

Planning and Control of Safety-Aware Plug & Produce

Bassam Massouh



Planning and Control of Safety-Aware Plug & Produce

Bassam Massouh

University West
Department of Engineering Science
SE-46186 Trollhättan
Sweden
+46 52022 30 00
www.hv.se

© Bassam Massouh 2024
ISBN 978-91-89325-66-1 (Printed version)
ISBN 978-91-89325-65-4 (Electronic version)

Acknowledgement

They say PhD is a lonely journey, yet that was not the case for me. I was blessed by the support of many who made my journey fulfilling, rewarding, and exciting.

First and foremost, I would like to express my appreciation to my supervisors, Prof Fredrik Danielsson and Dr Sudha Ramasamy for their invaluable support and guidance throughout this work. Fredrik for always being available to develop, discuss and make ideas a reality. Sudha for the unwavering support and presence, even during the busiest days.

I would like to extend my gratitude to Dr Mahmood Khabbazi and Prof Bengt Lennartsson. Their scholarly discussions and constructive feedback have been crucial in refining the ideas presented in this thesis. Also, I would thank Prof Anna-Karin Christiansson for reviewing this work and providing all-important feedback and proposals to improve and finalise this thesis.

Thanks are due to all my colleagues at University West for creating an enriching academic environment. Special mention to Xiaoxiao Zhang for his help and constructive discussions that aided my research progress.

To my family, in-laws, and my friends for their unwavering encouragement, and for being there for me during the highs and lows. To my parents, Ossama and Ghaida and to my siblings Hussam and Dona, your love and belief in my abilities have been my pillars of strength.

Lastly, but most importantly to beloved Raquiel, my companion in this journey and my life partner, without her love, warmth, and encouragement, I wouldn't have completed this work.

Bassam Massouh

Trollhättan, December 2023

Populärvetenskaplig sammanfattning

Title: Planering och styrning av säkerhetsmedveten Plug & Produce

Föreställ dig en automatiserad produktionsanläggning som omedelbart och automatiskt kan anpassa sig till förändringar utan att kompromissa med säkerheten för den personal som arbetar där. Denna avhandling strävar efter att uppnå just detta genom ett smartare sätt att säkerställa att produktionsanläggningar baserat på Plug & Produce kan hantera säkerhet. Detta innebär att konceptet Plug & Produce nu närmar sig ett industriellt förverkligande. Säkerhet för automatiserade produktionsanläggningar innebär att alla maskiner ska vara utrustade med skydd för att göra arbetet säkrare. Idag är det vanligt med övervakning som skydd, dvs en dator som övervakar att allt går rätt till och stänger av om något är på väg att hända.

I ett produktionsavsnitt som är baserat på Plug & Produce kan man enkelt ställa om, det vill säga, lägga till eller ta bort maskiner, ändra layouten eller ändra på produkter som produceras. Efter en sådan omställning så måste säkerheten i produktionsanläggningen ses över enligt föreskrivna lagar och regler. Traditionellt så kräver detta anlitan av en säkerhetsexpert. Detta medför att en omställning utifrån ett säkerhetsperspektiv är både kostsamt och tidskrävande.

Med resultatet från denna avhandling så går det nu att ställa om utan att behöva implementera nya säkerhetsfunktioner efter varje förändring. Denna forskning har utvidgat kunskapsområdet inom produktionsteknik för att skapa en "smartare fabrik" genom att inkludera säkerhetsfunktioner.

Resultatet inkluderar algoritmer som kan upptäcka potentiella faror i fabriken och automatiskt tillämpa säkerhetsåtgärder för ett övervakat system. Detta innebär mindre tidsåtgång och lägre kostnader för säkerhetsarbetet. De som drar mest nytta av detta är människorna som planerar för hur saker skall tillverkas med hjälp av Plug & Produce. Resultatet av detta arbete underlättar deras arbetsuppgifter och bevarar flexibiliteten i Plug & Produce, vilket eliminerar behovet av att välja mellan flexibilitet och säkerhet

.

Abstract

Title: Planning and Control of Safety-Aware Plug & Produce

Keywords: Plug & Produce, safety assurance, process planning, reconfigurable manufacturing.

ISBN: 978-91-89325-66-1 (Printed version)
978-91-89325-65-4 (Electronic version)

The Plug & Produce manufacturing system is a visionary concept that promises to facilitate the seamless integration and adaptation of manufacturing resources and production processes. The Plug & Produce control system allows for the automatic addition and removal of manufacturing resources, minimizing human intervention. However, the reconfigurability and autonomous decision-making features of Plug & Produce control systems pose challenges to safety design and control functions.

In contrast to conventional manufacturing systems with fixed layouts and processes, ensuring safety in Plug & Produce systems is complicated due to the complex risk assessment process, the difficulty of implementing non-restrictive safety measures covering all possible hazards, and the challenge of designing a reliable controller for consistent safe operation.

This thesis addresses these challenges through various contributions. It introduces an automatic hazard identification method, considering emergent hazards after reconfiguration. A novel domain ontology is developed, incorporating safety models specific to Plug & Produce systems. The work also proposes a generic, model-based, and automatic risk assessment method, along with a method for the safe execution of plans based on the results of the risk assessment.

The results of this research offer benefits to process planners, who are responsible for coordinating the manufacturing processes with product design in the Plug & Produce system. The proposed solution provides tools for process planners to validate their plans and reduces their safety-related responsibilities. The proposed safety assurance method seamlessly integrates into the multi-agent control of Plug & Produce, providing the control system with risk scenarios associated with process plans. This enables proactive and reliable control, effectively avoiding potential risks during system operation.

Acronyms and definitions

C-MAS: Configurable **M**ulti-**A**gent **S**ystem is a control framework for a Plug & Produce system in manufacturing. It leverages multi-agent technology for system control and user-friendly approaches to apply/configure the agents.

DRM: Design **R**esearch **M**ethods is a research methodology that aims to create understanding and support for the design research.

EFSM: Extended **F**inite-**S**tate **M**achine is an extension of traditional Finite-State Machine (FSM) and is used to represent the dynamic behaviour of a system by modelling its state transitions and events.

FMEA: Failure **M**ode and **E**ffects **A**nalysis is a technique for evaluating the effect of a failure of a subsystem or a component on the total system.

Hazard identification: is a systematic identification of reasonably foreseeable hazards.

Hazard: is any potential source of harm, particularly in the context of operations of machinery and equipment, and the physical characteristics of processes.

HAZOP: Hazard and **O**perability Study is a hazard identification technique that includes a structured process for carrying hazard identification of a system from the conceptual design to the decommissioning.

ISO: International **S**tandards **O**rganization.

Logical reconfiguration: is a change in the logic that controls the production system. Within the context of this thesis the controller is based on a multi-agent system and logical reconfiguration is a change in the multi-agent environment.

MBS: Model-**B**ased **S**afety is an umbrella term that covers safety assurance activities using analysis methods based on data models.

Physical reconfiguration: is a change in the layout including adding, removing, and moving resources, in a manufacturing system. In this work, the physical layout of a Plug & Produce system can be reconfigured by plugging or unplugging resources or changing their locations.

PLC: Programmable **L**ogical **C**ontroller is an electronic device that is programmable, often based on the standardised programming language IEC 61131-3. The device is widely used for the control of automated manufacturing systems.

