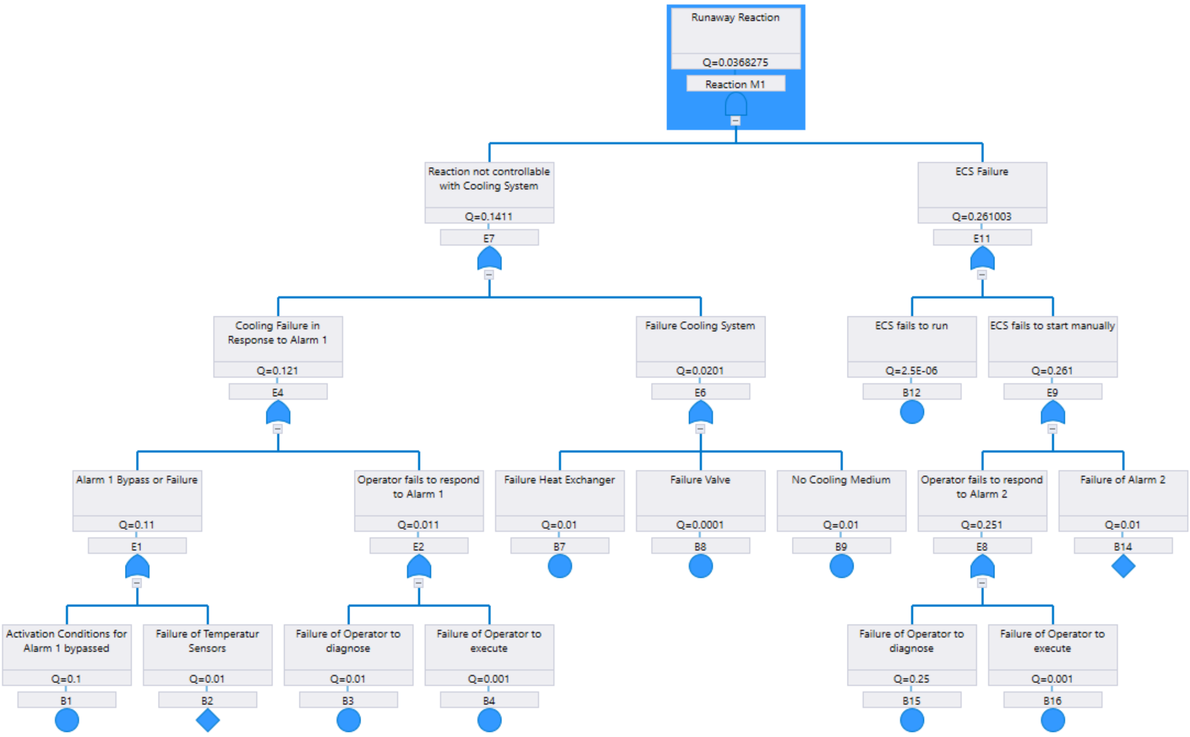
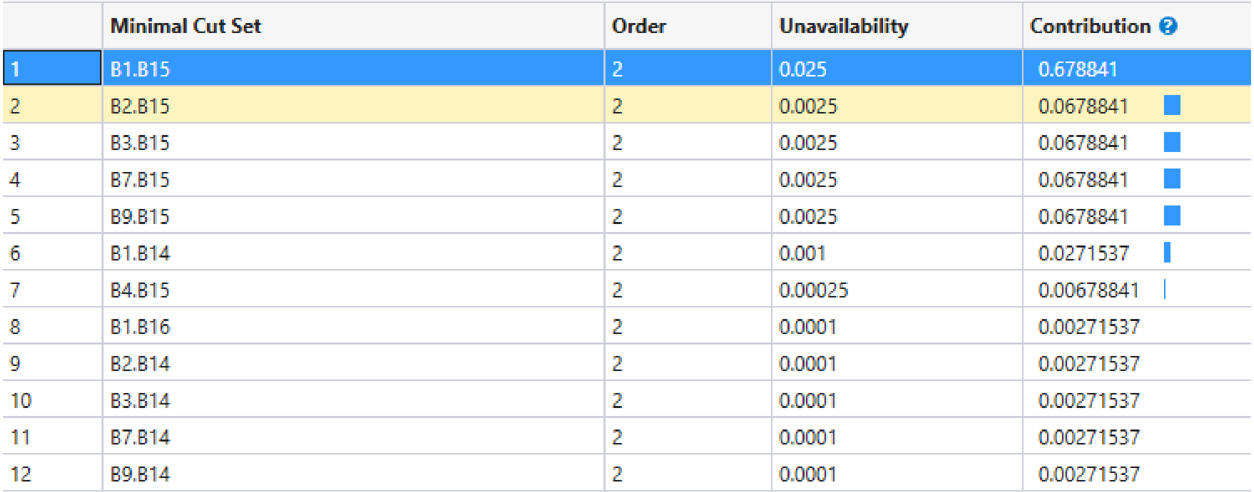

Runaway Reaction
Q=0.0368275
Reaction M1
Reaction not controllable with Cooling System
Q=0.1411
E7
ECS Failure
Q=0.261003
E11
Cooling Failure in Response to Alarm 1
Q=0.121
E4
Failure Cooling System
Q=0.0201
E6
ECS fails to run
Q=2.5E-06
B12
ECS fails to start manually
Q=0.261
E9
Alarm 1 Bypass or Failure
Q=0.11
E1
Operator fails to respond to Alarm 1
Q=0.011
E2
Failure Heat Exchanger
Q=0.01
B7
Failure Valve
Q=0.0001
B8
No Cooling Medium
Q=0.01
B9
Operator fails to respond to Alarm 2
Q=0.251
E8
Failure of Alarm 2
Q=0.01
B14
Activation Conditions for Alarm 1 bypassed
Q=0.1
B1
Failure of Temperatur Sensors
Q=0.01
B2
Failure of Operator to diagnose
Q=0.01
B3
Failure of Operator to execute
Q=0.001
B4
Failure of Operator to diagnose
Q=0.25
B15
Failure of Operator to execute
Q=0.001
B16

Figure 52 Fault tree for runaway reaction plant A

Table 15 FTA Minimal Cut Set - Plant A



	Minimal Cut Set	Order	Unavailability	Contribution
1	B1.B15	2	0.025	0.678841
2	B2.B15	2	0.0025	0.0678841
3	B3.B15	2	0.0025	0.0678841
4	B7.B15	2	0.0025	0.0678841
5	B9.B15	2	0.0025	0.0678841
6	B1.B14	2	0.001	0.0271537
7	B4.B15	2	0.00025	0.00678841
8	B1.B16	2	0.0001	0.00271537
9	B2.B14	2	0.0001	0.00271537
10	B3.B14	2	0.0001	0.00271537
11	B7.B14	2	0.0001	0.00271537
12	B9.B14	2	0.0001	0.00271537

5.1.2 Results for Plant B

Plant B adds a control system and simple controllers (see Figure 53). The probability of the top event is lower (see Table 18) The minimal cut set for plant B (see Table 16 FTA Minimal Cut Set - Plant B) relates to “activation conditions for alarming are bypassed” and” the ECS does not start automatically” and “the operator does not diagnose the emergency situation”.

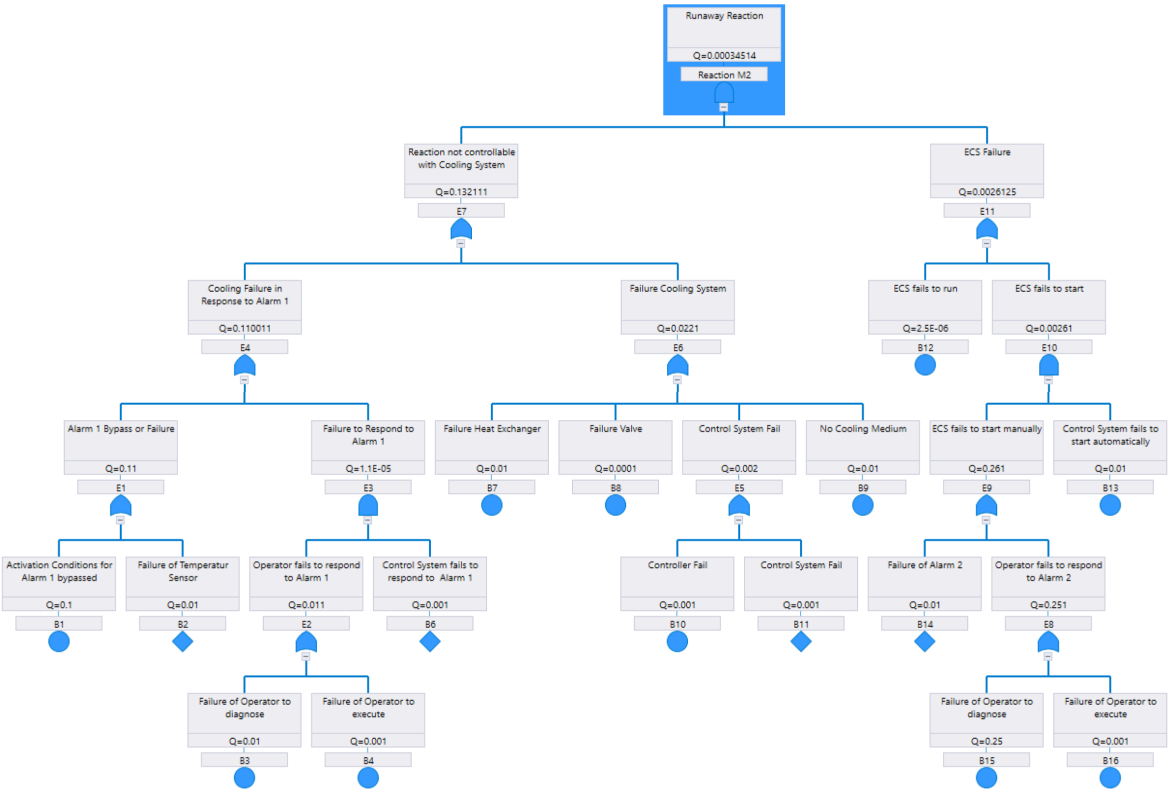
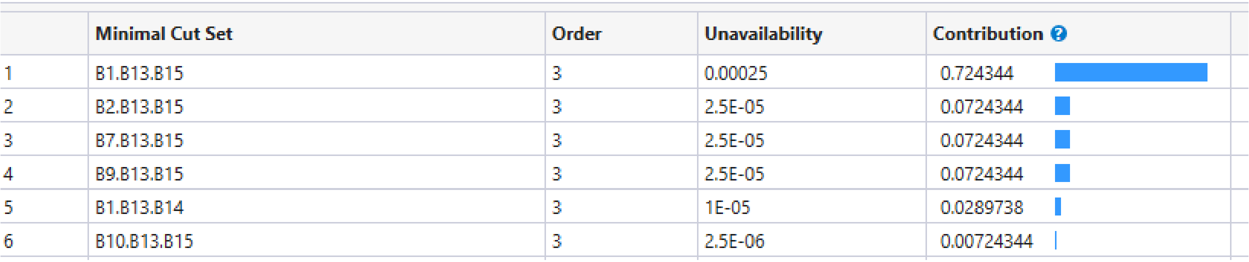

Runaway Reaction
Q=0.00034514
Reaction M2
Reaction not controllable with Cooling System
Q=0.132111
E7
ECS Failure
Q=0.0026125
E11
Cooling Failure in Response to Alarm 1
Q=0.110011
E4
Failure Cooling System
Q=0.0221
E6
ECS fails to run
Q=2.5E-06
B12
ECS fails to start
Q=0.00261
E10
Alarm 1 Bypass or Failure
Q=0.11
E1
Failure to Respond to Alarm 1
Q=1.1E-05
E3
Failure Heat Exchanger
Q=0.01
B7
Failure Valve
Q=0.0001
B8
Control System Fail
Q=0.002
E5
No Cooling Medium
Q=0.01
B9
ECS fails to start manually
Q=0.261
E9
Control System fails to start automatically
Q=0.01
B13
Activation Conditions for Alarm 1 bypassed
Q=0.1
B1
Failure of Temperatur Sensor
Q=0.01
B2
Operator fails to respond to Alarm 1
Q=0.011
E2
Control System fails to respond to Alarm 1
Q=0.001
B6
Controller Fail
Q=0.001
B10
Control System Fail
Q=0.001
B11
Failure of Alarm 2
Q=0.01
B14
Operator fails to respond to Alarm 2
Q=0.251
E8
Failure of Operator to diagnose
Q=0.01
B3
Failure of Operator to execute
Q=0.001
B4
Failure of Operator to diagnose
Q=0.25
B15
Failure of Operator to execute
Q=0.001
B16

Figure 53 Fault tree for runaway reaction plant B

Table 16 FTA Minimal Cut Set - Plant B



	Minimal Cut Set	Order	Unavailability	Contribution ?
1	B1.B13.B15	3	0.00025	0.724344
2	B2.B13.B15	3	2.5E-05	0.0724344
3	B7.B13.B15	3	2.5E-05	0.0724344
4	B9.B13.B15	3	2.5E-05	0.0724344
5	B1.B13.B14	3	1E-05	0.0289738
6	B10.B13.B15	3	2.5E-06	0.00724344

5.1.3 Results for Plant C

Plant C adds additional safety by adding high controllers (see Figure 54). The resulting probability of the top event is considerably lower than for plant A and B (see Table 18 Results of FTA).

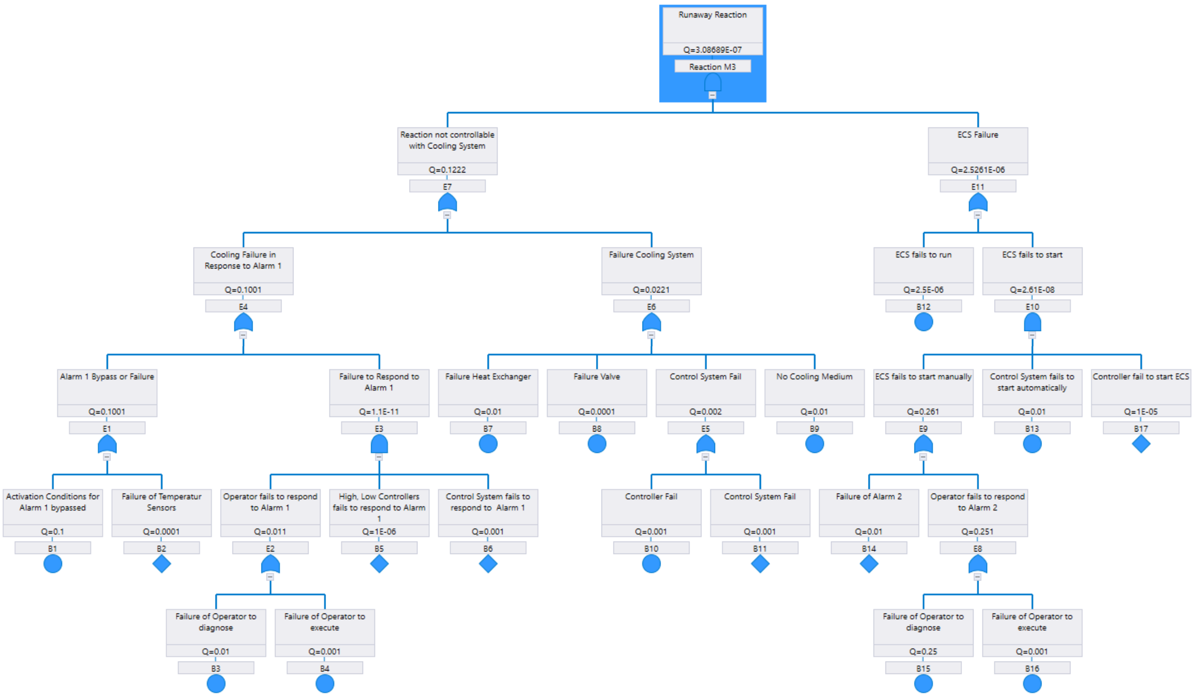
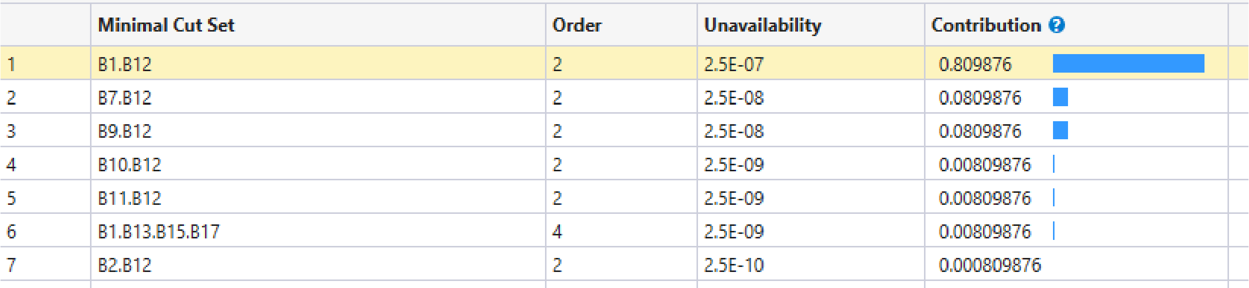

Runaway Reaction
Q=3.08689E-07
Reaction M3
Reaction not controllable with Cooling System
Q=0.1222
E7
ECS Failure
Q=2.5261E-06
E11
Cooling Failure in Response to Alarm 1
Q=0.1001
E4
Failure Cooling System
Q=0.0221
E6
ECS fails to run
Q=2.5E-06
B12
ECS fails to start
Q=2.61E-08
E10
Alarm 1 Bypass or Failure
Q=0.1001
E1
Failure to Respond to Alarm 1
Q=1.1E-11
E3
Failure Heat Exchanger
Q=0.01
B7
Failure Valve
Q=0.0001
B8
Control System Fail
Q=0.002
E5
No Cooling Medium
Q=0.01
B9
ECS fails to start manually
Q=0.261
E9
Control System fails to start automatically
Q=0.01
B13
Controller fail to start ECS
Q=1E-05
B17
Activation Conditions for Alarm 1 bypassed
Q=0.1
B1
Failure of Temperatur Sensors
Q=0.0001
B2
Operator fails to respond to Alarm 1
Q=0.011
E2
High, Low Controllers fails to respond to Alarm 1
Q=1E-06
B5
Control System fails to respond to Alarm 1
Q=0.001
B6
Controller Fail
Q=0.001
B10
Control System Fail
Q=0.001
B11
Failure of Alarm 2
Q=0.01
B14
Operator fails to respond to Alarm 2
Q=0.251
E8
Failure of Operator to diagnose
Q=0.01
B3
Failure of Operator to execute
Q=0.001
B4
Failure of Operator to diagnose
Q=0.25
B15
Failure of Operator to execute
Q=0.001
B16

Figure 54 Fault tree for runaway reaction plant C

Table 17 FTA Minimal Cut Set - Plant C



	Minimal Cut Set	Order	Unavailability	Contribution ?
1	B1.B12	2	2.5E-07	0.809876
2	B7.B12	2	2.5E-08	0.0809876
3	B9.B12	2	2.5E-08	0.0809876
4	B10.B12	2	2.5E-09	0.00809876
5	B11.B12	2	2.5E-09	0.00809876
6	B1.B13.B15.B17	4	2.5E-09	0.00809876
7	B2.B12	2	2.5E-10	0.000809876

The most dangerous minimal cut set for plant C (see Table 17 FTA Minimal Cut Set - Plant C) is if “activation conditions for alarming are bypassed” and “the ECS fails to work”

5.1.4 Discussion of results

As shown in Table 18, the higher the digitalization maturity level degree of the plant, the lower the probability of occurrence for the top event runaway reaction caused by deviation of process variables. Mapping the logarithm of the probability to the digitalization maturity levels of the plants indicates a relation between these variables (see Figure 55).

Table 18 Results of FTA

	probability	log(probability)
Plant A	0,0368000	-1,43
Plant B	0,0003450	-3,46
Plant C	0,0000003	-6,51

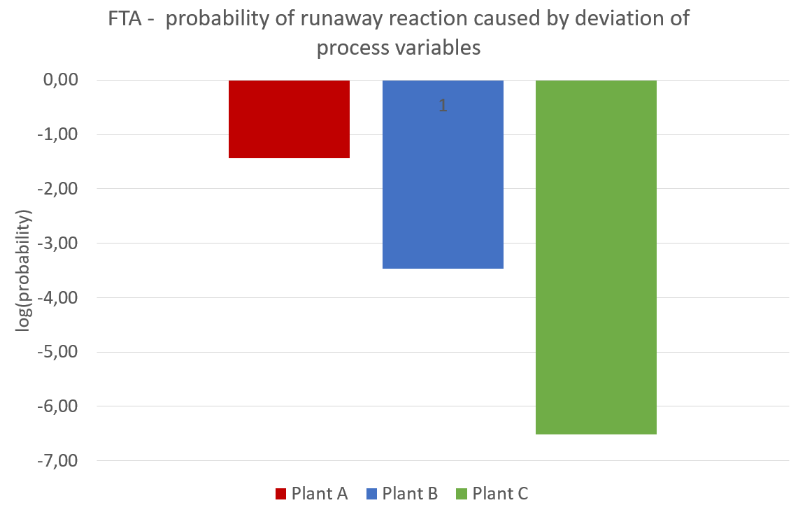
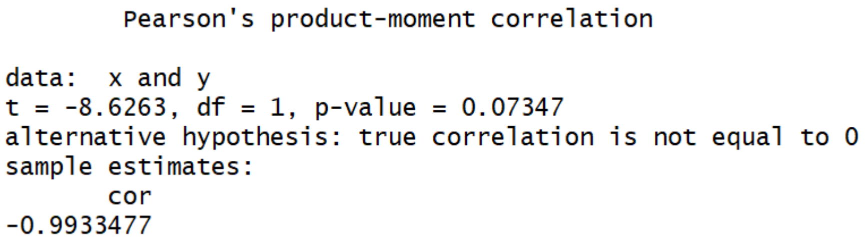


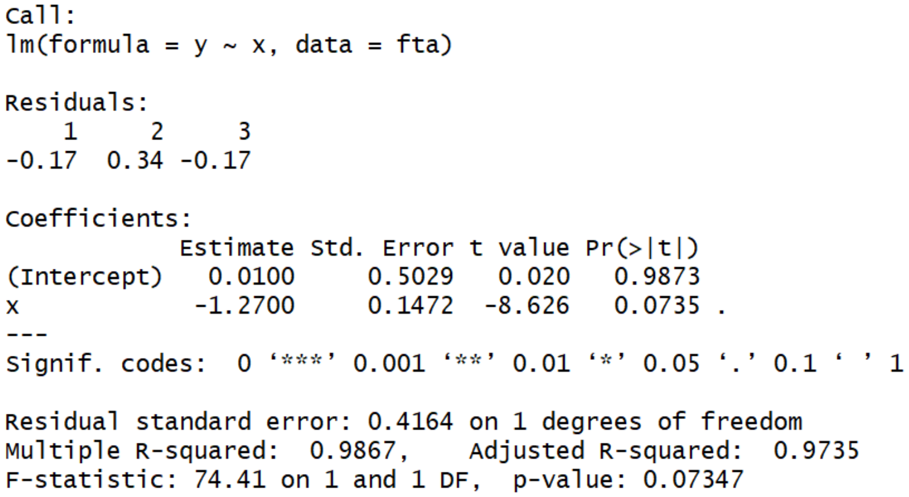
Figure 55 Result of FTA logarithm

While Pearson’s test for correlation indicate a correlation between digitalization maturity level and top-event probability occurrence, a linear regression analysis shows only weak support of a linear regression. The results of these statistical analysis should be taken with caution as the number of data points (three) is too low to make a statistically sound statement.



```
        Pearson's product-moment correlation

data:  x and y
t = -8.6263, df = 1, p-value = 0.07347
alternative hypothesis: true correlation is not equal to 0
sample estimates:
       cor 
-0.9933477 
```



```
Call:
lm(formula = y ~ x, data = fta)

Residuals:
    1     2     3 
-0.17  0.34 -0.17 

Coefficients:
            Estimate Std. Error t value Pr(>|t|)  
(Intercept)   0.0100     0.5029   0.020   0.9873  
x            -1.2700     0.1472  -8.626   0.0735 .
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 0.4164 on 1 degrees of freedom
Multiple R-squared:  0.9867,	Adjusted R-squared:  0.9735 
F-statistic: 74.41 on 1 and 1 DF,  p-value: 0.07347
```

The results demonstrate that increasing the digitalization leads to a lower top event probability (runaway reaction caused by deviation of process variables). Of interest is that the minimal cut sets for the plants are different. For all plants the condition “activation condition for alarm 1 bypassed” is included in the minimal cut set. For plant A, the minimal cut set is complemented with the condition “failure of operator to diagnose”. Plant B add to this cut set the condition “Control system fails to start ECS automatically”, while the minimal cut set of plant C only adds the condition “ECS fails to start”.

With all the limitations of a very specific scenario, the results demonstrate support of hypothesis H1 - the probability of a runaway reaction caused by reaction deviations is high, when the digital maturity level of the chemical plant is low.

5.2 FRAM Analysis of Performance Variability of Instantiated Plants

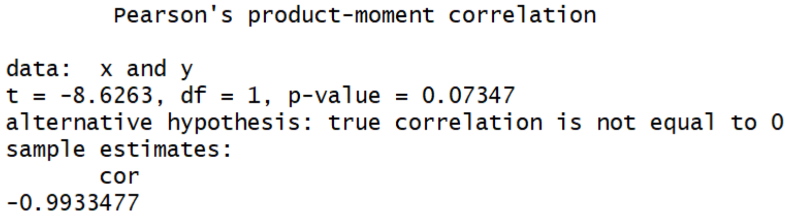
All test results combined give a distribution of performance variability of the entire plant. A summary of the results is shown in Table 19. The mean performance variability decreases with increasing digitalization maturity level. Of interest is, that the number of measurements points exceeding the defined threshold for criticality decreases sharply with increasing digitalization.

Table 19 Summary Results Performance Variability for all Plants

Cumulative Measures Points for all Couplings				
Plant	COUNT	SUM	MEAN	STD
A	49000	3290188,91	67,15	14,02
B	85000	5081344,62	59,78	15,52
C	87000	4151724,95	47,72	14,88
Cumulative Measures Only Critical Couplings Points with Performance Variability >82				

A	8434	732198,91	86,82	2,82
B	3457	292672,24	84,66	1,72
C	85	7185,24	84,53	1,47

Pearson’s test for correlation indicate a correlation between digitalization maturity level and top-event probability occurrence.



```
        Pearson's product-moment correlation

data:  x and y
t = -8.6263, df = 1, p-value = 0.07347
alternative hypothesis: true correlation is not equal to 0
sample estimates:
       cor
-0.9933477
```

Figure 56 shows a boxplot of the performance variability of plant A, B and C. Figure 56 shows the cumulative distribution function plot of plant A, B and C. These plots also indicate a negative correlation between the digitalization maturity and performance variability.

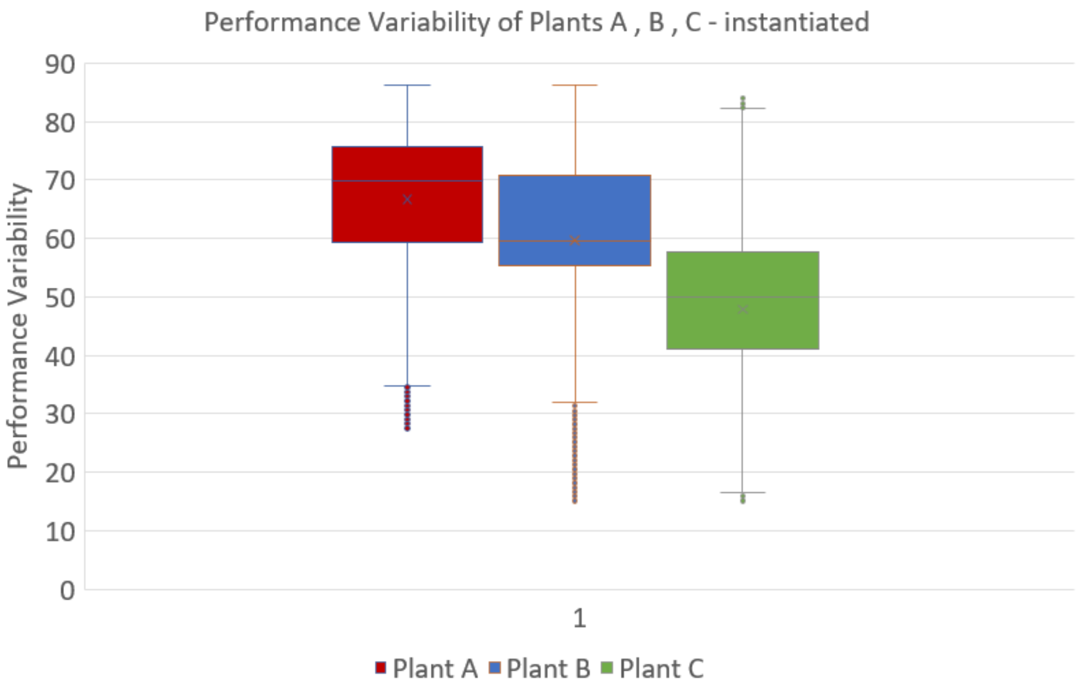


Figure 56 Performance Variability of entire plants

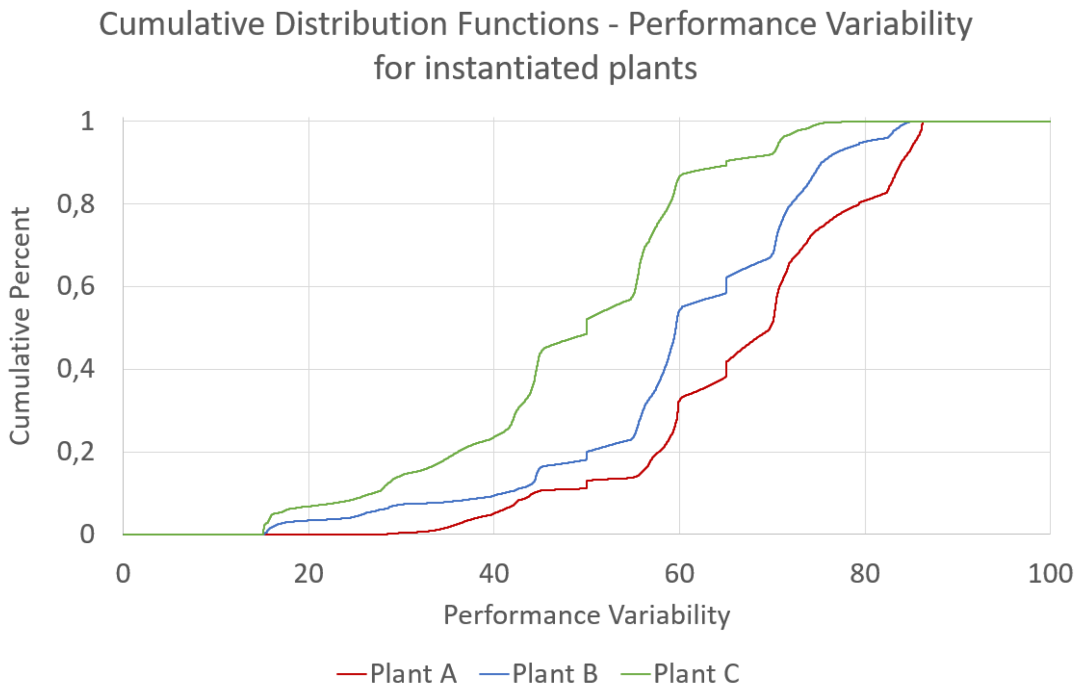


Figure 57 Cumulative Distribution Functions of Performance Variability of entire plants

The Kolmogorov-Smirnov test (Table 20) shows the effect of the maturity level for digitalization on the cumulative distribution functions of performance variability. These effects are in line with the above-mentioned statements indicating that the performance variability of entire plants decreases with increasing digitalization maturity level.

Table 20 Results of the Two-sample Kolmogorov-Smirnov Test

Performance Variability	D	p-Value
Plant A – Plant B	0.23789	< 2.2e-16
Plant A – Plant C	0.57424	< 2.2e-16
Plant B – Plant C	0.39212	< 2.2e-16

If we use the defined performance variability threshold of 82 to identify critical couplings, we find that the number of critical couplings and the performance variability of the critical couplings is lower if the digitalization is higher. Plant C in its instantiated state does not have a critical coupling (see Table 21).