Process Planner: is a stakeholder, commonly an engineer, that takes the role of coordination of the manufacturing processes to conform to the specifications of a product design. In Plug & Produce, a process planner is a stakeholder who has the manufacturing company's inhouse competence. Responsible for setting the manufacturing process plans and setting the goals for parts in a Plug & Produce multi-agent system.

Protective measures: are the measures implemented by designers and users to reduce or eliminate risks.

Risk analysis: is a process that includes hazard identification and risk estimation based on the probability of hazard occurrence and the severity of the harm resulting from a hazard.

Risk assessment: is a systematic process to evaluate risks. It includes hazard identification, risk estimation to decide on risk level and risk evaluation to decide if the risk needs reduction.

Risk reduction: a process that typically follows risk assessment when there exist risks that need to be eliminated or reduced.

Risk Scenario: the events that lead to the occurrence of a hazard.

Risk: the combination of the probability of occurrence of a hazard and the severity of harm caused by that hazard.

RMS: A **R**econfigurable **M**anufacturing **S**ystem is a manufacturing system that is designed for rapid change in hardware and software to adjust the production for different parts of the same product family.

Safety assurance: the planned and systematic actions to ensure that the system is acceptably safe.

Safety function: a function whose failure can cause an increase in risks.

Safety PLC: a special type of PLC that is designed to ensure the safe operation of processes by monitoring the system and controlling safety functions. It uses redundant hardware and safety-related programs to provide a high level of reliability in detecting and responding to potential hazards.

STPA: **S**ystems-**T**heoretic **P**rocess **A**nalysis, a hazard analysis technique used in systems engineering and safety engineering. STPA examines the control structure of the system that can contribute to hazards.

UML: Unified **M**odelling **L**anguage is a visual modelling language that is used to provide a standardized way for documenting object systems.

Appended papers

Paper A. A Framework for hazard identification of a collaborative Plug & Produce system

Presented at the 4th International Conference on Intelligent Technologies and Applications (INTAP) in Grimstad, Norway 2021. Published in Springer, Cham. https://doi.org/10.1007/978-3-031-10525-8_12 - Authors: Bassam Massouh, Sudha Ramasamy, Bo Svensson & Fredrik Danielsson

Author's contribution: Conducted the literature study, analysed the result from that study and earlier experiences, designed the framework, wrote the manuscript, and presented the paper at INTAP 2021 conference.

Paper B. Online hazard detection in reconfigurable Plug & Produce systems

Presented at 33rd International conference on flexible automation and intelligent manufacturing (FAIM) in Porto, Portugal 2023. Published in Springer, Cham. https://doi.org/10.1007/978-3-031-38241-3_97 - Authors: Bassam Massouh, Fredrik Danielsson, Sudha Ramasamy, Mahmood Khabbazi, Xiaoxiao Zhang

Author's contribution: Initiated the idea, conducted the literature study, designed the hazard model and the algorithm, planned, and conducted experiments, analysed the result, wrote the manuscript and presented the paper at FAIM 2023 conference.

Paper C. Model-based reasoning and decisions-making for safe operation in a Plug & Produce environment

Submitted and waiting for reviewers at IEEE Transaction on Industrial Informatics – Authors: Bassam Massouh, Fredrik Danielsson, Bengt Lennartson, Sudha Ramasamy, Mahmood Khabbazi

Author's contribution: Initiated the idea, conducted the literature study, designed the safety-related part of the ontology, main contributor to the algorithms, planned and conducted experiments, analysed the result, and wrote the manuscript.

Other papers by the author:

Software-supported Hazards Identification for Plug & Produce Systems

Presented at 33rd International conference on flexible automation and intelligent manufacturing (FAIM) in Porto, Portugal 2023. Published in Springer, Cham.
https://doi.org/10.1007/978-3-031-38241-3_68 – Authors: Waddah Mosa, Bassam Massouh, Mahmood Khabbazi, Mikael Eriksson, Fredrik Danielsson

Table of contents

Acknowledgement	i
Populärvetenskaplig sammanfattning	iii
Abstract	v
Acronyms and definitions	vi
Appended papers	ix
Table of contents	xi
1 Introduction	1
1.1 Background and basic concepts	2
1.2 Problem description and motivation	6
1.3 Research questions and objectives	7
1.4 Scope and delimitations	8
1.5 Contributions	9
2 Research approach	11
2.1 The model of the research approach	12
2.2 Evaluation of research results	14
3 State of the art	17
3.1 Integration of safety assurance activities within RMS	17
3.2 Model-based solutions to support safety-aware planning and control of RMS	19
3.3 Frame of reference	19
4 The proposed model-based and safety-aware method for planning and control of Plug & Produce	25
4.1 Safety domain ontology of Plug & Produce	25
4.2 Emergent hazards identification and validation of plans safety	28
4.3 Automatic risk assessment and deployment of safety-aware control actions	31
5 Validation of results	35
5.1 Plug & Produce manufacturing scenario	35
5.2 Test results and discussion	37

6 Conclusion..... 41

6.1 Answers to the research questions..... 41

6.2 Recommendations for future research 42

7 Summary of appended papers 45

7.1 Paper A..... 45

7.2 Paper B..... 46

7.3 Paper C..... 47

8 References 49

Appended papers

- Paper A** A Framework for hazard identification of a collaborative Plug & Produce system.
- Paper B** Online hazard detection in reconfigurable Plug & Produce systems
- Paper C** Model-based reasoning and decisions-making for safe operation in a Plug & Produce environment

1 Introduction

This thesis addresses safety issues related to advanced autonomous and automation concepts in production technology. It addresses the shift towards more efficient and flexible production. Within the fourth industrial revolution, Industry 4.0, there is an aim for a paradigm shift with enabling technologies that include and integrate smart and digital factories as well as more human-machine collaboration in production. Plug & Produce is a highly flexible production concept within the context of Industry 4.0.

The idea of Plug & Produce is a production system that undergoes a physical or logical reconfiguration with minimum effort and time. The physical reconfiguration refers to the automatic identification and integration of new manufacturing resources into the Plug & Produce manufacturing system. Also, it refers to rearranging the resources to change the layout of the system. The logical reconfiguration refers to adjusting the control logic that governs the operations of the Plug & Produce manufacturing system. This logic dictates the parts to be produced, the process plans to produce the parts and the communication between logic entities. In Plug & Produce, logical reconfiguration is advantageous as the control logic is created and modified within the company's in-house competencies without the need for consulting external expertise.

In addition, humans and machines are expected to collaborate, ushering in the era of Industry 5.0. The realization of this vision depends on effectively addressing the challenge of safety assurance within flexible manufacturing systems. The established safety assurance methods and standards are built to meet the safety requirements of traditional manufacturing where no changes to the setup are expected. Hence, the reconfiguration property of Plug & Produce is new and challenging from the perspective of common safety assurance practices.

This licentiate addresses the safety assurance problems within the Plug & Produce concept. It contributes to the area of production technology and specifically to the safety of Plug & Produce production systems. One main contribution revolves around the development of support for the process planner. A process planner is a stakeholder in the organisation that utilizes the Plug & Produce technology and has in-house competence. The process planner is responsible for setting the manufacturing process plans and setting the production goals to conform to product design. The proposed solution supports safety validation by the process planner and aims to ensure safety with reduced time and effort after

a reconfiguration in a Plug & Produce system. Another contribution includes the development of a control strategy within the Plug & Produce controller, that reduces the dependence on physical safety measures and safety stops while automatically managing risks. This eases the load on the process planner by eliminating the necessity for extensive safety configuration and maintains the system's flexibility through less restrictive safety measures.