Table 21 Critical Couplings in Instantiated Plants

Plants in instantiated state			
Plant	Percent over Threshold	FRAM Function OUT	FRAM Function IN
A	0,999	Follow Procedures	Start Emergency Cooling Shutdown
A	0,917	Understand procedures	Monitor Reaction
A	0,863	Schedule	Start Reaction
A	0,842	Feed Chemicals	Start Reaction
A	0,698	Plan Maintenance	Do planned maintenance
A	0,688	Monitor Reaction	Control Equipment Target Values
A	0,507	Monitor Reaction	Start Emergency Cooling Shutdown
A	0,499	Keep track of production activities	Plan and organize Production
A	0,053	Make Performance Evaluation	Manage Work Team
B	0,831	Control System	Control Equipment Target Values
B	0,577	Feed Chemicals	Start Reaction
B	0,407	Follow Procedures	Start Emergency Cooling Shutdown
B	0,313	Understand procedures	Monitor Reaction
B	0,307	Schedule	Start Reaction
B	0,262	Operate Servers	Provide IT Services
B	0,195	Manage IT Security	Manage IT Services
B	0,18	Provide Prevention & Detections Services	Operate Clients
B	0,141	Manage IT Assets	Manage IT Services
B	0,115	Monitor Reaction	Control Equipment Target Values
B	0,083	Monitor Reaction	Start Emergency Cooling Shutdown

All these results support hypothesis H3 - if the digitalization maturity level of the chemical plant increases, the robustness of the whole plant, expressed as the accumulated performance variability increases.

5.3 FRAM Analysis of Performance Variability of entire plants - scenarios

The aforementioned FRAM analysis only considers instantiated plants. One focus of interest is how do plants perform under influence of disturbances. The extended FRAM simulation model is capable of examining the effect of disturbance scenarios using as baseline the instantiated simulations.

To compare we need to establish a baseline - the number of critical and highly critical FRAM couplings in the instantiated plants (see Table 22)

Table 22 Number of Critical and Highly Critical Couplings for Instantiated Plants

	Critical	Highly Critical
A	9	4
B	11	1
C	0	0

Applying the change of shift scenario, increases the number of critical couplings. Plant C is almost not effect by this scenario (see Table 23).

Table 23 Number of Critical and Highly Critical Couplings for Plants Scenario Change of Shift

	Critical	Highly Critical
A	19	10
B	10	6
C	1	1

Applying the software update scenario, does no effect on plant A at all, but has severe consequences for plant B and C (see Table 24).

Table 24 Number of Critical and Highly Critical Couplings for Plants Software Update

	Critical	Highly Critical
A	9	4
B	35	27
C	28	23

Applying the deviation of process conditions scenario, effects all plants (see Table 25). This scenario can be used for comparison with the FTA analysis of chapter 5.1.

Table 25 Number of Critical and Highly Critical Couplings for Deviation of Process Conditions

	Critical	Highly Critical
A	26	13
B	21	13
C	8	3

Another approach is to compare the coupled critical functions for each system, instantiated and disturbed. Comparing Figure 58 and Figure 59 one, can see that number of coupled critical functions increases in case of scenario deviation of process conditions, essentially giving one cluster.

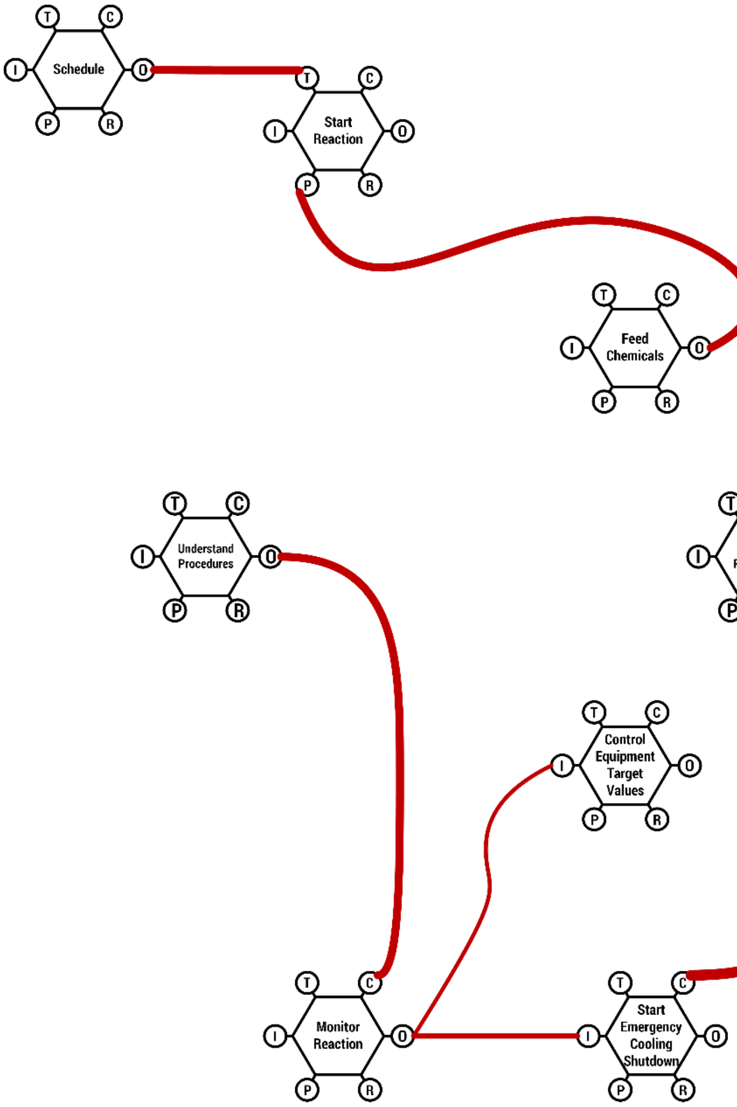


Figure 58 Critical Couplings Plant A - instantianted

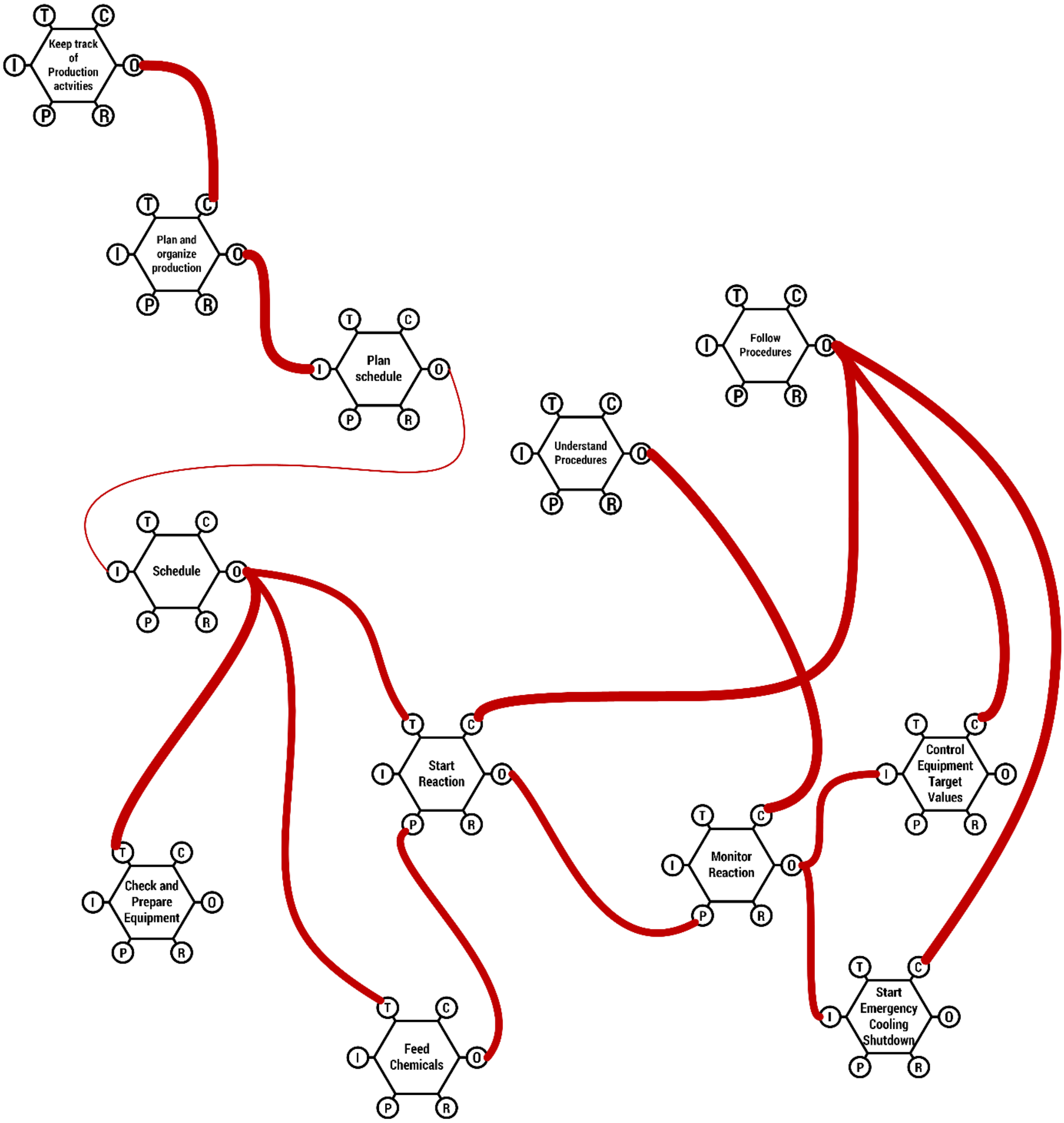

Keep track of Production actvities
Plan and organize production
Plan schedule
Follow Procedures
Understand Procedures
Schedule
Start Reaction
Control Equipment Target Values
Monitor Reaction
Check and Prepare Equipment
Start Emergency Cooling Shutdown
Feed Chemicals
T
C
I
O
P
R

Figure 59 Critical couplings of plant A scenario deviation of process parameters

Compared to plant A, plant B has more linked critical couplings clusters, but with fewer and weaker connections within the clusters (see Figure 60). Applying the scenario deviation of process conditions, results in one cluster with highly critical couplings and three solitary cluster with to members each (Figure 62).

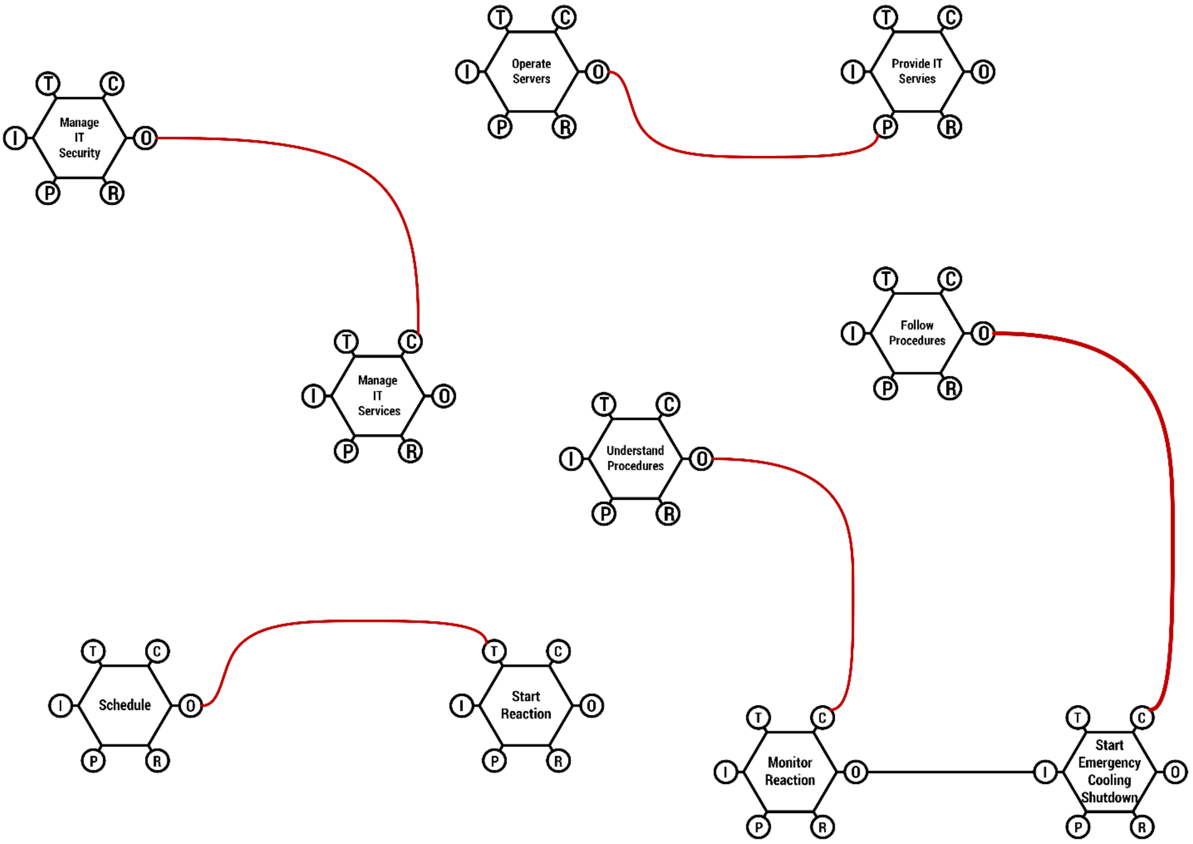


Figure 60 Critical Couplings Plant B - instantianted

Plant C has no critical couplings in its instantiated state, applying scenario deviation of process conditions yields a small cluster with only two highly critical couplings (see Figure 63). Figure 61 clearly shows that the performance variability of plant C is lower than that of plant B. Plant A has the highest performance variability in this scenario. These results are in concordance with the results of the FTA analysis in chapter 5.1.4 and support hypothesis H1 - the probability of a runaway reaction caused by reaction deviations is high, when the digital maturity level of the chemical plant is low.

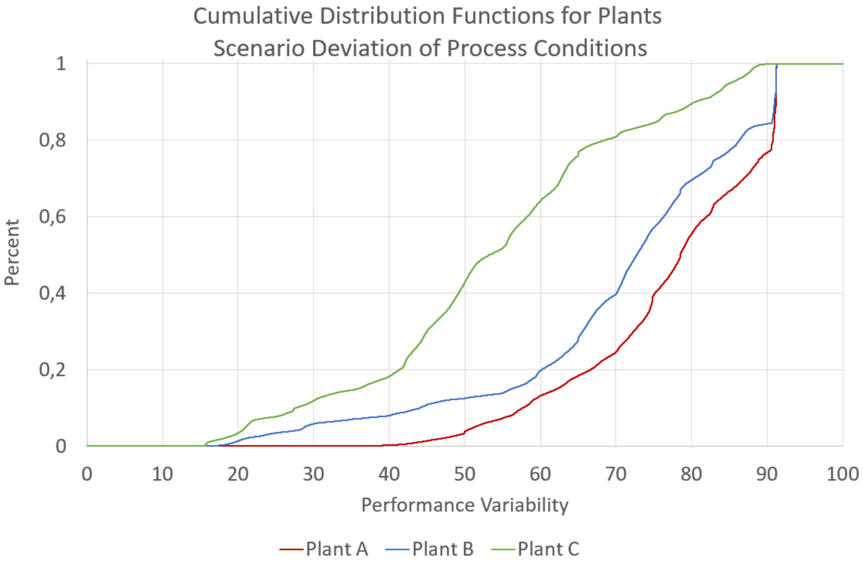


Figure 61 Cumulative Distribution Functions for Scenario Deviation of Process Conditions