It is important to note that, at this stage of my research journey, this licentiate work primarily involves theoretical development and simulation-based formal validation. I acknowledge that this approach is grounded in theory, and I aim to bridge the gap between theory and practice in future research towards a PhD.

Furthermore, it is essential to recognize that Plug & Produce represents a visionary solution that facilitates the transition from traditional manufacturing to a new era of industry. As we look into the future, envisioning broad adoption and implementation of Plug & Produce, it becomes clear that safety challenges will arise. Currently, there might not be available accident data to analyse and compare because Plug & Produce is not the present but the future of manufacturing industries adopting Industry 4.0 technologies. However, by addressing safety concerns proactively and leveraging the insights gained from our theoretical results, this thesis aims to lay the foundation for safer and more efficient manufacturing as we move into the future.

1.1 Background and basic concepts

This section contains a description of the core concepts and topics in this thesis. Subsection 1.1.1 describes the concept of Plug & Produce from the perspective of different industrial testbeds. Subsection 1.1.2 describes the most relevant industrial safety standards and discusses their applicability to Plug & Produce. Subsection 1.1.3 describes the concept of model-based safety which is an approach that links the design of a system with safety assurance.

1.1.1 Plug & Produce

A Plug & Produce manufacturing system can automatically handle two types of reconfigurations: physical and logical. The physical reconfigurability of a Plug & Produce system comes from the ability of the system to accept adding or removing modular production components or modifying the physical layout [1]. The logical reconfigurability of Plug & Produce arises from its ability to adapt to modified system logic and changes in production plans. During physical reconfiguration, new resources must collaborate seamlessly with existing ones, to ensure harmonious operations within the system. Similarly, in logical reconfiguration, the logic entities, each with its autonomy, collaborate to conform

to modified control logic. The holonic control structure, which is characterized by autonomy and collaboration, aligns with the Plug & Produce system's reconfiguration [2]. This control structure can be achieved with a multi-agent control for Plug & Produce [3]. The multi-agent controller approach proved valid to support the concept of Plug & Produce [4], [5]. In a multi-agent control structure, each modular component is controlled by an agent. An agent is a logic entity that incorporates and integrates the functional features of physical hardware. When combined with the hardware, an agent represents an example of a cyber-physical entity. This allows for a loosely coupled control structure where each agent, representing a component, will be engaged in autonomous decision-making. All agents negotiate and decide the allocation of tasks automatically among each other, without manual intervention, achieving higher flexibility through autonomy [6].

A notable work on Plug & Produce is the IDEA project [7] in which the viability of multi-agent control for seamless shop-floor reconfiguration has been proven by industrial experiments. The multi-agent controller finds operational plans and distributes the tasks automatically based on the production cost and the availability of resources. A more recent advancement within the topic of multi-agent control of Plug & Produce systems is the concept of Configurable Multi-Agent System (C-MAS) [8]. In the C-MAS, there are two main types of agents namely parts and resources. A part agent represents a product, and a resource agent represents manufacturing equipment. For instance, a robot or a machine is modelled as a resource in the C-MAS system. Parts agents are configured with goals. All goals together describe how the part must be manufactured from the start until a finalised product, without specifying details such as needed resources. To achieve a goal, a part makes use of process plans that are designed by a process planner in advance. The C-MAS has the potential to shorten the engineering time and reduce the level of needed competencies by the use of configurable process plans [9].

1.1.2 Safety standards

European directives and national legislation enforce the health and safety of workers in the workplace. While directives define the essential safety legal requirements, standards and guidelines are non-binding documents that aim to facilitate the implementation of the directives. The ISO standards are internationally agreed upon by experts and are widely adopted globally and in the EU as a reference to describe the requirements in the directives.

Noticeably, the ISO standards distinguish between inherent safety (or safety by design) and functional safety. Inherent safety focuses on reducing or eliminating risks by implementing measures within the design of the product, the machine, or

the processes. Functional safety, focuses on the safety-related part of the control system, ensuring that the system is performing its intended functions safely in the presence of a failure that could cause harm.

Several standards provide principles and methodologies for safe design. ISO 12100:2010 provides general principles for risk assessment and safe design of machinery. ISO 13850:2015 provides the principles for the design of emergency stops. ISO 13855:2010 provides guidelines for the position of safeguards in regard to the movement of the human body. ISO 14119:2013 describes the principles of designing interlocking mechanisms to prevent access to hazardous areas if guards are not properly closed. Other ISO standards focus on the design of robotic systems such as the ISO 10218:2011 which provides guidelines for the safe design and use of industrial robots, and the technical specification ISO/TS 15066:2016 specifies the safety requirements for collaborative robot systems and their work environment.

Safety standards that are concerned with the design of the safety-related part of the control system are considered functional safety standards. Notably, ISO 13849:2023 focuses on designing the safety-related part of the control system and provides guidelines for ensuring the safety and reliability of the safety controller. It outlines the method of assessing the Performance Level (PL) of safety functions, which is the required reliability of the controller to mitigate the risks. Also, while it is not an ISO standard, the IEC 61508:2010 is widely used as a functional safety standard. It provides guidelines for the design of the safety-related part of the control system that performs the automated safety functions.

While both ISO 13849:2023 and IEC 61508:2010 use different metrics to determine the requirement for the design of the safety functions, they both emphasise the key role of risk assessment to derive the specifications of the safety-related part of the controller. These standards don't specifically state whether the safety-related part of the control system, which carries out safety functions, must be separated from the equipment control system. However, in practice, there is a tendency to deploy the safety control on a special "Safety PLC" which is a different type from the standard PLC. The safety PLC is designed for higher reliability in the performance of the safety functions including redundancy and failure modes.

Safety standards have generally been well-suited for traditional manufacturing practices. The processes of hazard identification and risk assessment along with the design of emergency stops, interlocking mechanisms, and the placement of physical barriers are made based on the assumption that there will be no alterations to the system's physical or logical configuration. However, they fall

short in guiding the hazard identification, risk assessment and risk reduction of a Plug & Produce system due to its reconfigurability features.

On the other hand, functional safety which has been leveraged for flexible safety logic [10] is a promising notion as it offers a solution for adapting safety measures within a dynamic manufacturing environment. This provides the legal and standardised framework to program the safety-related part of the control system. i.e., apply safety logic in a safety PLC.

While the proposed solution for safety, in this thesis, may be complemented by protective measures and benefit from the legal and standardized implementation of functional safety, it provides a broader solution that integrates safe decision-making logic within the C-MAS control structure.

1.1.3 Model-based safety

Risk analysis and risk assessment must be performed following the guidelines provided by relevant standards. Traditional risk analysis methods such as HAZOP, FMEA, etc. [11] are engineering tools to systematically create risk analysis documentation and achieve safety assurance. However, the increasing complexity of the safety problem as well as the concerns around efficiency and quality of the risk analysis and documentation arises in flexible systems such as Plug & Produce.

Traditional engineering practices for risk analysis and risk assessment often rely on digital documents and drawings as the primary means of communication between the different stakeholders including design engineers, safety engineers, operators, and management. These digital documents may become disconnected, outdated or error prone. One reason is that they are typically done manually which is time and effort consuming. Another reason is that different engineers may work in isolation, leading to the isolation of expertise, knowledge, and potential interoperability problems. Furthermore, traditional approaches cannot perform validation via simulations.

To overcome the issues related to systems complexity, model-based engineering solutions have been used [12]. Within this context, Model-Based Safety (MBS) is suitable for complex and flexible systems such as Plug & Produce [13]. Model-based safety describes model-based development, that is centred on a formal specification or model of the control system and the physical components, followed by a safety analysis of the formal system model [14]. It aims to automate the risk assessment process, reduce the effort and improve its quality, especially in complex systems [15]. In addition, it aims to closely integrate the risk assessment and the design models, as would any change in the model be traced

by the safety assessment [16]. Furthermore, it enables the reusability of the safety-related information which makes it suitable for flexible systems such as Plug & Produce.

MBS and traditional safety methods are interconnected but they serve different purposes within the safety engineering process. Traditional methods excel at hazard identification and risk assessment, while MBS leverages models to analyse system behaviour, enabling automation of the risk assessment and validation activities. For the scope of this work, MBS is used as a foundational framework to approach the safety problem in Plug & Produce which is described in the next section.

1.2 Problem description and motivation

In this section, a description of the safety assurance problem of Plug & Produce is presented along with the motivation for a solution.

There is a legal requirement to perform a risk assessment after each change in a manufacturing system. Also, new safety measures must be implemented based on the newly performed risk assessment. This requirement adds to the time needed for the system to reach full operational capacity which opposes the advantages of the Plug & Produce concept. Hence, there is a need to develop methods and tools to support the risk assessment activities after reconfiguration and to implement modification, if needed, to the safety measures.

Three factors, I-III described below, contribute to the complexity of safety measures modification.

I- emergent hazards: it is complicated to achieve a risk assessment process that results in deducting the required safety measures, this is due to the inherent adaptability of the Plug & Produce system. The supplier of individual resources may provide specifications that help to perform risk assessment. However, a risk assessment must consider the entire system including the composition of all resources, human workers, and processes. In a static system, the identification of these emergent hazards can be done once during the commissioning of the system. However, Plug & Produce systems allow for change in resources and processes which complicates the identification of these emergent hazards.

II- autonomous decision-making: a Plug & Produce system commonly implements a multi-agent controller that is based on autonomous collaboration and decision-making between agents. Autonomous decision-making improves efficiency by automating task distribution and execution and providing optimisation possibilities during runtime. However, this complicates the

implementation of safety measures. The risk assessment must be performed in a way that perceives every possible task distribution and plan execution. Also, the safety measures must cover all these possibilities. Adding this to the issues related to the dynamic nature of Plug & Produce only increases the difficulty of achieving safety. Additionally, the difficulty of perceiving the exact behaviour of the system leads to the implementation of overly restrictive safety measures. This in turn limits the system's flexibility and ability to make decisions for efficient production.

III- risk-free control actions: in traditional automation, the safety requirements are static, and it is possible to design a controller that always satisfies the safety requirements. However, in the case of the Plug & Produce system, due to its dynamic and autonomous features, these requirements are not static and are related to the combination of resources, processes, autonomous task allocation, and plan scheduling. Thus, it is possible that the controller of Plug & Produce violates the safety requirements and produces control actions that generate a risk scenario.

To recapitulate, it is possible to achieve safety by design for conventional manufacturing systems as the layout, the resources, the processes, and the task allocation are all known beforehand and are not changeable. However, in Plug & Produce manufacturing systems, the features of reconfigurability and autonomous decision-making complicate the safety design and the safety control functions. This is because I- the complicated risk assessment process, II- the difficulty to implement safety measures that cover all possible hazards without being restrictive, III- the difficulty to design a reliable controller that leads the system always to safe behaviour.

1.3 Research questions and objectives

The purpose of this research is to bring the Plug & Produce concept to reality by introducing safety. The vision is that organisations that will adopt Plug & Produce for their production will be able to fully utilize the inherent flexibility to effectively respond to changes in demand. Based on this and the problem description in the previous section, the aim of this thesis is:

- To preserve the advantages of swift reconfiguration of Plug & Produce manufacturing systems without neglecting the safety.

To achieve this aim, two objectives have been established.

The first objective is to develop a framework to support safe process planning in a Plug & Produce system. This includes the automatic identification of the

emergent hazard after logical or physical reconfiguration and the delivery of safety-related information to the process planners to validate their plans.

The second objective is to develop a safety-aware control strategy. This includes automatic risk assessment and automatic deployment of control actions that ensure the system's behaviour doesn't generate unsafe situations.

Accordingly, the following research question has been formulated:

RQ1. How can a generic hazard identification method that identifies emerging hazards and supports safety-aware planning and validation for a Plug & Produce system be formulated?

RQ2. How can a Plug & Produce system control strategy automatically perform risk assessment and satisfy control requirements for safety?

This thesis answers the research questions and contributes to the achievement of the declared objectives by going beyond state-of-the-art research in the field. The answers to research question RQ1 were validated by demonstrating use cases and the answers to research question RQ2 were validated using a formal verification method.

1.4 Scope and delimitations

Within the scope of this work, the concept of a Reconfigurable Manufacturing System (RMS) is included. A reconfigurable manufacturing system is a manufacturing system that is designed for rapid change in hardware and software to adjust the production for different parts of the same product family. The literature on the safety of Plug & Produce systems is limited. Thus, the literature study includes previous works on RMS safety. The literature on RMS safety is relevant since Plug & Produce is an implementation of a reconfigurable manufacturing system and it shares the same core characteristics of RMS as described by Koren [17].

This thesis focuses on the model-based approaches used for the safety of RMS and Plug & Produce systems. Established and commonly used risk analysis methods such as HAZOP, and FMEA [11] are considered within the framework of model-based safety; however, this thesis is not limited to a specific method. Instead, it examines the broader, more generic term of model-based safety, allowing for a comprehensive exploration of safety assurance within the context of RMS and Plug & Produce systems.

It's important to clarify that the scope of this thesis does not include the safe design of individual components or the design of physical safety barriers and emergency stops within a manufacturing system. Additionally, topics related to

ergonomics are beyond the purview of this research. Moreover, it's worth noting that hazards and safety issues arising from the unintended use of resources or unsafe interaction between the operator and machines are not within the scope of this thesis. These types of hazards can be mitigated with established safety assurance methods and addressed by engineering practices. More advanced human-machine interaction has been studied before, most recently Hanna [18] explored the safety of human-robot collaboration. Such approaches and other traditional approaches for designing the safety-related part of the control system i.e., the safety PLC, cover the topics of safety from a human-machine interaction perspective. Instead, the focus of this work is addressing safety concerns related to the system's reconfiguration, and control actions.

1.5 Contributions

The contribution of this work is in the domain of production technology and specifically in the topic of safety assurance of Plug & Produce manufacturing systems. The contributions are summarized as follows.