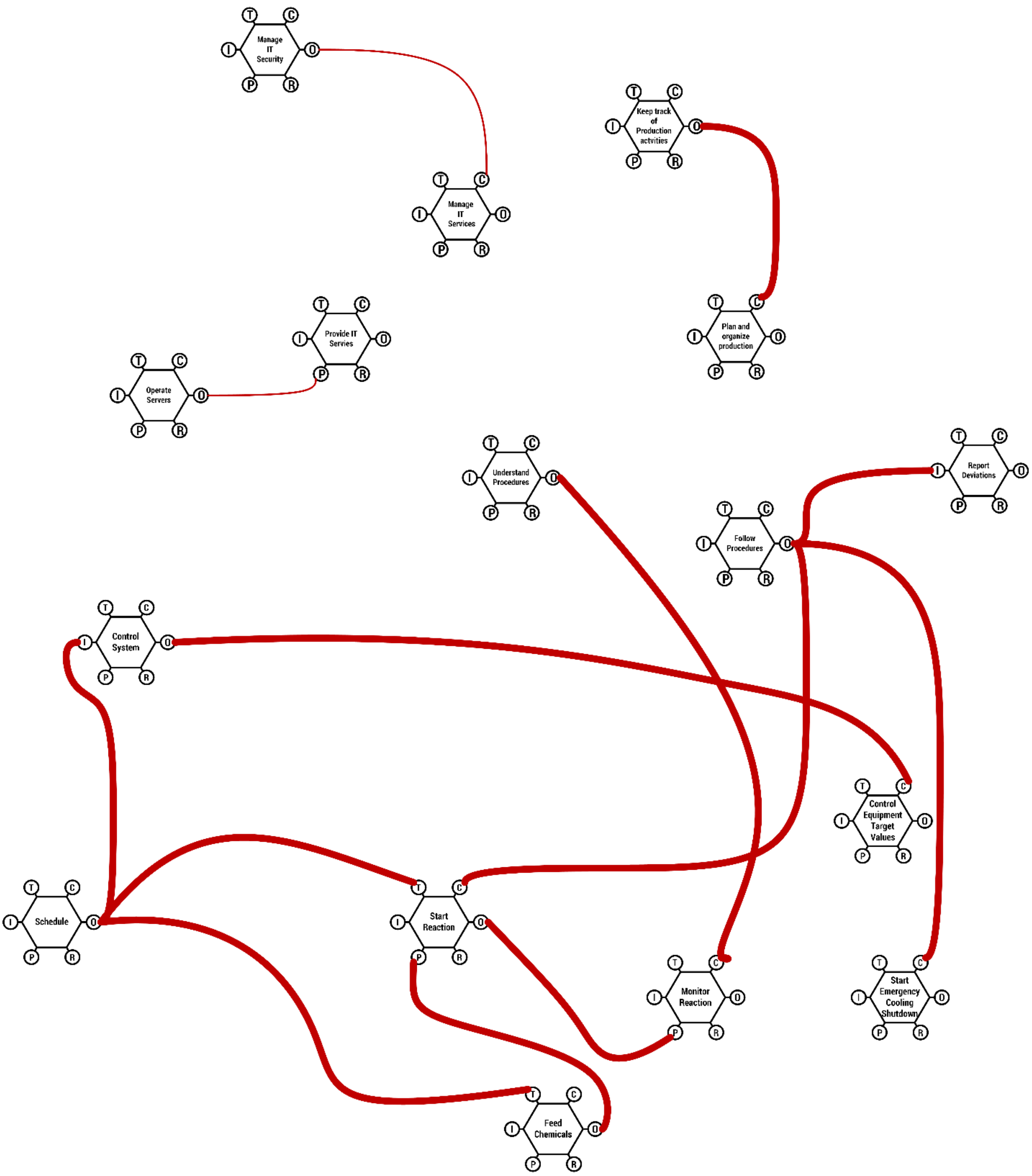


Figure 62 Critical couplings of plant B scenario deviation of process parameters

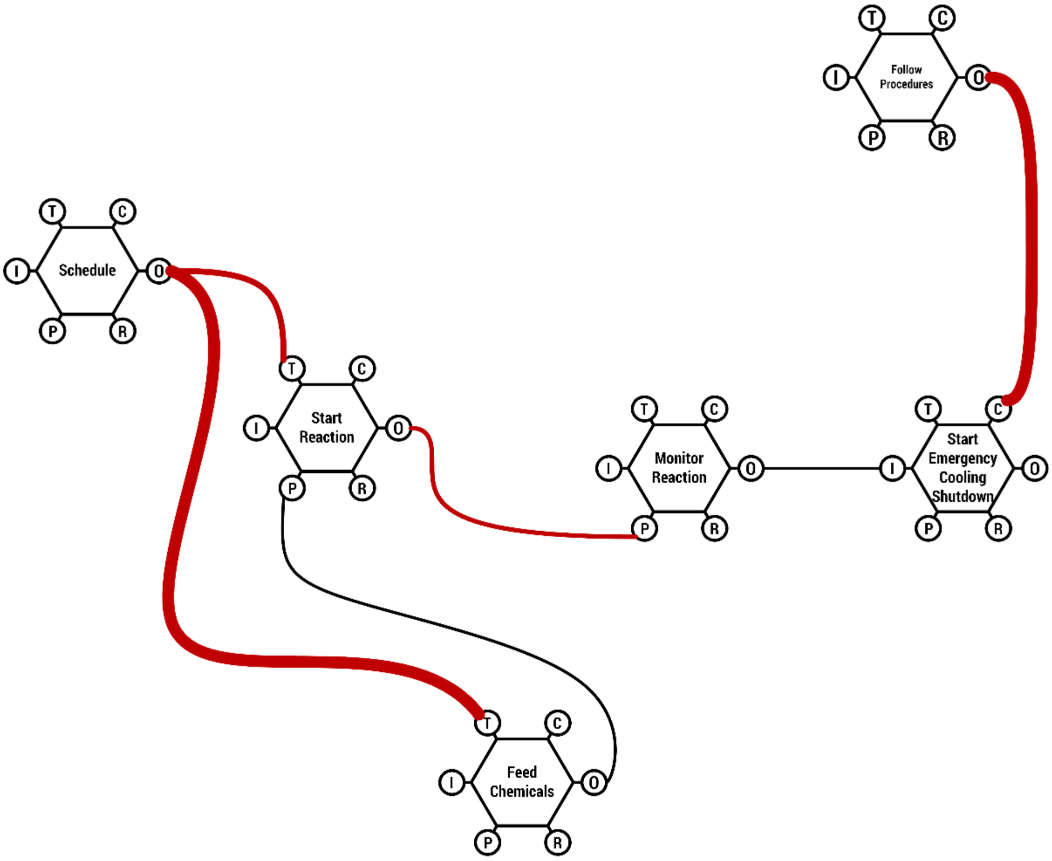


Figure 63 Critical couplings of plant C scenario deviation of process parameters

Applying the deadline pressure scenario has severe consequences for all plants (see Table 26).

Table 26 Number of Critical and Highly Critical Couplings for Plants Scenario Deadline Pressure

	Critical	Highly Critical
A	32	26
B	55	49
C	37	25

If we use Kolmogorov-Smirnov to quantify the effect for each plant, we find that almost all scenarios show increasing performance variabilities (see Table 27).

Table 27 Results of Kolmogorov-Smirnov Analysis for plants dealing with disruptions

Scenario	Performance Variability	D	p-Value
Change of Shift	Plant A – Plant A with Scenario	0.25809	< 2.2e-16
	Plant B– Plant B with Scenario	0.21625	< 2.2e-16

Scenario	Performance Variability	D	p-Value
	Plant C – Plant C with Scenario	0.057744	< 2.2e-16
Weak Understanding Process	Plant A – Plant A with Scenario	0.33812	< 2.2e-16
	Plant B– Plant B with Scenario	0.38847	< 2.2e-16
	Plant C – Plant C with Scenario	0.23145	< 2.2e-16
Deadline Pressure	Plant A – Plant A with Scenario	0.59553	< 2.2e-16
	Plant B– Plant B with Scenario	0.62854	< 2.2e-16
	Plant C – Plant C with Scenario	0.79125	< 2.2e-16
Deviation Process Variables	Plant A – Plant A with Scenario	0.37865	< 2.2e-16
	Plant B– Plant B with Scenario	0.34984	< 2.2e-16
	Plant C – Plant C with Scenario	0.22454	< 2.2e-16
DDOS Attack	Plant A – Plant A with Scenario	0	1
	Plant B– Plant B with Scenario	0.72903	< 2.2e-16
	Plant C – Plant C with Scenario	0.778	< 2.2e-16
Deteriorating Valve Conditions	Plant A – Plant A with Scenario	0.1929	< 2.2e-16
	Plant B– Plant B with Scenario	0.18191	< 2.2e-16
	Plant C – Plant C with Scenario	0.061506	< 2.2e-16
Deviation Operating Procedures	Plant A – Plant A with Scenario	0.4928	< 2.2e-16
	Plant B– Plant B with Scenario	0.46085	< 2.2e-16
	Plant C – Plant C with Scenario	0.3186	< 2.2e-16
Mix 1	Plant A – Plant A with Scenario	0.25823	< 2.2e-16
	Plant B– Plant B with Scenario	0.39385	< 2.2e-16
	Plant C – Plant C with Scenario	0.32218	< 2.2e-16

Scenario	Performance Variability	D	p-Value
Mix2	Plant A – Plant A with Scenario	0.33673	< 2.2e-16
	Plant B– Plant B with Scenario	0.50126	< 2.2e-16
	Plant C – Plant C with Scenario	0.42885	< 2.2e-16
Mix3	Plant A – Plant A with Scenario	0.19263	< 2.2e-16
	Plant B– Plant B with Scenario	0.23425	< 2.2e-16
	Plant C – Plant C with Scenario	0.13598	< 2.2e-16
Mix4	Plant A – Plant A with Scenario	0.59547	< 2.2e-16
	Plant B– Plant B with Scenario	0.6528	< 2.2e-16
	Plant C – Plant C with Scenario	0.53738	< 2.2e-16
Mix5	Plant A – Plant A with Scenario	0.26008	< 2.2e-16
	Plant B– Plant B with Scenario	0.39414	< 2.2e-16
	Plant C – Plant C with Scenario	0.32276	< 2.2e-16

Detailed results of the impact of scenarios can be found in Appendix A.

All these results show no conclusive, congruent assertion. Some disturbances affect all plants, other disturbances impact severely only one plant. Generally, it can be argued that disturbances increase performance variability, with the side not “it depends”. These results do not support hypothesis H4 - if the digitalization maturity level of the chemical plant increases, the robustness of the whole plant, expressed as the accumulated performance variability, when confronted with disturbances, will increase.

One explanation could be that the expansion in FRAM functions and couplings by increasing digitalization, leads to more functions open to disturbance impacts. Another possible explanation could be, that there is little experience with the performance variability of chemistry 4.0 plants and consequently the estimates of the expert were not accurate. This suggests future work on this subject.

5.4 FRAM Analysis of Performance Variability of FRAM Coupling Reactive Maintenance -> Schedule

The results of the simulations show that there is no obvious correlation between the digitalization maturity degree and performance variability for the coupling between the FRAM functions reactive maintenance and schedule. While the performance variability decreases between plant A and plants with higher digitalization maturity, no discernible difference was found between the performance variability of plant B and plant C. Figure 64 shows a boxplot of the performance variability of plant A, B and C. Figure 65 shows the cumulative distribution function plot of plant A, B and C. These plots indicate a negative correlation between the digitalization maturity and performance variability

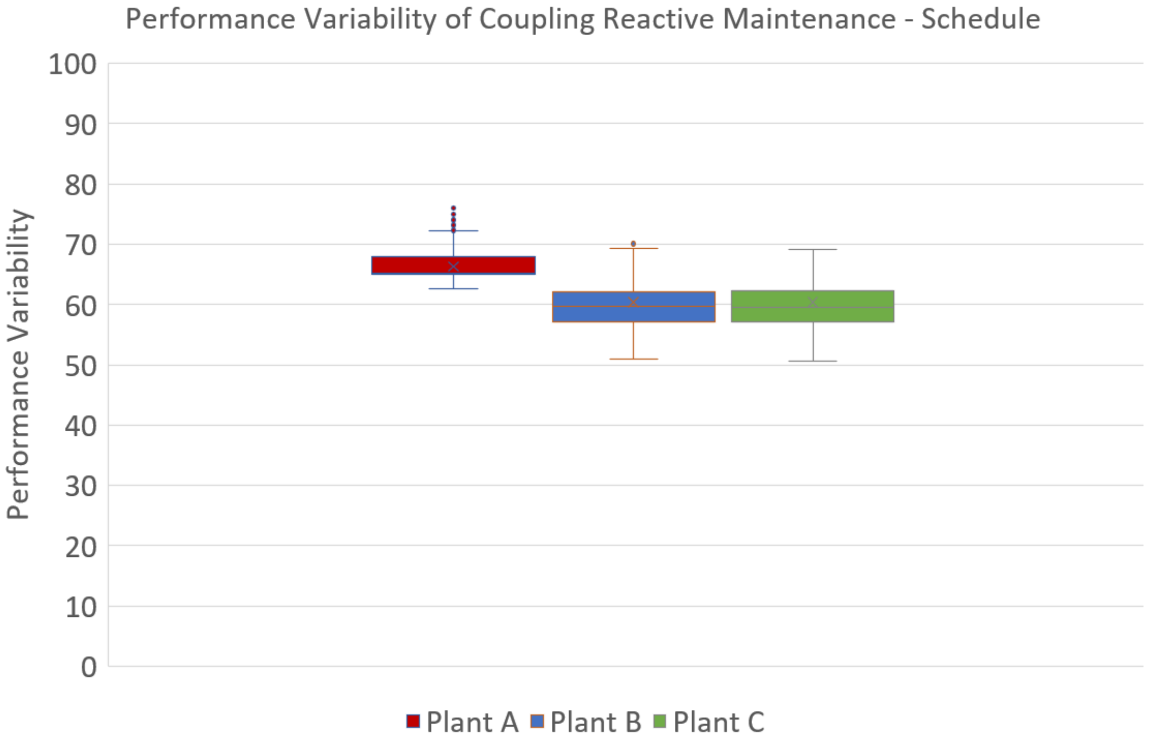


Figure 64 Boxplot Performance Variability Couping Reactive Maintenance - Schedule

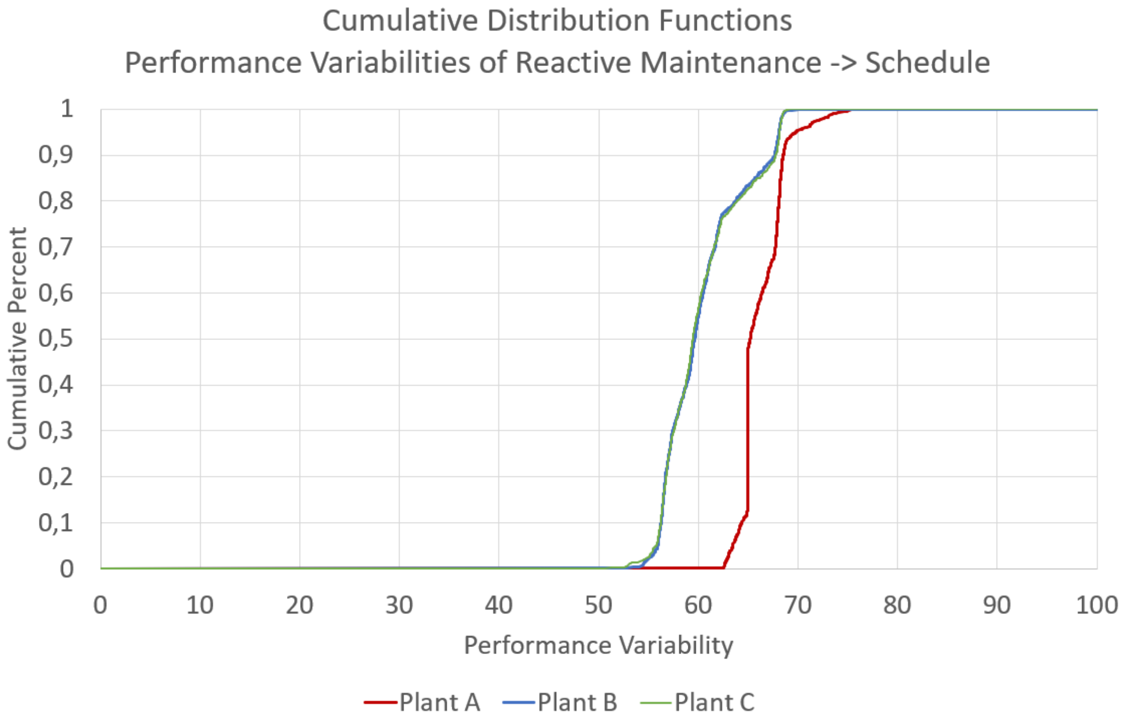


Figure 65 Cumulative Distribution Functions of Performance Variability of Coupling Reactive Maintenance -> Schedule

The Kolmogorov-Smirnov test (Table 28) shows the effect of the maturity level for digitalization on the cumulative distribution functions of performance variability for the coupling between reactive maintenance and scheduling. Although a small effect can be found between plant B and plant C, tis effect is to small to make a statistically sound statement. These effects are in line with the above-mentioned statements indicating that there is no evident correlation between the digitalization maturity level and the performance Variability for the coupling of the FRAM Functions reactive maintenance and schedule.