- An automated hazard identification method for Plug & Produce, that identifies emergent hazards is formulated and developed. This provided process planners with safety awareness facilitating plan validation.
- A new domain ontology that integrates safety models in Plug & Produce systems is presented. The ontology is designed to automatically update knowledge through application models.
- A generic model-based approach for automatic risk assessment using the domain ontology is formulated and developed.
- A control strategy is formulated within the C-MAS controller of Plug & Produce emphasising proactive safety-aware control actions to prevent risks before they occur and reduce safety responsibilities and effort through reliable control.

2 Research approach

In the field of engineering science, commonly employed research methodologies include experiments, surveys, case studies, design research, action research, and interactive research [19]. Experiments, surveys, and case studies are methodologies typically employed to gain a deeper understanding of existing phenomena. For instance, experiments are used to analyse how a system or a process behaves under different conditions while surveys and case studies gather data to analyse patterns and relationships within specific contexts.

Interactive research is a research approach that emphasises collaboration and active engagement between researchers and stakeholders [20]. This approach is often used to address practical, real-world problems, making it particularly suitable for interdisciplinary and community-focused research.

Action research is concerned with addressing practical problems, with a focus on actions to achieve the needed change and a focus on collaboration between researchers and other stakeholders. It involves iterative cycles of planning, action, observation, and reflection to understand and improve existing practices or situations in a practical and context-specific manner [21].

In contrast, design researchers often aim to contribute to the theoretical understanding of design and innovation. Design research focuses on the creation of artefacts to solve practical problems and involves evaluating the merits of the solution to determine the usefulness of the artefacts to the targeted group [22].

Blessing and Chakrabarti [23] define design as, “Design is a complex activity that involves artefacts, people, tools, processes, organisations, and the environment in which this takes place. Design research aims at increasing our understanding of the phenomena of design in all its complexity.” They state that design research has two aims, first to create knowledge about the development process of the artifact and second to improve the artifact development and its results. In this context, an artefact is commonly understood as a human-made object created to address a practical problem.

Design Research Methods (DRM) is a well-established and comprehensive framework that covers the entire design research process [23]. It emphasizes the iterative development of solutions. The DRM consist of four steps, Research clarification, Descriptive study I, Prescriptive study, and Descriptive study II. Research Clarification is the first step of DRM, an initial description of the current

and the future desired state is made. This phase provides a solid foundation for the subsequent stages. Next, during Descriptive Study I, a comprehensive investigation into the current state is conducted, resulting in a clearer description of the problem. In depth-literature review and empirical study can be a foundation to gather the required data for analysis and gain deeper insights, setting the stage for identifying areas in need of improvement. The third step is a Prescriptive study, in which innovative solutions (artefacts) or design principles are proposed based on the findings from the previous steps. These solutions aim to address the identified problem effectively, often drawing from established theories and best practices within the relevant field. Finally, the fourth step is Descriptive Study II: following the implementation of the proposed solutions, an evaluation is conducted, on the impact of the developed solutions to support the achievement of the desired future state. This step involves empirical studies to collect data and evaluate the effectiveness of the solutions, identify any unexpected issues, and gather insights to further refine the design.

2.1 The model of the research approach

The DRM proposed by [23] was chosen as a research methodology for the systematic achievement of the intended solution in this thesis. The reason for choosing this methodology is that the Plug & Produce system is still not adopted in the industry. Thus, it is difficult to obtain data from the real-world. The DRM is relevant as it provides the framework for the theoretical contribution.

It is worth noting that the DRM was not followed obediently but an adaption of it was used to systematically design the needed solution. Figure 1 describes the four stages, in the context of this thesis, including the used approach, the deliverables and the results at each stage.

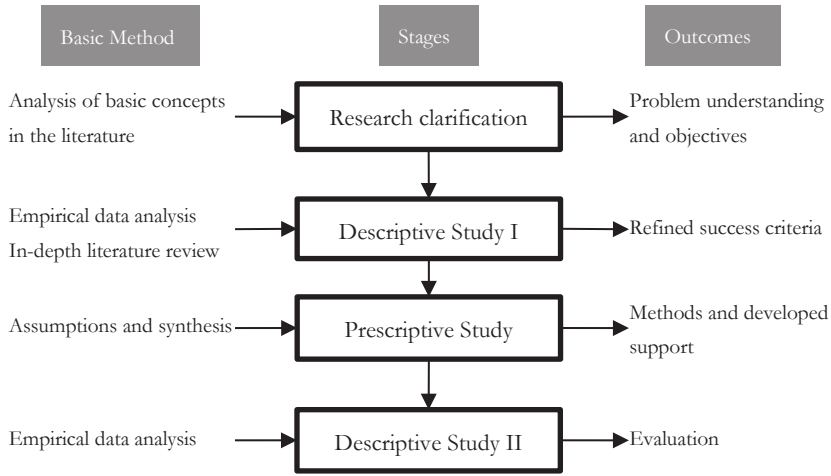


Figure 1 The DRM stages adopted in this thesis.

In the Research Clarification stage, an analysis of the literature and the basic concepts was achieved to find factors that help to validate and clarify the objectives and the development of a successful solution. Based on the findings, an initial understanding of the situation is developed as well as an initial description of the desired situation. The initial understanding describes the current problems facing the realization of safe Plug & Produce which is as described in the introduction, the requirement of risk assessment and reduction after a change in the system. The initial desired future situation is described to support the safety assurance process after a system reconfiguration.

The Descriptive Study I stage includes an in-depth literature review in the area of safety of reconfigurable manufacturing systems. It has been noticed that the scientific literature regarding the safety of the Plug & Produce system is rather small and to obtain a deeper clarification of the problem area, the literature on safety in RMS was studied. Furthermore, to obtain a better understanding of the existing situation, the research presented in paper A was conducted and descriptive data were gathered based on the use case scenario of human-robot collaboration within Plug & Produce. The logical reasoning obtained from this study as well as the findings in the literature led to a better description of the problems and refined success criteria. This includes the identification of the potential emergent hazards that are related to the system reconfiguration and the complexity of the hazard identification in general due to several factors that include lack of interoperability, autonomous decision making and the changing safety requirements. These problems are thoroughly described in section 1.2.

based on the increased understanding, the detailed objectives were derived. These objectives are described in section 1.3.

In the Prescriptive Study step, the in-depth understanding from the previous step is used to elaborate on the desired future state. This involves formulating assumptions that contribute to achieving the desired future state. In this step, one assumption was that a model-based and automatic hazard identification method is useful to tackle the complexity of risk assessment of Plug & Produce. Another assumption was that synthesising a control algorithm that automatically discovers the risk situations and generates control actions that avert the risk situations, leads to non-restrictive and proactive safety control. The result of this step is a solution that is ready to be evaluated. The developed solution includes model-based and automatic hazard identification to support safety-aware planning, and second, a safety-aware control strategy that schedules the execution of the plans safely.

In the Descriptive Study II step, two studies were carried out to evaluate the developed solution. Paper B presented a model-based and automatic hazard detection method for Plug & Produce, that allowed the process planner to receive a generated hazard list based on the logical configuration of the system. Furthermore, paper C presented a method for model-based reasoning and decision-making for safe operation in Plug & Produce. The presented method includes a control strategy within the Plug & Produce controller that guarantees the safe execution of plans. The results of the method were validated using a formal verification.

2.2 Evaluation of research results

The main approach to achieve the solution in this thesis was an algorithmic approach, which was presented in papers B and C. The proposed algorithms were verified using formal methods which are widely used in the automatic control domain to proof validity and reliability [24].

Moreover, validity concerns the accuracy of the results as if the result corresponds to what is intended to be studied and concerns that the results are valid. To address this matter, this section describes the correlation between the appended papers and the research questions, the objectives, and the aim of this thesis.

Three papers contributed to answering the research questions. The results of papers A and B include the definition and the detection of emergent hazards within the Plug & Produce reconfiguration, the automatic detection and visualization of hazards after reconfiguration and the foundation for model-based and automatic risk assessment of Plug & Produce systems. Paper C presented a novel domain ontology that includes safety models. Also, completed the model-

based and automatic risk assessment and implemented an algorithm for safety planning and decision-making within the C-MAS controller.

The first research question addressed in this work is to formulate a generic hazard identification method that supports safety-aware planning and validation, with papers A and B contributing to answering this question. Additionally, for the second research question, which explored the development of a system control strategy that automatically performs risk assessment and reduces risks, papers B and C contributed to the answers. By addressing research question one, it becomes clear that automated hazard identification can equip process planners with the safety knowledge required for safety-aware planning, reducing their responsibilities and efforts. Thus, the first objective of achieving the safe aware process is achieved. Furthermore, the second objective is realized by maintaining the generality of the automated assessment methodology, enabling the identification of safety requirements and the development of a reliable controller that always meets these requirements, effectively satisfying objective number two. With the fulfilment of objectives one and two, the research's goals are accomplished. Figure 2 describes the validity of the research outcome so that they are accurate and achieve the aim.

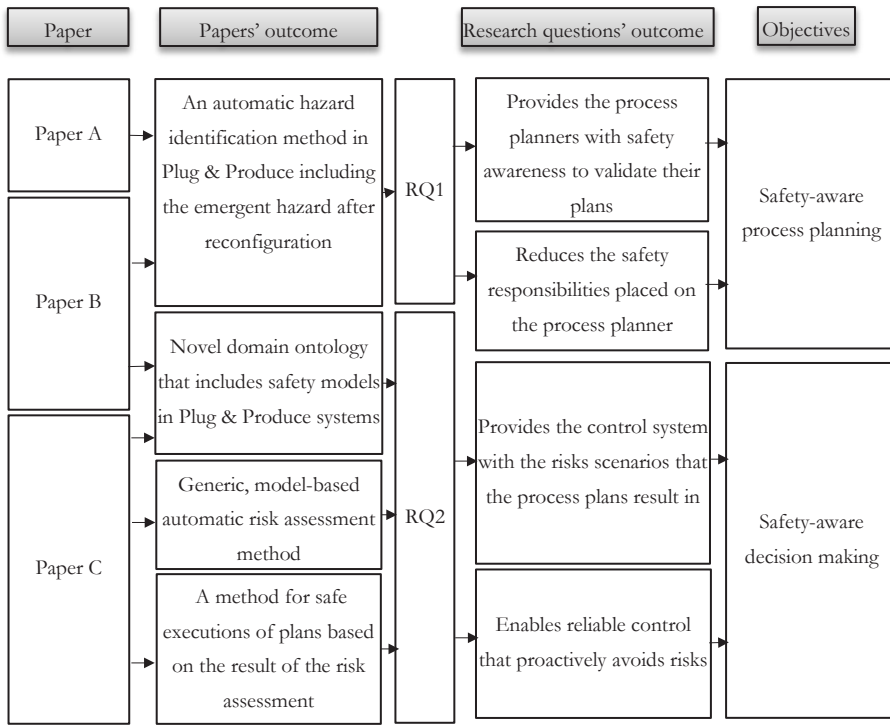


Figure 2 The validity of the appended papers to answer the research questions and achieve the objectives.

3 State of the art

The state-of-the-art chapter comprises three key sections, Section 3.1, explores safety assurance approaches within RMS and the involvement of different stakeholders in safety assurance activities. Section 3.2, focuses on model-based safety approaches, with an emphasis on knowledge representation and automated risk assessment. In section 3.3, a frame of reference is presented to position this thesis within the existing literature, underscoring its two significant contributions: first empowering process planners to validate the safety of production plans, and second formulating a safety-aware control strategy for Plug & Produce systems. Figure 3 shows a stacked Venn diagram of the focus scientific area that this work contributes to which is Plug & Produce safety and its relationship with broader scientific areas.

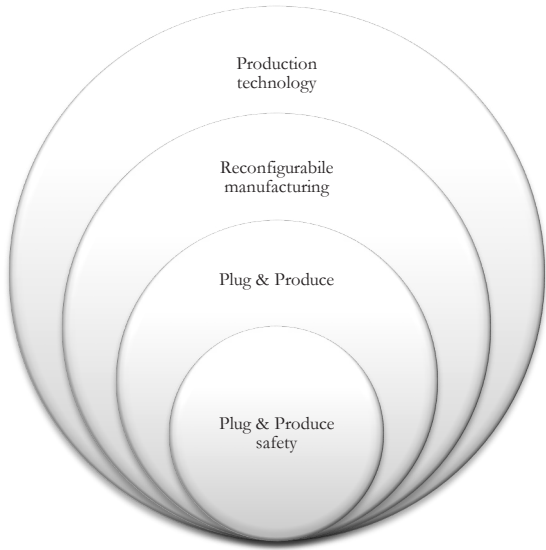


Figure 3 Stacked Venn diagram representing the focus scientific area of contribution of the thesis.

3.1 Integration of safety assurance activities within RMS

New methods are needed to support the integration of safety in RMS [25]. This entails identifying key safety activities spanning from the system's design phase to

the deployment of reconfigurations and must address the changes in both hardware and software [26]. Safety assurance for RMS, as described by Jaradat et al. [27], is characterized by modularity, cooperation, continuity, and on-demand capabilities. This approach involves the formulation of safety assurance cases, which consist of a network of services involving RMS stakeholders, including component suppliers and integrators. These services encompass safety information descriptions for individual components and the integrated system. Moreover, Etz et al. [28] have identified safety service groups that are a foundation for the implementation of functional safety within RMS. These service groups include knowledge representation, discovery of change, visualization and modification, configuration, and deployment. Knowledge representation focuses on information storage and automated reasoning, aided by semantics and ontologies. The discovery service group automates information detection and gathering from the physical world, representing it in the ontology. Visualization and modification enable the exchange of information with the knowledge representation service. Configuration is responsible for creating safety reconfigurations based on ontology information, and deployment oversees the implementation of desired configurations.

The involvement of different stakeholders is necessary throughout these safety activities [26]. Involving all parties in risk assessment and feedback ensures comprehensive safety assurance. In addition, the safety assurance methods must consider providing seamless interaction between the employees and the smart manufacturing system. According to Jaradat et al. [27], machine suppliers have the responsibility of ensuring individual machine safety and providing comprehensive safety information. System integrators, on the other hand, are responsible for ensuring complete system safety. Hillen et al. [29] align with Jaradat's distribution of safety assurance activities, proposing an RMS safety assurance lifecycle derived from the IEC 61508 functional safety lifecycle. This approach advocates interoperable safety cases from machine suppliers and empowers RMS users to dynamically compose a general safety case from modular safety cases provided by suppliers.