Table 28 Results of Kolmogorov Smirnov test for the coupling of Reactive maintenance and schedule

Performance Variability	D	p-Value
Plant A – Plant B	0.77323	< 2.2e-16
Plant A – Plant C	0.76523	< 2.2e-16
Plant B – Plant C	0.030969	0.3829

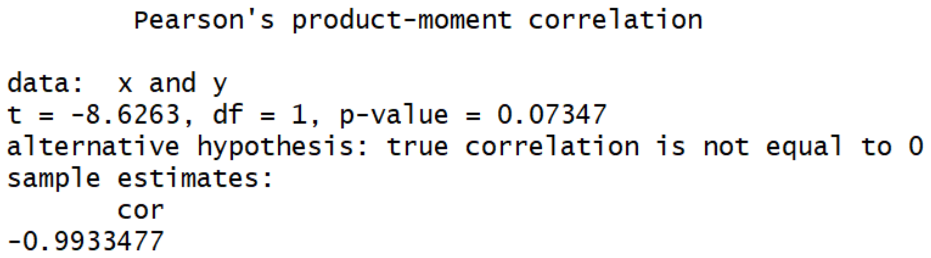
These results contrast with the aggregated performance variability results for all coupling which are maintenance related. Table 29 summarizes the results of the simulation. The mean value of performance variability decreases with increasing digitalization maturity degree.

Table 29 Summary Results Performance Variability for all Maintenance related Couplings

Cumulative Measures Points for all Maintenance related Couplings

Plant	COUNT	MEAN	STD
A	4000	69,18	9,34
B	4000	59,84	8,48
C	5000	45,1	12,14

Pearson’s test for correlation also indicate a correlation between digitalization maturity level and the aggregated performance variability for all maintenance related couplings.



```
        Pearson's product-moment correlation

data:  x and y
t = -8.6263, df = 1, p-value = 0.07347
alternative hypothesis: true correlation is not equal to 0
sample estimates:
       cor
-0.9933477
```

Figure 66 shows a boxplot of the performance variability of plant A, B and C. Figure 67 shows the cumulative distribution function plot of plant A, B and C. These plots indicate a negative correlation between the digitalization maturity and performance variability.

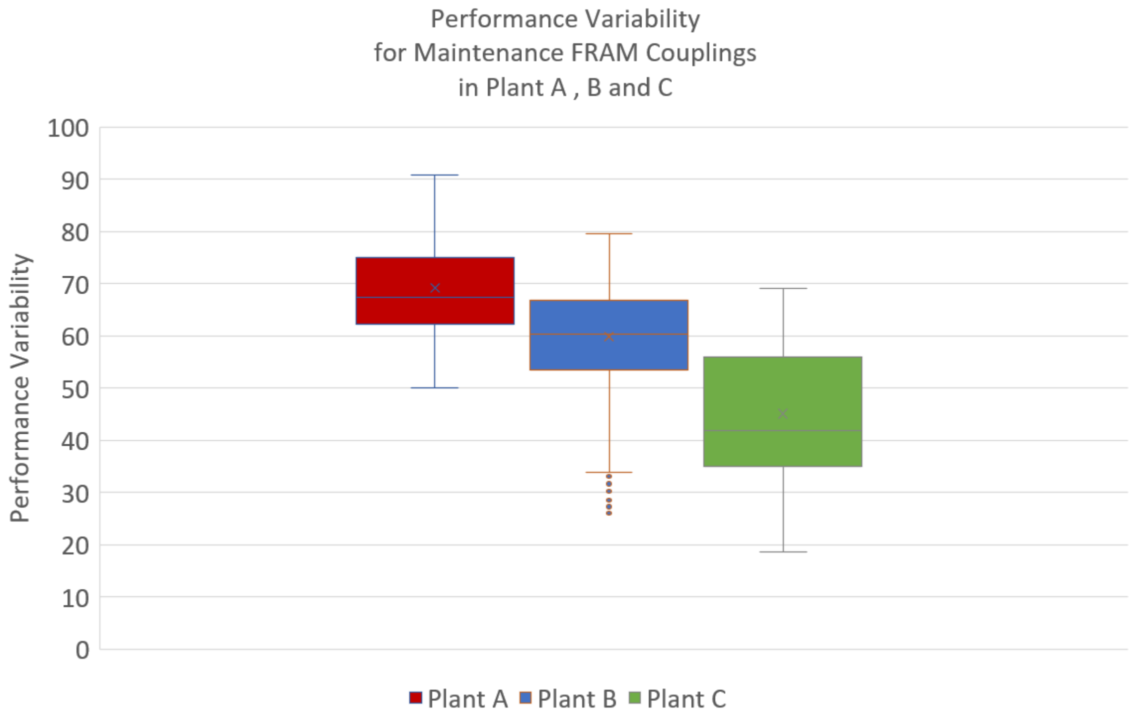


Figure 66 Boxplot Aggregated Performance Variability for all maintenance related Couplings

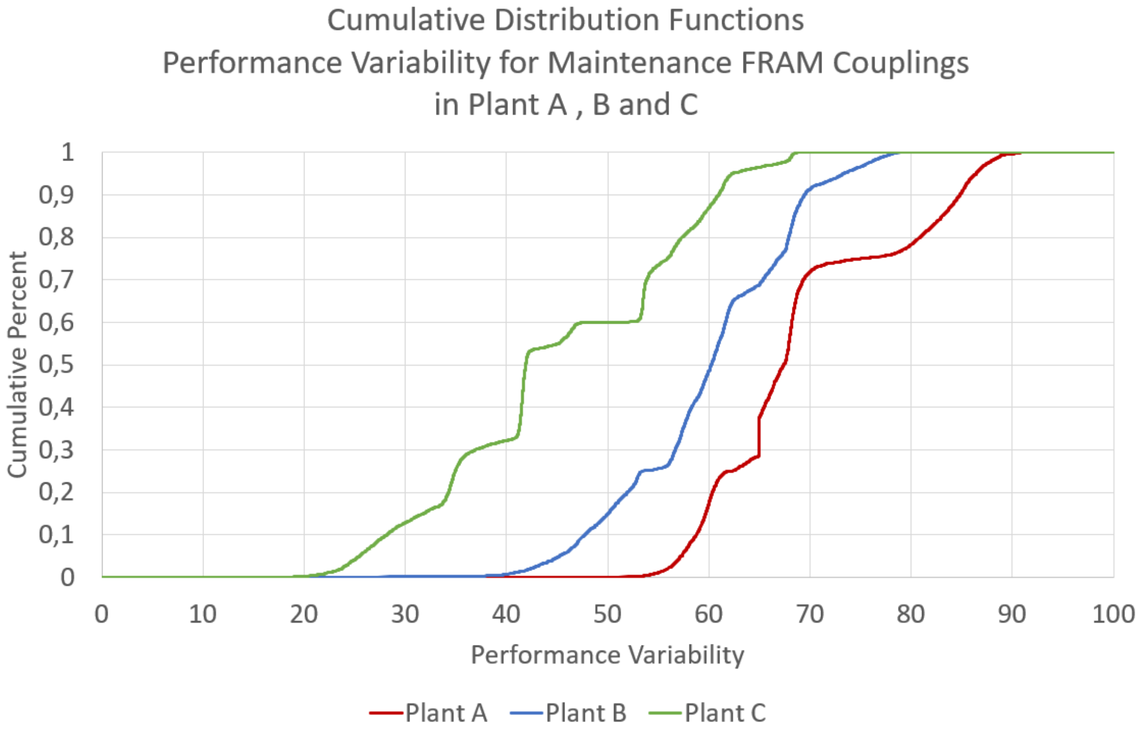


Figure 67 Cumulative Distribution Functions of aggregated Performance Variability for all maintenance related Couplings

One explanation for these results could be, that while the step from analog to centralized control plants improve performance variability for this specific coupling, no additional advantage is gained by raising the digitalization level. Another possible explanation could be that the estimates of the chemical expert for this specific coupling were not correct, leading to an anomaly, as indicated by the aggregated values which show a negative correlation between performance variability and digitalization degree over all plants.

6 THREATS TO VALIDITY

One common threat to validity is the low number of interviewed experts. More interviews would result in a statistically sound database. Generally, it is difficult to find experts with knowledge in all domains of interest. So rating differences between experts cannot be ruled out, as their individualistic bias, is amplified by different domain approaches.

As no chemistry 4.0 and analog plants for this specific reaction can be investigated at this time, three hypothetical case studies were formulated to compare plants with different digitalization maturity levels. Additional hypothetical plants with additional maturity levels, would yield more data for statistical analysis. The restriction on a batch plant with exactly one type of reaction, limits the generalization of results.

The FRAM analysis does not yet include technological failures - in this way it is limited to activities where humans participate.

7 CONCLUSION

This chapter is a summary of the findings of this study and proposes some further directions of research.

7.1 Research work summary

This thesis investigated changing risk expressed as performance variability in chemical plants doing batch reactions, as a result of different digitalization maturity levels. To do this, three fictional plants representing three different degrees of digitalization maturity were devised. Plant A corresponds to an analog, pre-digital plant while plant B represents a plant with centralized IT which can be approximately placed in the year 1980. Plant C represents the future of chemical plants and includes the aspects of Chemistry 4.0. In these case studies, all plants perform an exothermic reaction, all plant have different equipment, corresponding to their digitalization maturity.

FTA analyses for the specific top event run-away reaction were done to calculate probabilities of occurrence. The results demonstrate that increasing the digitalization leads to a lower top event probability (runaway reaction caused by deviation of process variables). With all the limitations of a very specific scenario, the results demonstrate support of hypothesis H1 - the probability of a runaway reaction caused by reaction deviations is high, when the digital maturity level of the chemical plant is low.

A new hybrid simulation methodology, that combines functional resonance accident methodology and fuzzy logic to simulate chemical plants was developed. This simulation methodology can generally be used to identify risks in complex socio-technological systems. A new metric was proposed and used to identify critical couplings.

Three FRAM models were developed for the plants, each representing a different stage of digitalization. These models were validated by experts. For each coupling, experts gave their estimates of aspect variabilities like timing, precision or effects in form of distributions with their parameters. In a Monte-Carlo-style simulation, performance variability distributions were computed. A threshold for identifying critical was defined.

The performance variability of the FRAM coupling between reactive maintenance and scheduling was examined. The results of the simulations do not support the hypothesis H2 that, if the digitalization maturity level of the chemical plant increases, the performance variability of scheduling, caused by reactive maintenance, will decrease. While the performance variability decreases between plant A and plants with higher digitalization maturity, no discernible difference was found between the performance variability of plant B and plant C. This contrast with the results covering all maintenance related couplings, where a correlation was found and invites to further research.

The aggregated performance variability of entire plants was computed and used in an analysis for hypothesis H3. The results support hypothesis H3 - if the digitalization maturity level of the chemical plant increases, the robustness of the whole plant, expressed as the accumulated performance variability increases. The behavior of the plants under disturbance was also examined. The scenario used in the FTA analysis was applied to the instantiated FRAM models supporting the evidence of the FTA analysis that the probability of a runaway reaction caused by reaction deviations is high, when the digital maturity level of the chemical plant is low (hypothesis H1). While this scenario supports hypothesis H4 - if the digitalization maturity level of the chemical plant increases, the robustness of the whole plant, expressed as the accumulated performance variability, when confronted with disturbances, will increase – other scenarios contradict hypothesis 4. Some disturbances affect all plants, other disturbances impact severely only one plant. Summing up

One explanation could be that the expansion in FRAM functions and couplings by increasing digitalization, leads to more functions open to disturbance impacts. Another possible explanation could be, that there is little experience with the performance variability of chemistry 4.0 plants and consequently the estimates of the expert were not accurate. This suggests future work on this subject.

The extended FRAM model proved to be a valuable method. Its applicability and its capability for risk identification suggest a supplemental methodology for risk evaluations.

7.2 Further Studies

Some issues emerged during work on this thesis. These points could be starting points for future research developments.

The first question relates to the human centric approach of FRAM. Can this model be further developed to include technical only systems, especially in light of Industry 4.0 where distributed control networks might employ artificial intelligence and simulate human like behavior for decisions.

A second question relates to the comparison of nominal and normal scenarios. In a nominal scenario, the process designer decides what people or system should do. In a normal scenario you see what people actually do. A comparison of these two approaches with FRAM methodology might be an interesting approach for future work.

A third issue concerns data collection for further research. More data will improve the reliability of this method.

A final point relates to an extension of the FRAM methodology with system dynamics. An interesting approach to include feedback loops and performance variability propagation could be the inclusion of system dynamics.

APPENDIX A – CRITICAL FRAM COUPLINGS

Plant	Scenario	Percent	NameOUT	NameIN
A	6	0,999	Follow Procedures	Report Deviations
A	6	0,999	Schedule	Feed Chemicals
A	6	0,999	Schedule	Start Reaction
A	6	0,999	Feed Chemicals	Start Reaction
A	6	0,999	Monitor Reaction	Control Equipment Target Values
A	6	0,997	Monitor Reaction	Start Emergency Cooling Shutdown
A	6	0,971	Follow Procedures	Start Emergency Cooling Shutdown
A	6	0,582	Schedule	Check & Prepare Equipment
A	6	0,467	Start Reaction	Monitor Reaction
A	6	0,224	Check & Prepare Equipment	Feed Chemicals
A	6	0,115	Understand procedures	Monitor Reaction
A	6	0,066	Reactive Maintenance (Repair)	Schedule
A	8	0,999	Follow Procedures	Report Deviations
A	8	0,999	Follow Procedures	Start Reaction
A	8	0,999	Follow Procedures	Start Emergency Cooling Shutdown
A	8	0,999	Plan Schedule	Plan Material Supply
A	8	0,999	Plan Schedule	Schedule
A	8	0,999	Schedule	Start Reaction
A	8	0,999	Feed Chemicals	Start Reaction
A	8	0,983	Understand procedures	Monitor Reaction
A	8	0,878	Understand procedures	Follow Procedures
A	8	0,844	Schedule	Feed Chemicals
A	8	0,644	Monitor Reaction	Control Equipment Target Values
A	8	0,521	Monitor Reaction	Start Emergency Cooling Shutdown
A	8	0,52	Plan Material Supply	Plan Schedule
A	8	0,196	Plan and organize Production	Plan Material Supply
A	8	0,095	Plan and organize Production	Manage Work Team
A	8	0,069	Supervise	Work with Chemicals
A	8	0,059	Plan and organize Production	Plan Schedule
A	9	0,999	Keep track of production activities	Plan and organize Production
A	9	0,999	Keep track of production activities	Make Performance Evaluation
A	9	0,999	Keep track of production activities	Schedule
A	9	0,999	Plan and organize Production	Manage Work Team
A	9	0,999	Plan and organize Production	Plan Material Supply
A	9	0,999	Plan and organize Production	Plan Schedule
A	9	0,999	Support Production	Coordinate Plant Operations
A	9	0,999	Manage Resources	Coordinate Plant Operations
A	9	0,999	Understand procedures	Monitor Reaction

A	9	0,999	Schedule	Feed Chemicals
A	9	0,999	Schedule	Start Reaction
A	9	0,999	Check & Prepare Equipment	Feed Chemicals
A	9	0,999	Feed Chemicals	Start Reaction
A	9	0,999	Start Reaction	Monitor Reaction
A	9	0,999	Monitor Reaction	Start Emergency Cooling Shutdown
A	9	0,999	Monitor Reaction	Control Equipment Target Values
A	9	0,999	Follow Procedures	Start Emergency Cooling Shutdown
A	9	0,999	Plan Material Supply	Plan Schedule
A	9	0,999	Plan Schedule	Plan Material Supply
A	9	0,999	Plan Schedule	Schedule
A	9	0,999	Plan Maintenance	Plan Schedule
A	9	0,999	Plan Maintenance	Do planned maintenance
A	9	0,998	Reactive Maintenance (Repair)	Schedule
A	9	0,947	Schedule	Check & Prepare Equipment
A	9	0,244	Make Performance Evaluation	Manage Work Team
A	9	0,237	Coordinate Plant Operations	Work with Chemicals
A	9	0,058	Follow Procedures	Report Deviations
A	9	0,058	Follow Procedures	Start Reaction
A	10	0,999	Follow Procedures	Report Deviations
A	10	0,999	Follow Procedures	Start Reaction
A	10	0,999	Follow Procedures	Start Emergency Cooling Shutdown
A	10	0,999	Schedule	Feed Chemicals
A	10	0,999	Schedule	Start Reaction
A	10	0,999	Feed Chemicals	Start Reaction
A	10	0,999	Start Reaction	Monitor Reaction
A	10	0,997	Keep track of production activities	Plan and organize Production
A	10	0,981	Understand procedures	Monitor Reaction
A	10	0,968	Keep track of production activities	Schedule
A	10	0,65	Plan Maintenance	Do planned maintenance
A	10	0,558	Schedule	Check & Prepare Equipment
A	10	0,199	Monitor Reaction	Start Emergency Cooling Shutdown
A	10	0,166	Monitor Reaction	Control Equipment Target Values
A	12	0,999	Schedule	Start Reaction
A	12	0,999	Feed Chemicals	Start Reaction
A	12	0,999	Start Reaction	Monitor Reaction
A	12	0,853	Follow Procedures	Start Emergency Cooling Shutdown
A	12	0,799	Schedule	Feed Chemicals
A	12	0,352	Plan Maintenance	Do planned maintenance
A	12	0,17	Monitor Reaction	Start Emergency Cooling Shutdown
A	12	0,166	Monitor Reaction	Control Equipment Target Values
A	12	0,084	Understand procedures	Monitor Reaction
A	12	0,051	Reactive Maintenance (Repair)	Schedule
A	13	0,999	Follow Procedures	Report Deviations
A	13	0,999	Follow Procedures	Start Reaction