Another aspect to be considered when developing safety methods for RMS is that the smart manufacturing system must include methods to manage the risks on its own reducing the burden on employees to process excessive safety information [17]. The presented model-based approach in this thesis emphasizes this idea, it also focuses on the control structures and the systematic identification of interactions within a system that lead to a hazard. The reviewed approaches focus on functional safety and primarily centre on ensuring the safety of individual functions within a system through redundancy and fault tolerance measures. The

presented model-based approach in this thesis seeks to uncover the causes of harm by modelling and analysing how the control processes manage hazards.

3.2 Model-based solutions to support safety-aware planning and control of RMS

Knowledge representation plays a vital role in achieving interoperability and reusability across various phases and responsibilities, from suppliers to integrators and from the design of machines to system configuration. Knowledge representation is often facilitated by the utilization of ontologies, which serve as a fundamental means of knowledge representation [30]. Sonfack et al. [31] have categorized ontologies into three levels: top-level ontologies, which provide high-level knowledge representation and can be further customized for specific domains; domain and task ontologies, which focus on specific concepts and offer reusable knowledge within their respective domains; and application ontologies, which are tailored to specific use cases within a domain. Many ontologies have been developed to support hazard analysis techniques like HAZOP and FMEA [32]–[35].

Model-based hazard identification techniques enhance interoperability and reusability of safety knowledge and enable the inference of hazards. This enables the automation of the risk assessment process and accelerates the safety confirmation process [36]. Furthermore, the confirmation of control and decision-making processes involves the modelling of plans, and using model checking makes it possible to confirm that manually set safety requirements are satisfied [37].

The automated risk assessment can contribute to the generation of safety requirements, which are used to apply physical safety reconfiguration [13] or to provide a generalized safety program. This safety program needs to be deployed to the safety-related components of the control system. This deployment can be performed manually with support from the system [38], or it can be automatically deployed to a safety PLC [39].

3.3 Frame of reference

Similar to the concepts presented in [26]–[29], in the context of C-MAS Plug & Produce, the distribution of tasks among stakeholders evolves across different phases, each with distinct responsibilities. The main stakeholders involved in the safety assurance process of Plug & Produce are the process planners and the suppliers of resources such as robots, machines, and conveyors.

Suppliers take on the role of ensuring the safe design of their equipment. They are also responsible for offering comprehensive safety information that aids in identifying potential hazards within operational workspaces. They provide safety-related information about their resources in a format that is both understandable and exchangeable, allowing interoperability among stakeholders as proposed in [27][28]. Within this work, resources may come pre-configured with all hazard-related data already from the supplier. However, a process planner can add hazard information to a resource if it is necessary.

For Plug & Produce the process planners replace some of the tasks of the traditional system integrators as in [27][29]. These tasks include determining the location of resources, identifying resources to be plugged in/out of production, and the location of generic physical barriers and emergency stops. Additionally, process planners are responsible for designing the production plans and creating the logic for parts' goals.

Figure 4 describes safety assurance activities within the safety life cycle of a Plug & Produce system as proposed in this thesis. It shows the position of the thesis compared to the literature. The dotted boxes highlight the new contributions of this thesis.

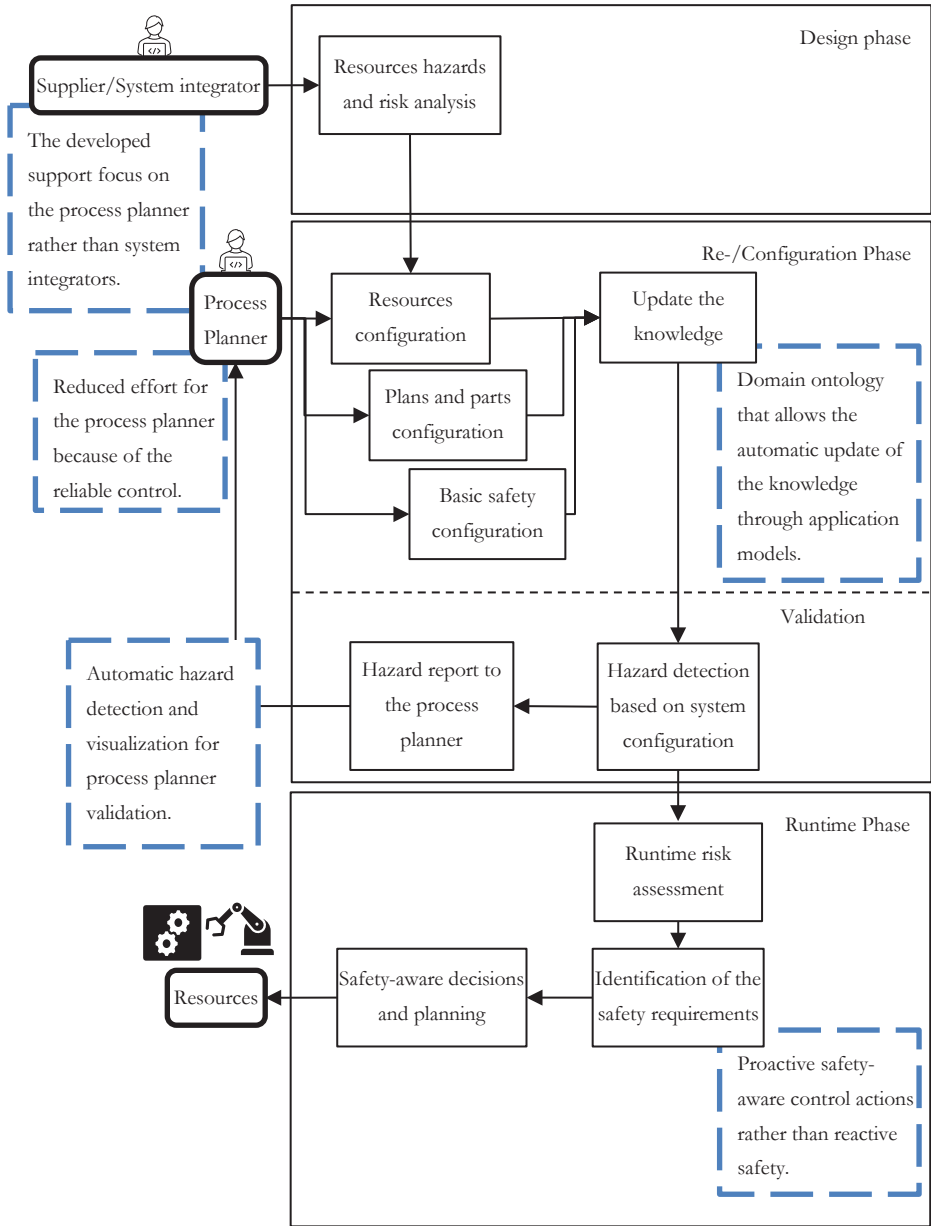


Figure 4 The safety lifecycle of the Plug & Produce system. The text in the blue dashed boxes describes the contributions of the thesis.