A	13	0,999	Follow Procedures	Start Emergency Cooling Shutdown
A	13	0,999	Schedule	Feed Chemicals
A	13	0,999	Schedule	Start Reaction
A	13	0,999	Start Reaction	Monitor Reaction
A	13	0,996	Feed Chemicals	Start Reaction
A	13	0,995	Understand procedures	Monitor Reaction
A	13	0,994	Keep track of production activities	Plan and organize Production
A	13	0,993	Schedule	Check & Prepare Equipment
A	13	0,94	Keep track of production activities	Schedule
A	13	0,919	Plan Schedule	Plan Material Supply
A	13	0,898	Plan Schedule	Schedule
A	13	0,841	Supervise	Work with Chemicals
A	13	0,696	Support Production	Coordinate Plant Operations
A	13	0,636	Monitor Reaction	Control Equipment Target Values
A	13	0,588	Check & Prepare Equipment	Feed Chemicals
A	13	0,493	Monitor Reaction	Start Emergency Cooling Shutdown
A	13	0,2	Plan Maintenance	Do planned maintenance
A	13	0,194	Plan and organize Production	Plan Material Supply
A	13	0,136	Coordinate Plant Operations	Work with Chemicals
A	13	0,102	Plan and organize Production	Manage Work Team
A	13	0,082	Supervise	Coordinate Plant Operations
A	13	0,065	Plan and organize Production	Plan Schedule
A	14	0,999	Follow Procedures	Report Deviations
A	14	0,999	Schedule	Feed Chemicals
A	14	0,999	Schedule	Start Reaction
A	14	0,999	Feed Chemicals	Start Reaction
A	14	0,999	Monitor Reaction	Control Equipment Target Values
A	14	0,998	Monitor Reaction	Start Emergency Cooling Shutdown
A	14	0,979	Follow Procedures	Start Emergency Cooling Shutdown
A	14	0,595	Schedule	Check & Prepare Equipment
A	14	0,457	Start Reaction	Monitor Reaction
A	14	0,213	Check & Prepare Equipment	Feed Chemicals
A	14	0,096	Understand procedures	Monitor Reaction
A	14	0,051	Reactive Maintenance (Repair)	Schedule
A	16	0,999	Follow Procedures	Report Deviations
A	16	0,999	Follow Procedures	Start Reaction
A	16	0,999	Follow Procedures	Start Emergency Cooling Shutdown
A	16	0,999	Plan Schedule	Plan Material Supply
A	16	0,999	Plan Schedule	Schedule
A	16	0,999	Schedule	Start Reaction
A	16	0,999	Feed Chemicals	Start Reaction
A	16	0,974	Understand procedures	Monitor Reaction
A	16	0,86	Understand procedures	Follow Procedures
A	16	0,843	Schedule	Feed Chemicals
A	16	0,647	Monitor Reaction	Control Equipment Target Values

A	16	0,551	Monitor Reaction	Start Emergency Cooling Shutdown
A	16	0,525	Plan Material Supply	Plan Schedule
A	16	0,177	Plan and organize Production	Plan Material Supply
A	16	0,125	Plan and organize Production	Manage Work Team
A	16	0,074	Supervise	Work with Chemicals
A	16	0,057	Plan and organize Production	Plan Schedule
B	6	0,999	Manage IT Assets	Manage IT Services
B	6	0,999	Manage IT Security	Manage IT Services
B	6	0,999	Feed Chemicals	Start Reaction
B	6	0,703	Monitor Reaction	Control Equipment Target Values
B	6	0,624	Monitor Reaction	Start Emergency Cooling Shutdown
B	6	0,283	Schedule	Start Reaction
B	7	0,999	Plan IT Policies	Enforce IT Policies
B	7	0,999	Enforce IT Policies	Supervise Network
B	7	0,999	Enforce IT Policies	Provide Prevention & Detections Services
B	7	0,999	Operate Servers	Provide Communication Services
B	7	0,999	Operate Servers	Provide IT Services
B	7	0,999	Provide Mitigation Services	Provide IT Services
B	7	0,999	Supervise Network	Provide Client Support
B	7	0,999	Supervise Network	Provide Prevention & Detections Services
B	7	0,999	Supervise Network	Operate Network
B	7	0,999	Provide Client Support	Operate Clients
B	7	0,999	Provide Communication Services	Control System
B	7	0,999	Provide Prevention & Detections Services	Provide Client Support
B	7	0,999	Provide Prevention & Detections Services	Operate Clients
B	7	0,999	Provide Prevention & Detections Services	Operate Network
B	7	0,999	Operate Network	Operate Servers
B	7	0,999	Operate Network	Provide Communication Services
B	7	0,999	Provide IT Services	Plan Schedule
B	7	0,999	Provide IT Services	Analyse predicitive Maintenance
B	7	0,999	Operate Network	Provide IT Services
B	7	0,999	Feed Chemicals	Start Reaction
B	7	0,999	Monitor Reaction	Start Emergency Cooling Shutdown
B	7	0,999	Monitor Reaction	Control Equipment Target Values
B	7	0,999	Control System	Start Reaction
B	7	0,999	Control System	Control Equipment Target Values
B	7	0,998	Control System	Start Emergency Cooling Shutdown
B	7	0,997	Provide Mitigation Services	Operate Servers
B	7	0,984	Provide IT Services	Plan Material Supply
B	7	0,978	Operate Network	Operate Clients
B	7	0,958	Enforce IT Policies	Provide Client Support

B	7	0,91	Start Reaction	Monitor Reaction
B	7	0,852	Plan Maintenance	Do planned maintenance
B	7	0,808	Provide Prevention & Detections Services	Operate Servers
B	7	0,531	Supervise Hardware	Provide Client Support
B	7	0,522	Enforce IT Policies	Supervise Hardware
B	7	0,394	Monitor Reaction	Control System
B	7	0,065	Plan Maintenance	Plan Schedule
B	8	0,999	Manage IT Assets	Manage IT Services
B	8	0,999	Manage IT Security	Manage IT Services
B	8	0,999	Follow Procedures	Report Deviations
B	8	0,999	Follow Procedures	Start Reaction
B	8	0,999	Follow Procedures	Start Emergency Cooling Shutdown
B	8	0,999	Operate Servers	Provide Communication Services
B	8	0,999	Operate Servers	Provide IT Services
B	8	0,999	Plan Schedule	Plan Material Supply
B	8	0,999	Plan Schedule	Schedule
B	8	0,999	Schedule	Start Reaction
B	8	0,999	Feed Chemicals	Start Reaction
B	8	0,821	Control System	Control Equipment Target Values
B	8	0,789	Provide Communication Services	Control System
B	8	0,68	Schedule	Feed Chemicals
B	8	0,664	Understand procedures	Monitor Reaction
B	8	0,232	Supervise Hardware	Provide Client Support
B	8	0,109	Provide IT Services	Operate Clients
B	9	0,999	Manage IT Assets	Manage IT Services
B	9	0,999	Manage IT Security	Manage IT Services
B	9	0,999	Manage IT Services	Keep track of production activities
B	9	0,999	Manage IT Services	Plan and organize Production
B	9	0,999	Keep track of production activities	Plan and organize Production
B	9	0,999	Keep track of production activities	Schedule
B	9	0,999	Plan and organize Production	Manage Work Team
B	9	0,999	Plan and organize Production	Plan Material Supply
B	9	0,999	Support Production	Coordinate Plant Operations
B	9	0,999	Plan IT Policies	Enforce IT Policies
B	9	0,999	Enforce IT Policies	Supervise Network
B	9	0,999	Provide Mitigation Services	Provide IT Services
B	9	0,999	Supervise Network	Provide Prevention & Detections Services
B	9	0,999	Provide Client Support	Operate Clients
B	9	0,999	Enforce IT Policies	Provide Prevention & Detections Services
B	9	0,999	Operate Network	Operate Servers
B	9	0,999	Operate Network	Provide Communication Services
B	9	0,999	Operate Network	Operate Clients
B	9	0,999	Operate Network	Provide IT Services
B	9	0,999	Plan Schedule	Plan Material Supply
B	9	0,999	Plan Schedule	Schedule
B	9	0,999	Schedule	Feed Chemicals

B	9	0,999	Schedule	Start Reaction
B	9	0,999	Check & Prepare Equipment	Feed Chemicals
B	9	0,999	Feed Chemicals	Start Reaction
B	9	0,999	Start Reaction	Monitor Reaction
B	9	0,999	Monitor Reaction	Start Emergency Cooling Shutdown
B	9	0,999	Monitor Reaction	Control System
B	9	0,999	Monitor Reaction	Control Equipment Target Values
B	9	0,999	Provide Prevention & Detections Services	Provide Client Support
B	9	0,999	Provide Prevention & Detections Services	Operate Clients
B	9	0,999	Reactive Maintenance (Repair)	Schedule
B	9	0,999	Plan Maintenance	Plan Schedule
B	9	0,999	Plan Maintenance	Do planned maintenance
B	9	0,998	Provide Prevention & Detections Services	Operate Network
B	9	0,998	Provide IT Services	Plan Schedule
B	9	0,998	Provide IT Services	Analyse predicitive Maintenance
B	9	0,997	Enforce IT Policies	Provide Client Support
B	9	0,996	Follow Procedures	Start Emergency Cooling Shutdown
B	9	0,991	Manage Resources	Coordinate Plant Operations
B	9	0,991	Plan and organize Production	Plan Schedule
B	9	0,986	Provide IT Services	Plan Material Supply
B	9	0,975	Provide Prevention & Detections Services	Operate Servers
B	9	0,954	Schedule	Control System
B	9	0,953	Understand procedures	Monitor Reaction
B	9	0,95	Keep track of production activities	Make Performance Evaluation
B	9	0,934	Provide Mitigation Services	Operate Servers
B	9	0,823	Control System	Control Equipment Target Values
B	9	0,497	Enforce IT Policies	Supervise Hardware
B	9	0,05	Make Performance Evaluation	Manage Work Team
B	10	0,999	Feed Chemicals	Start Reaction
B	10	0,999	Start Reaction	Monitor Reaction
B	10	0,999	Follow Procedures	Report Deviations
B	10	0,999	Follow Procedures	Start Reaction
B	10	0,999	Follow Procedures	Start Emergency Cooling Shutdown
B	10	0,999	Schedule	Feed Chemicals
B	10	0,999	Control System	Control Equipment Target Values
B	10	0,998	Schedule	Start Reaction
B	10	0,857	Control System	Start Reaction
B	10	0,655	Understand procedures	Monitor Reaction
B	10	0,609	Schedule	Control System
B	10	0,503	Keep track of production activities	Schedule
B	10	0,454	Keep track of production activities	Plan and organize Production
B	11	0,999	Supervise Hardware	Operate Servers

B	11	0,999	Operate Servers	Provide Communication Services
B	11	0,999	Operate Servers	Provide IT Services
B	11	0,999	Supervise Network	Provide Prevention & Detections Services
B	11	0,999	Supervise Network	Operate Network
B	11	0,999	Provide Client Support	Operate Clients
B	11	0,999	Provide Prevention & Detections Services	Provide Client Support
B	11	0,999	Provide Prevention & Detections Services	Operate Clients
B	11	0,999	Provide Prevention & Detections Services	Operate Network
B	11	0,999	Operate Network	Operate Servers
B	11	0,999	Operate Network	Provide Communication Services
B	11	0,999	Operate Network	Operate Clients
B	11	0,999	Operate Network	Provide IT Services
B	11	0,999	Provide Communication Services	Control System
B	11	0,999	Provide IT Services	Analyse predicitive Maintenance
B	11	0,998	Supervise Network	Provide Client Support
B	11	0,998	Provide IT Services	Plan Schedule
B	11	0,988	Provide IT Services	Plan Material Supply
B	11	0,979	Provide Prevention & Detections Services	Operate Servers
B	11	0,878	Supervise Hardware	Provide Client Support
B	11	0,717	Plan IT Policies	Enforce IT Policies
B	11	0,363	Provide Mitigation Services	Provide IT Services
B	11	0,165	Provide Communication Services	Operate Clients
B	11	0,161	Provide Mitigation Services	Operate Servers
B	12	0,999	Schedule	Start Reaction
B	12	0,999	Feed Chemicals	Start Reaction
B	12	0,968	Control System	Control Equipment Target Values
B	12	0,922	Start Reaction	Monitor Reaction
B	12	0,518	Control System	Start Reaction
B	12	0,062	Schedule	Feed Chemicals
B	13	0,999	Follow Procedures	Report Deviations
B	13	0,999	Follow Procedures	Start Reaction
B	13	0,999	Follow Procedures	Start Emergency Cooling Shutdown
B	13	0,999	Schedule	Feed Chemicals
B	13	0,999	Schedule	Start Reaction
B	13	0,999	Feed Chemicals	Start Reaction
B	13	0,999	Start Reaction	Monitor Reaction
B	13	0,999	Control System	Start Reaction
B	13	0,999	Control System	Start Emergency Cooling Shutdown
B	13	0,999	Control System	Control Equipment Target Values
B	13	0,962	Schedule	Control System
B	13	0,909	Understand procedures	Monitor Reaction
B	13	0,478	Keep track of production activities	Schedule
B	13	0,429	Check & Prepare Equipment	Feed Chemicals
B	13	0,413	Keep track of production activities	Plan and organize Production

B	13	0,201	Supervise	Work with Chemicals
B	13	0,058	Support Production	Coordinate Plant Operations
B	14	0,999	Manage IT Assets	Manage IT Services
B	14	0,999	Manage IT Security	Manage IT Services
B	14	0,999	Plan IT Policies	Enforce IT Policies
B	14	0,999	Enforce IT Policies	Supervise Network
B	14	0,999	Enforce IT Policies	Provide Prevention & Detections Services
B	14	0,999	Operate Servers	Provide Communication Services
B	14	0,999	Operate Servers	Provide IT Services
B	14	0,999	Provide Mitigation Services	Provide IT Services
B	14	0,999	Supervise Network	Provide Client Support
B	14	0,999	Supervise Network	Provide Prevention & Detections Services
B	14	0,999	Supervise Network	Operate Network
B	14	0,999	Provide Client Support	Operate Clients
B	14	0,999	Provide Communication Services	Control System
B	14	0,999	Provide Prevention & Detections Services	Provide Client Support
B	14	0,999	Provide Prevention & Detections Services	Operate Clients
B	14	0,999	Provide Prevention & Detections Services	Operate Network
B	14	0,999	Operate Network	Operate Servers
B	14	0,999	Operate Network	Provide Communication Services
B	14	0,999	Provide IT Services	Plan Schedule
B	14	0,999	Provide IT Services	Analyse predicitive Maintenance
B	14	0,999	Operate Network	Provide IT Services
B	14	0,996	Feed Chemicals	Start Reaction
B	14	0,995	Provide Mitigation Services	Operate Servers
B	14	0,987	Operate Network	Operate Clients
B	14	0,983	Provide IT Services	Plan Material Supply
B	14	0,953	Enforce IT Policies	Provide Client Support
B	14	0,918	Control System	Control Equipment Target Values
B	14	0,826	Provide Prevention & Detections Services	Operate Servers
B	14	0,724	Monitor Reaction	Control Equipment Target Values
B	14	0,632	Monitor Reaction	Start Emergency Cooling Shutdown
B	14	0,536	Supervise Hardware	Provide Client Support
B	14	0,496	Enforce IT Policies	Supervise Hardware
B	14	0,496	Control System	Start Reaction
B	14	0,289	Schedule	Start Reaction
B	16	0,999	Follow Procedures	Report Deviations
B	16	0,999	Follow Procedures	Start Reaction
B	16	0,999	Follow Procedures	Start Emergency Cooling Shutdown
B	16	0,999	Plan IT Policies	Enforce IT Policies
B	16	0,999	Schedule	Start Reaction
B	16	0,999	Feed Chemicals	Start Reaction
B	16	0,999	Provide Prevention & Detections Services	Provide Client Support
B	16	0,999	Provide Prevention & Detections Services	Operate Clients

B	16	0,999	Provide Prevention & Detections Services	Operate Network
B	16	0,999	Operate Network	Operate Servers
B	16	0,999	Operate Network	Provide Communication Services
B	16	0,999	Operate Network	Provide IT Services
B	16	0,999	Plan Schedule	Plan Material Supply
B	16	0,999	Plan Schedule	Schedule
B	16	0,999	Manage IT Assets	Manage IT Services
B	16	0,999	Manage IT Security	Manage IT Services
B	16	0,999	Operate Servers	Provide Communication Services
B	16	0,999	Operate Servers	Provide IT Services
B	16	0,999	Supervise Network	Provide Client Support
B	16	0,999	Supervise Network	Provide Prevention & Detections Services
B	16	0,999	Supervise Network	Operate Network
B	16	0,999	Provide Client Support	Operate Clients
B	16	0,999	Provide Communication Services	Control System
B	16	0,999	Provide IT Services	Plan Material Supply
B	16	0,999	Provide IT Services	Plan Schedule
B	16	0,999	Provide IT Services	Analyse predicitive Maintenance
B	16	0,998	Provide Prevention & Detections Services	Operate Servers
B	16	0,985	Control System	Control Equipment Target Values
B	16	0,983	Operate Network	Operate Clients
B	16	0,965	Provide Mitigation Services	Provide IT Services
B	16	0,947	Enforce IT Policies	Provide Prevention & Detections Services
B	16	0,85	Control System	Start Reaction
B	16	0,733	Provide Mitigation Services	Operate Servers
B	16	0,664	Understand procedures	Monitor Reaction
B	16	0,622	Schedule	Feed Chemicals
B	16	0,511	Provide Communication Services	Operate Clients
B	16	0,47	Enforce IT Policies	Supervise Network
B	16	0,208	Provide IT Services	Operate Clients
C	7	0,999	Operate Network	Provide IT Services
C	7	0,999	Operate Servers	Provide Communication Services
C	7	0,999	Operate Servers	Provide IT Services
C	7	0,999	Supervise Network	Operate Network
C	7	0,999	Provide Client Support	Operate Clients
C	7	0,999	Provide Communication Services	Control System
C	7	0,999	Provide Prevention & Detections Services	Operate Clients
C	7	0,999	Provide Prevention & Detections Services	Operate Network
C	7	0,999	Operate Network	Operate Servers
C	7	0,999	Operate Network	Provide Communication Services
C	7	0,988	Operate Network	Operate Clients
C	7	0,988	Enforce IT Policies	Provide Prevention & Detections Services
C	7	0,954	Enforce IT Policies	Supervise Network
C	7	0,837	Enforce IT Policies	Provide Client Support

C	7	0,814	Enforce IT Policies	Supervise Hardware
C	7	0,808	Plan IT Policies	Enforce IT Policies
C	7	0,712	Supervise Network	Provide Prevention & Detections Services
C	7	0,481	Provide IT Services	Plan Schedule
C	7	0,461	Provide IT Services	Analyse predicitive Maintenance
C	7	0,444	Provide Mitigation Services	Operate Servers
C	7	0,431	Provide Mitigation Services	Provide IT Services
C	7	0,393	Supervise Network	Provide Client Support
C	7	0,337	Control System	Start Emergency Cooling Shutdown
C	7	0,29	Provide Prevention & Detections Services	Provide Client Support
C	7	0,075	Control System	Control Equipment Target Values
C	7	0,065	Provide IT Services	Plan Material Supply
C	8	0,999	Manage IT Assets	Manage IT Services
C	8	0,999	Operate Servers	Provide Communication Services
C	8	0,999	Operate Servers	Provide IT Services
C	8	0,259	Follow Procedures	Start Emergency Cooling Shutdown
C	8	0,164	Understand procedures	Monitor Reaction
C	9	0,999	Manage IT Assets	Manage IT Services
C	9	0,999	Operate Network	Operate Servers
C	9	0,999	Operate Network	Provide Communication Services
C	9	0,999	Operate Network	Provide IT Services
C	9	0,999	Reactive Maintenance (Repair)	Schedule
C	9	0,999	Supervise Network	Operate Network
C	9	0,999	Provide Client Support	Operate Clients
C	9	0,999	Provide IT Services	Plan Schedule
C	9	0,999	Provide IT Services	Analyse predicitive Maintenance
C	9	0,999	Provide Prevention & Detections Services	Operate Clients
C	9	0,999	Plan Maintenance	Do planned maintenance
C	9	0,994	Enforce IT Policies	Supervise Network
C	9	0,994	Schedule	Start Reaction
C	9	0,992	Operate Network	Operate Clients
C	9	0,99	Enforce IT Policies	Supervise Hardware
C	9	0,953	Enforce IT Policies	Provide Client Support
C	9	0,939	Provide IT Services	Plan Material Supply
C	9	0,893	Provide Prevention & Detections Services	Operate Network
C	9	0,778	Plan and organize Production	Manage Work Team
C	9	0,738	Manage IT Security	Manage IT Services
C	9	0,726	Supervise Network	Provide Prevention & Detections Services
C	9	0,62	Provide Prevention & Detections Services	Provide Client Support
C	9	0,591	Schedule	Feed Chemicals
C	9	0,512	Enforce IT Policies	Provide Prevention & Detections Services
C	9	0,261	Plan IT Policies	Enforce IT Policies
C	9	0,26	Provide Prevention & Detections Services	Operate Servers
C	9	0,138	Plan Maintenance	Plan Schedule

C	9	0,073	Check & Prepare Equipment	Feed Chemicals
C	9	0,072	Provide Mitigation Services	Provide IT Services
C	10	0,983	Follow Procedures	Start Emergency Cooling Shutdown
C	10	0,887	Schedule	Start Reaction
C	10	0,238	Feed Chemicals	Start Reaction
C	10	0,09	Follow Procedures	Report Deviations
C	10	0,079	Start Reaction	Monitor Reaction
C	10	0,053	Follow Procedures	Start Reaction
C	11	0,999	Provide Prevention & Detections Services	Operate Clients
C	11	0,999	Operate Servers	Provide Communication Services
C	11	0,999	Operate Servers	Provide IT Services
C	11	0,999	Provide Client Support	Operate Clients
C	11	0,999	Provide Communication Services	Control System
C	11	0,999	Operate Network	Operate Servers
C	11	0,999	Operate Network	Provide Communication Services
C	11	0,999	Operate Network	Operate Clients
C	11	0,999	Operate Network	Provide IT Services
C	11	0,998	Supervise Network	Operate Network
C	11	0,996	Provide Prevention & Detections Services	Operate Network
C	11	0,975	Control System	Start Emergency Cooling Shutdown
C	11	0,739	Control System	Control Equipment Target Values
C	11	0,654	Provide Prevention & Detections Services	Provide Client Support
C	11	0,495	Provide IT Services	Plan Schedule
C	11	0,488	Provide IT Services	Analyse predicitive Maintenance
C	11	0,42	Control System	Start Reaction
C	11	0,333	Supervise Network	Provide Prevention & Detections Services
C	11	0,188	Plan IT Policies	Enforce IT Policies
C	11	0,149	Supervise Network	Provide Client Support
C	11	0,144	Provide Prevention & Detections Services	Operate Servers
C	11	0,07	Provide IT Services	Plan Material Supply
C	11	0,061	Control System	Analyse predicitive Maintenance
C	12	0,28	Feed Chemicals	Start Reaction
C	13	0,999	Follow Procedures	Start Emergency Cooling Shutdown
C	13	0,903	Schedule	Start Reaction
C	13	0,336	Follow Procedures	Report Deviations
C	13	0,168	Follow Procedures	Start Reaction
C	14	0,999	Operate Servers	Provide Communication Services
C	14	0,999	Operate Servers	Provide IT Services
C	14	0,999	Supervise Network	Operate Network
C	14	0,999	Provide Client Support	Operate Clients
C	14	0,999	Provide Communication Services	Control System
C	14	0,999	Provide Prevention & Detections Services	Operate Network
C	14	0,999	Operate Network	Operate Servers

C	14	0,999	Operate Network	Provide Communication Services
C	14	0,999	Operate Network	Provide IT Services
C	14	0,998	Provide Prevention & Detections Services	Operate Clients
C	14	0,994	Operate Network	Operate Clients
C	14	0,982	Enforce IT Policies	Provide Prevention & Detections Services
C	14	0,97	Enforce IT Policies	Supervise Network
C	14	0,834	Enforce IT Policies	Supervise Hardware
C	14	0,824	Enforce IT Policies	Provide Client Support
C	14	0,798	Plan IT Policies	Enforce IT Policies
C	14	0,691	Supervise Network	Provide Prevention & Detections Services
C	14	0,517	Provide IT Services	Analyse predicitive Maintenance
C	14	0,479	Provide IT Services	Plan Schedule
C	14	0,449	Provide Mitigation Services	Provide IT Services
C	14	0,431	Provide Mitigation Services	Operate Servers
C	14	0,377	Supervise Network	Provide Client Support
C	14	0,273	Provide Prevention & Detections Services	Provide Client Support
C	14	0,077	Provide IT Services	Plan Material Supply
C	16	0,999	Provide Prevention & Detections Services	Operate Clients
C	16	0,999	Provide Prevention & Detections Services	Operate Network
C	16	0,999	Operate Network	Operate Servers
C	16	0,999	Operate Network	Provide Communication Services
C	16	0,999	Operate Network	Operate Clients
C	16	0,999	Operate Network	Provide IT Services
C	16	0,999	Supervise Network	Provide Prevention & Detections Services
C	16	0,999	Supervise Network	Operate Network
C	16	0,999	Provide Client Support	Operate Clients
C	16	0,999	Provide Communication Services	Control System
C	16	0,999	Provide IT Services	Plan Schedule
C	16	0,999	Provide IT Services	Analyse predicitive Maintenance
C	16	0,999	Manage IT Assets	Manage IT Services
C	16	0,999	Operate Servers	Provide Communication Services
C	16	0,999	Operate Servers	Provide IT Services
C	16	0,99	Provide Prevention & Detections Services	Provide Client Support
C	16	0,943	Provide IT Services	Plan Material Supply
C	16	0,773	Plan IT Policies	Enforce IT Policies
C	16	0,658	Supervise Network	Provide Client Support
C	16	0,453	Provide Prevention & Detections Services	Operate Servers
C	16	0,236	Follow Procedures	Start Emergency Cooling Shutdown
C	16	0,164	Understand procedures	Monitor Reaction

LIST OF ABBREVATIONS

CPS	Cyber Physical System
DDOS	Distributed-Denial-of-Service Attacks
ECS	Emergency Control System
ERP	Enterprise Resource Planning
FMEA	Failure Modes and Effect Analysis
FRAM	Functional Resonance Accident Method
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability Study
HCR	Human-Robot-Collaboration
HR	Human Resource Department
IoS	Internet of Services
IoT	Internet of Things
IT	Information Technology
MES	Manufacturing Execution System
PCDA	Plan Do Check Act
PESTEL	Political, Economic, Social, Technical, Environmental and Legal Analysis
R & D	Research and Development
RFID	Radio Frequency Identification
RPN	Risk Priority Number
SERP	Enterprise Resource Planning System
SPICE	Software Process Improvement and Capability Determination
STEP	Sequential Time Events Plotting method
TCS	Temperature Control System

ILLUSTRATION DIRECTORY

LIST OF TABLES

REFERENCES

Abul-Haggag, O. Y., & Barakat, W. (2013 Vol 3). Application of Fuzzy Logic Application of Fuzzy Logic Application of Fuzzy Logic Application of Fuzzy Logic Application of Fuzzy Logic Application of Fuzzy Logic Application of Fuzzy Logic Application of Fuzzy Logic Application of Fuzzy Logic Application of Fuzzy Logic Application of Fuzzy Logic for Risk Assessment for Risk Assessment for Risk Assessment for Risk Assessment for Risk Assessment for Risk Assessment using Risk Matrix. *International Journal of Emerging Technology and Advanced Engineering*. (1), 49–54.

Ahlan, A. R., & Arshad, Y. (2012). Understanding Components of IT Risks and Enterprise Risk Management. In J. Emblemsvåg (Ed.), *Risk Management for the Future – Theory and Cases* (297-18). INTECH Open Access Publisher.

Arpornwichanop, A., Kittisupakorn, P., & Mujtaba, I. M. (2005). On-line dynamic optimization and control strategy for improving the performance of batch reactors. *Chemical Engineering and Processing: Process Intensification*, *44*(1), 101–114. https://doi.org/10.1016/j.cep.2004.04.010

Arpornwichanop, A., Kittisupakorn, P., & Hussain, M. A. (2002). Model-based control strategies for a chemical batch reactor with exothermic reactions. *Korean Journal of Chemical Engineering*, *19*(2), 221–226. https://doi.org/10.1007/BF02698405

Aven, T. (2012). The risk concept—historical and recent development trends. *Reliability Engineering & System Safety*, *99*, 33–44. https://doi.org/10.1016/j.ress.2011.11.006

Bakule, L. (2008). Decentralized control: An overview. *Annual Reviews in Control*, *32*(1), 87–98. https://doi.org/10.1016/j.arcontrol.2008.03.004

Bandemer, H., & Gottwald, S. (1995). *Fuzzy sets, fuzzy logic, fuzzy methods*. Chichester [u.a.]: Wiley.

Bao, J., & Xu, S. (2012). Plantwide Control via a Network of Autonomous Controllers. In G. P. Rangaiah & V. Kariwala (Eds.), *Plantwide Control: Recent Developments and Applications* (2nd ed., pp. 387–416). Hoboken: John Wiley & Sons.

Besnard, D., & Baxter, G. (2003). *Human compensations for undependable systems: Technical Report Series* (No. CS-TR-819).

Besnard, D., & Hollnagel, E. (2014). I want to believe: Some myths about the management of industrial safety. *Cognition, Technology & Work*, *16*(1), 13–23. https://doi.org/10.1007/s10111-012-0237-4

Bird, F. E., Germain, G. L., & Clark, M. D. (2014). *Practical loss control leadership* (Third edition). Katy, TX: DNV GL Business Assurance USA, Inc.

Brettel, M., Friederichsen, N., Keller, M., & Rosenberg, M. (2014). How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective. *International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering*, *8*(1), 37–44.

Deutsches Institut für Normung e.V. *Saftey Aspects*. (ISO/IEC Guide, 51:2014).

Dutta, P., Boruah, H., & Ali, T. (2011). Fuzzy Arithmetic with and without using α-cutmethod: A Comparative Study. *International Journal of Latest Trends in Computing*, *2*(1), 99–107.

E.Hollnagl & E.Rigaud (Ed.) 2006. *Stress-Strain Plots as aModel of an Organization's Resilience.*

Engell, S. (2006). Feedback Control for Optimal Process Operation. *IFAC Proceedings Volumes*, *39*(2), 13–26. https://doi.org/10.3182/20060402-4-BR-2902.00013

Feeney, A. B., Frechette, S. P., & Srinivasan, V. (2015). A Portrait of an ISO STEP Tolerancing Standard as an Enabler of Smart Manufacturing Systems. *Journal of Computing and Information Science in Engineering*, *15*(2), 21005. https://doi.org/10.1115/1.4029050

Gerace, T., & Cavusoglu, H. (2009). The critical elements of the patch management process. *Communications of the ACM*, *52*(8), 117. https://doi.org/10.1145/1536616.1536646

Gilchrist, A. (2016). *Industry 4.0*. Berkeley, CA: Apress.

Gökalp, E., Sener, U., & Eren, P. E. (2017). Development of an Assessment Model for Industry 4.0: Industry 4.0-MM. In A. Mas, A. Mesquida, R. V. O'Connor, T. Rout, A. Dorling, & M. Richter (Eds.), *Communications in Computer and Information Science: Vol. 770. Software process improvement and capability determination: 17th International Conference, SPICE 2017, Palma de Mallorca, Spain, October 4-5, 2017, proceedings* (pp. 128–142). Cham: Springer.

Gryna, F. M., Chua, R. C. H., & DeFeo, J. A. (2007). *Juranś quality planning and analysis: For enterprise quality* (5. ed.). *McGraw-Hill series in industrial engineering and management science*. Boston, Mass.: McGraw-Hill.

Gunes, V., Peter, S., Givargis, T., & Vahid, F. (2014). A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems. *KSII Transactions on Internet and Information Systems*, *8*(12). https://doi.org/10.3837/tiis.2014.12.001

Hecklau, F., Galeitzke, M., Flachs, S., & Kohl, H. (2016). Holistic Approach for Human Resource Management in Industry 4.0. *Procedia CIRP*, *54*, 1–6. https://doi.org/10.1016/j.procir.2016.05.102

Heidarinejad, M., Liu, J., La Muñoz de Peña, D., Davis, J. F., & Christofides, P. D. (2011). Handling communication disruptions in distributed model predictive control. *Journal of Process Control*, *21*(1), 173–181. https://doi.org/10.1016/j.jprocont.2010.11.005

Heinrich, H. (1931). *Industrial accident prevention – A scientific approach.* New York: McGraw-Hill book Company.

Hermann, M., Pentek, T., & Otto, B. (2015). *Design Principles for Industrie 4.0 Scenarios: A Literature Review*. Retrieved from Fakultät Maschinenbau website: https://www.researchgate.net/publication/307864150_Design_Principles_for_Industrie_40_Scenarios_A_Literature_Review

Hester, P. T., Collins, A. J., Ezell, B., & Horst, J. (2016). A Review of Problem Structuring Methods for Consideration in Prognostics and Smart Manufacturing. *International Journal of Prognostics and Health Management*. (7). Retrieved from https://www.phmsociety.org/sites/phmsociety.org/files/phm_submission/2016/ijphm_16_016.pdf

Hollnagel, E., Leonhardt, J., Licu, T., Shorrock, & S. *From Safety-I to Safety-II: A White Paper*. Retrieved from https://www.skybrary.aero/bookshelf/books/2437.pdf

Hollnagel, E. (2003). *An Application of the Functional Resonance Analysis Method (FRAM) to Risk Assessment of Organisational Ch: Report Number 2003:09.*

Hollnagel, E. (Ed.). (2006). *Resilience engineering: Concepts and precepts*. Aldershot [u.a.]: Ashgate.

Hollnagel, E., Hounsgaard, J., & Colligan, L. (2014). *FRAM - the Functional Resonance Analysis Method: A handbook for the practical use of the method* (1. ed.). [Middelfart]: Centre for Quality, Region of Southern Denmark.

Hopkins, A. (1999). The limits of normal accident theory. *Safety Science*, *32*(2-3), 93–102. https://doi.org/10.1016/S0925-7535(99)00015-6

Hyatt, N. (2004). *Guidelines for process hazards analysis, hazards identification & risk analysis* (1. ed., [Nachdr.]). Toronto, Ontario, Boca Raton: Dyadem Press; CRC Press Vertrieb.

Ilie-Zudor, E., Kemény, Z., & Preuveneers, D. (2016). Efficiency and Security of Process Transparency in Production Networks—A View of Expectations, Obstacles and Potentials. *Procedia CIRP*, *52*, 84–89. https://doi.org/10.1016/j.procir.2016.07.018

Isermann, R. (1998). On fuzzy logic applications for automatic control, supervision, and fault diagnosis. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, *28*(2), 221–235. https://doi.org/10.1109/3468.661149

Jogwar, S. S., & Daoutidis, P. (2017). Community-based synthesis of distributed control architectures for integrated process networks. *Chemical Engineering Science*, *172*, 434–443. https://doi.org/10.1016/j.ces.2017.06.043

Jokinen, T., Ylén, P., & Jouni, P. (2011). Dynamic Model for Estimating the Added Value of Maintenance Services. In J. M. Lyneis (Ed.), *29th international conference of the System Dynamics Society 2011: Washington, DC, USA, 24 - 28 July 2011* (Vol. 3, pp. 1713–1730). Red Hook, NY: Curran.

Karanki, D. R., Dang, V. N., MacMillan, M. T., & Podofillini, L. (2018). A comparison of dynamic event tree methods – Case study on a chemical batch reactor. *Reliability Engineering & System Safety*, *169*, 542–553. https://doi.org/10.1016/j.ress.2017.10.003

Khalid, A., Kirisci, P., Ghrairi, Z., Thoben, K.-D., & Pannek, J. (2017). Towards Implementing Safety and Security Concepts forHuman-Robot-Collaboration in the context of Industry 4.0. In *39th International MATADOR Conference on Advanced Manufacturing,.* Retrieved from https://www.researchgate.net/publication/318340673_Implementing_Safety_and_Security_Concepts_for_Human-Robot_Collaboration_in_the_context_of_Industry_40

Kletz, T. A. (1982). Human Problems with Computer Control. *Plant/Operations Progress*, *1*(4), 209–211. https://doi.org/10.1002/prsb.720010404

Kletz, T. A. (1991). Human problems with computer control: An update. *Plant/Operations Progress*, *10*(1), 17–21. https://doi.org/10.1002/prsb.720100106

Kletz, T. A. (2001). *An engineer's view of human error: The theme of this book: try to change situations, not people* (3. ed.). New York, NY: Taylor & Francis.

Lachenmaier, J., Lasi, H., & Kemper H.G. Entwicklung und Evaluation eines Informationsversorgungskonzepts für die Prozess- und Produktionsplanung im Kontext von Industrie 4.0. Retrieved from http://www.wi2015.uni-osnabrueck.de/Files/WI2015-D-14-00135.pdf

Lee, E. A. (2008). *Cyber Physical Systems - Design Challenges: Technical Report No. UCB/EECS-2008-8*. Berkeley. Retrieved from EECS University of California website: http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008

Lee, J., Ghaffari, M., & Elmeligy, S. (2011). Self-maintenance and engineering immune systems: Towards smarter machines and manufacturing systems. *Annual Reviews in Control*, *35*(1), 111–122. https://doi.org/10.1016/j.arcontrol.2011.03.007

Lee, J., Bagheri, B., & Kao, H.-A. (2015). A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing letters*, *3*, 18–23. https://doi.org/10.1016/j.mfglet.2014.12.001

Lee, R. M., Assante, M. J., & Conway, T. (2014). German Steel Mill Cyber Attack. Retrieved from https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

Liu, J., La Muñoz de Peña, D., Ohran, B. J., Christofides, P. D., & Davis, J. F. (2010). A two-tier control architecture for nonlinear process systems with continuous/asynchronous feedback. *International Journal of Control*, *83*(2), 257–272. https://doi.org/10.1080/00207170903141051

Lu, Y., Morris, K. C., & Frechette, S. (2016). *Current Standards Landscape for Smart Manufacturing Systems*: National Institute of Standards and Technology.

Lynch, R. (2006). *Corporate strategy* (4. ed.). Harlow: FT/Prentice Hall.

Manhart, K. (2015). Industrie 4.0 - Die nächste Revolution? Potenzial für den Mittelstand. Retrieved from https://www.tecchannel.de/a/industrie-4-0-die-naechste-revolution,2077662

Marwedel, P. (2011). *Embedded System Design*. Dordrecht: Springer Netherlands.

Matson, E., & Prusak, L. (2003). The Performance Variability Dilemma. Retrieved from https://sloanreview.mit.edu/article/the-performance-variability-dilemma/

McConnell, S. (2009). *Code Complete* (2nd ed.). Sebastopol: O'Reilly Media Inc.

Menon, B. G., Praveensal, C. J., & Madhu, G. (2015). Determinants of job stress in chemical process industry: A factor analysis approach. *Work (Reading, Mass.)*, *52*(4), 855–864. https://doi.org/10.3233/WOR-152119

Michael Kohlegger, Ronald Maier, Stefan Thalmann (2009). Understanding Maturity Models: Results of a Structured Content Analysis. In K. Tochtermann & A. Paschke (Eds.): *Journal of universal computer science J.UCS conference proceedings series, Proceedings of I-KNOW '09: 9th International Conference on Knowledge Management and Knowledge Technologies ; proceedings of I-SEMANTICS '09, 5th International Conference on Semantic Systems, Graz, Austria, September 2 - 4, 2009* (pp. 51–61). Graz: Verl. d. Techn. Univ.

Necci, A., Cozzani, V., Spadoni, G., & Khan, F. (2015). Assessment of domino effect: State of the art and research Needs. *Reliability Engineering & System Safety*, *143*, 3–18. https://doi.org/10.1016/j.ress.2015.05.017

Patriarca, R., Bergström, J., & Di Gravio, G. (2017). Defining the functional resonance analysis space: Combining Abstraction Hierarchy and FRAM. *Reliability Engineering & System Safety*, *165*, 34–46. https://doi.org/10.1016/j.ress.2017.03.032

Patriarca, R., Di Gravio, G., & Costantino, F. (2017). A Monte Carlo evolution of the Functional Resonance Analysis Method (FRAM) to assess performance variability in complex systems. *Safety Science*, *91*, 49–60. https://doi.org/10.1016/j.ssci.2016.07.016

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. New York, NY: Basic Books.

Piggin, R. (2011). Lessons learned in automation security? *Assembly Automation*.

Podofillini, L., & Dang, V. N. (2012). Conventional and dynamic safety analysis: Comparison on a chemical batch reactor. *Reliability Engineering & System Safety*, *106*, 146–159. https://doi.org/10.1016/j.ress.2012.04.010

Podofillini, L., Sudret, B., Stojadinović, B., Zio, E., & Kröger, W. (Eds.). (2015). *Safety and reliability of complex engineered systems: Proceedings of the 25th European Safety and Reliability Conference, ESREL 2015, Zürich, Switzerland, 7-10 September 2015*. Boca Raton, London, New York: CRC Press Taylor & Francis Group a Balkema book.

Popovic, V. M., Vasic, B. M., Rakicevic, B. B., & Vorotovic, G. S. (2012). Optimisation of maintenance concept choice using risk-decision factor – a case study. *International Journal of Systems Science*, *43*(10), 1913–1926. https://doi.org/10.1080/00207721.2011.563868

Porter, M., & Heppelmann, J. (2015). How smart,connected products are transforming competition. *Hardvard Business Review*. (October 2015), 96–112,114.

Praetorius, G., Hollnagel, E., & Dahlman, J. (2015). Modelling Vessel Traffic Service to understand resilience in everyday operations. *Reliability Engineering & System Safety*, *141*, 10–21. https://doi.org/10.1016/j.ress.2015.03.020

Qureshi, Z. (2008). *A Review of Accident Modelling Approaches for Complex Critical Sociotechnical Systems*. Retrieved from Australian Government Department of Defence website: http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/9120/1/DSTO-TR-2094%20PR.pdf

Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010). *Proceedings of the 47th Design Automation Conference*. New York, NY: ACM.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, *27*(2-3), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Rausand, M. (2013). *Risk Assessment: Theory, Methods, and Applications*. *Statistics in Practice*. Hoboken: Wiley.

Reason, J. (2009). *Human error* (20. print). Cambridge: Cambridge Univ. Press.

Renn, O., & Klinke, A. (2004). Systemic risks: A new challenge for risk management. *EMBO reports*, *5 Spec No*, S41-6. https://doi.org/10.1038/sj.embor.7400227

Rigaud, E., Hollnagel, E., & Pieri, F. (Eds.) 2008. *Proceedings of the third Resilience engineering symposium: 28-30 October, 2008, Antibes-Juan-les-Pins, France*. *Collection Sciences économiques et sociales*. Paris: Mines Paris, les presses.

Schumacher, A., Erol, S., & Sihn, W. (2016). A Maturity Model for Assessing Industry 4.0 Readiness and Maturity of Manufacturing Enterprises. *Procedia CIRP*, *52*, 161–166. https://doi.org/10.1016/j.procir.2016.07.040

Seck, B., & Forbes, J. F. (2012). Coordinated, Distributed Plantwide Control. In G. P. Rangaiah & V. Kariwala (Eds.), *Plantwide Control: Recent Developments and Applications* (2nd ed., pp. 417–440). Hoboken: John Wiley & Sons.

Šindelář, R. (2005). HIERARCHICAL FUZZY SYSTEMS. *IFAC Proceedings Volumes*, *38*(1), 245–250. https://doi.org/10.3182/20050703-6-CZ-1902.01119

Skogestad, S. (2004). Control structure design for complete chemical plants. *Computers & Chemical Engineering*, *28*(1-2), 219–234. https://doi.org/10.1016/j.compchemeng.2003.08.002

Slifkin, A. B., & Newell, K. M. (1998). Is Variability in Human Performance a Reflection of System Noise? *Current Directions in Psychological Science*, *7*(6), 170–177. https://doi.org/10.1111/1467-8721.ep10836906

Storbakken, R. (2002). AN INCIDENT INVESTIGATION PROCEDURE FOR USE IN INDUSTRY (A Research Paper Submitted in Partial Fulfillment of the Requirements for the Masters of Science Degree in Risk Control). University of Wisconsin-Stout, Menomonie. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.390.6364&rep=rep1&type=pdf

Swanson, L. (2001). Linking maintenance strategies to performance. *International Journal of Production Economics*, *70*(3), 237–244. https://doi.org/10.1016/S0925-5273(00)00067-0

Tippett, M. J., & Bao, J. (2015). Distributed control of chemical process networks. *International Journal of Automation and Computing*, *12*(4), 368–381. https://doi.org/10.1007/s11633-015-0895-9

Toft, Y., Dell, G., Klockner, K., & Hutton, A. (2012). Models of Causation: Safety. In *The core body of knowledge for generalist OHS professionals* (pp. 1–25). Tullamarine, Vic.: Safety Institute of Australia.

Tzezana, R. (2017). High-probability and wild-card scenarios for future crimes and terror attacks using the Internet of Things. *Foresight*, *19*(1), 1–14. https://doi.org/10.1108/FS-11-2016-0056

Van Thienen, S., Clinton, A., Mahto, M., & Sniderman, B. (2016). Industry 4.0 and the chemicals industry: **Catalyzing tranformation through operations improvement and business growth**. Retrieved from https://www2.deloitte.com/insights/us/en/focus/industry-4-0/chemicals-industry-value-chain.html

Vasudevan, S., & Rangaiah, G. P. (2012). Performance Assessment of Plantwide Control Systems. In G. P. Rangaiah & V. Kariwala (Eds.), *Plantwide Control: Recent Developments and Applications* (2nd ed., pp. 253–272). Hoboken: John Wiley & Sons.

Venezia, R. (2012). Software updates: The good, the bad, and the fatal. Retrieved from https://www.infoworld.com/article/2615258/data-center/software-updates--the-good--the-bad--and-the-fatal.html

Verband der chemischen Industrie e.V. (2016). Die Entwicklung der chemischen Industrie - Von Chemie 1.0 zu 4.0: Innovationen für eine Welt im Umbruch: Chemie 4.0. Retrieved from https://www.vci.de/vci/downloads-vci/publikation/2016-12-08-flyer-entwicklung-der-chemischen-industrie-bis-chemie-4-0-druckfreundlich.pdf

Veza, I., Mladineo, M., & Gjeldum, N. (2015). Managing Innovative Production Network of Smart Factories. *IFAC-PapersOnLine*, *48*(3), 555–560. https://doi.org/10.1016/j.ifacol.2015.06.139

Villa, V., Paltrinieri, N., Khan, F., & Cozzani, V. (2016). Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry. *Safety Science*, *89*, 77–93. https://doi.org/10.1016/j.ssci.2016.06.002

Ydstie, B. E. (2002). New vistas for process control: Integrating physics and communication networks. *AIChE Journal*, *48*(3), 422–426. https://doi.org/10.1002/aic.690480302

Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, *8*(3), 338–353. https://doi.org/10.1016/S0019-9958(65)90241-X

Zadeh, L. A. (2008). Is there a need for fuzzy logic? *Information Sciences*, *178*(13), 2751–2779. https://doi.org/10.1016/j.ins.2008.02.012

Zhao, C., Bhushan, M., & Venkatasubramanian, V. (2005). PHASuite: An Automated HAZOP Analysis Tool for Chemical Processes: Part I: Knowledge Engineering Framework. *Process Safety and Environmental Protection*, *83*(6), 509–532. https://doi.org/10.1205/psep.04055

Zukin, M., & Young, R. E. (2010). Applying fuzzy logic and constraint networks to a problem of manufacturing flexibility. *International Journal of Production Research*, *39*(14), 3253–3273. https://doi.org/10.1080/00207540110053570