Notably, there are three distinguished phases, design of resources, Plug & Produce system configuration, and runtime. In the design phase, the supplier provides instructions on the safe operation of their equipment which forms the safety knowledge about individual resources. This knowledge is used to create resource models that incorporate safety information. In the system configuration phase, the process planner formulates both process plans and goals for parts that later will form the multi-agent system's behaviour. This phase results in a logical configuration. Next, the emerging hazards of the newly established agent's behaviour are identified, and the process planner gains a comprehensive understanding of the hazards associated with logical reconfiguration. This supports the process planner with the safety validation task.

During runtime, automatic risk assessment is performed constantly to identify the control actions that result in a risk scenario in the executable plans. The C-MAS controller, equipped with the result of the risk assessment, makes informed decisions. These decisions are safety-aware, with the primary objective of allocating tasks to the available resources without generating a risk scenario.

From the literature, safety assurance in previous approaches ultimately depends on the system integrators' safety configuration. In this new approach, the control system is trusted with significant responsibility for avoiding risks. The developed method in this thesis targets the process planner which is a novelty as usually the support is provided to system integrators.

Previously proposed hazard ontologies are within different levels, ranging from high-level representations [31] to domain-specific ontologies like those focused on hazards in construction activities [40], cyber-physical systems [41], or fire and explosions in the process industry [42]. Some also are lower application-level ontologies, as in [39][38]. In this thesis, a novel domain ontology is introduced to represent safety knowledge within the context of Plug & Produce systems. This ontology can be implemented in RMS as they share the same or similar control structure. High-level ontologies give the inspiration to develop the Plug & Produce domain ontology which is unique as no other Plug & Produce domain ontology, that includes safety knowledge, can be found in the literature. High-level ontologies are general purpose and can be the foundation for developing more tailored ontologies, but lower-level ones suffer from the need that the system model must be changed if the application of the system has changed. This thesis introduces an ontology at the domain level and represents the safety knowledge within Plug & Produce.

Moreover, model-based approaches such as in [32]–[35], [43]–[45], leverage ontologies to address system complexity and hazard identification. Some other model-based approaches further develop the solution to automate the risk

analysis, such as [36][46]. Others also automate the deployment of new safety configurations to PLCs, as demonstrated in [39][38]. However, the contribution of the approach presented in this thesis lies in its comprehensive safety solution for ensuring the safety of reconfigurable manufacturing systems encompassing safety knowledge representation, discovery of change, visualization of safety information and validation, safety configuration, and deployment. Unlike the solutions found in the reviewed literature, this approach eliminates the need for creating a new model for each new application.

In contrast to existing solutions, which commonly focus on reactive functional safety measures aimed at minimizing risks associated with risk scenarios, the approach proposed in this thesis is proactive. Rather than relying on reactive measures, such as those associated with functional safety, this approach emphasises safe control actions and planning.

The originality is the focus on detecting and implementing control actions, which are decisions made by the system's controller, that actively work to prevent the emergence of risk situations. This approach is different from other solutions that primarily rely on reactive measures, such as functional safety, to manage risks after they have occurred. While reactive safety measures are crucial for responding to failures and unintended use of the system, proactive safety aims to reduce the likelihood of risk scenarios altogether.

4 The proposed model-based and safety-aware method for planning and control of Plug & Produce

This chapter describes the solution to the safety problems of Plug & Produce addressed by this thesis. Section 4.1 presents the proposed safety domain ontology; section 4.2 presents the method to identify the emergent hazards and plan validation; section 4.3 presents the method for automatic risk assessment and safety-aware control actions.

4.1 Safety domain ontology of Plug & Produce

The Plug & Produce system's logic architecture is based on multi-agent system in which an agent is a software component that embodies the functional aspects of physical hardware. The C-MAS Plug & Produce ontology incorporates the system's logic architecture and safety-related information. The ontology includes two types of agents: parts and resources. A part agent represents a product to be produced and a resource agent represents a manufacturing resource in the multi-agent system.

A part agent has one or more goals to be achieved and to achieve the goals they use process plans. Process plans are representations of the operations that are needed to achieve a production goal. These process plans are composed in an abstract way as they are made without specifying which resources to use. This non-restrictive design of plans enables one aspect of the C-MAS flexibility, in which a part autonomously chooses the execution of an abstract plan based on negotiations and its decision-making strategy.

A resource agent has one or more interfaces, and the interfaces have one or more skills. Skills represent resources' capabilities and interfaces represent the resources' compatibility to participate in a process plan. Also, interfaces group the skills of a resource, to enable or disable these skills based on agents' negotiation.

Abstract process plans are composed of abstract interfaces which ensures that plans are made without specific instances of interfaces. In these abstract process plans, skills are demanded on abstract interfaces. Moreover, to provide higher flexibility, skills can also be abstract, this is typical for a skill that requires other skills to be able to complete its task. An example is a robotic gripper tool that has

the skill "*load*". This skill will include a process plan that demands another skill "*moveTool*" that can be offered by a robot.

This thesis proposes a C-MAS Plug & Produce ontology that incorporates safety-related information with the system's logic architecture. This information enables the automatic risk assessment of the process plans. One piece of information is related to hazard identification. According to the safety standard ISO 12100, the objective of hazard identification of a machine is to list all hazards within the determined machine limitation. This includes investigating the intended use of the machine and identifying any source of harm within the associated task. In a Plug & Produce environment, this corresponds to hazard identification of resources. Hazard identification of a single resource includes determining the set of skills that the resource can perform and identifying the hazards associated with each of the skills.

A skill's process plan can include a structured text code that is communicated with the physical resources in the production system. When a skill is composed in a way that only includes the agent logic that instructs the physical resource, the hazards can be easily identified and fetched from the hazard information identified in the design phase. However, when the process plan includes other skills to be achieved by other resources then it is required to fetch the hazards related to these remote skills. Modelling the hazards associated with a skill allows for including this safety-related information within the system's logical configuration and allows for the reusability of this information when the skill is demanded for the execution of a process plan.

The flowing formalism is proposed to incorporate safety-related information with the system's logic architecture and establish the ontology model. An interface is denoted as *if*, and is defined as the tuple, $if = \langle S_{if}, V_{if} \rangle$, where S_{if} is a set of skills of the interface and V_{if} is a set of variables. A skill $s \in S_{if}$ is defined as the tuple: $s = \langle \pi_s, \tau_s, H_s, o_s \rangle$, where π_s is the process plan of skill s , τ_s is the type of skill, H_s is a set of hazards, and o_s is operating space. Hazards that are identified on skills during the resource design phase are also included in the ontology. A single hazard denoted $h \in H_s$ is defined with the tuple, $h = \langle k_h, \tau_h \rangle$, where k_h is risk level and τ_h is the type of targeted skill by the hazard h . The operating space o_s is the physical space in which a resource performs the skill s and this attribute is used to detect unsafe situations in a certain space. The term is adapted from the standard ISO 10218 and is extended to represent the occupied space by a resource while it performs the skill s . The operating space is defined by its shape and dimension, and it has a coordinate system that is relative to the resource coordinate system.

The ontology is modelled using the Unified Modelling Language (UML). UML is a visual representation tool used to depict and communicate the structural and behavioural aspects of a software system's architecture. The UML model of the ontology is shown in Figure 5. The proposed ontology extends, with safety models, an ontology proposed earlier for multi-agent control of Plug & Produce [47]. Figure 5 shows a UML model that focuses on the safety-related part of the system's logic architecture, mainly the classes Skill, Hazard, Space and Risk.

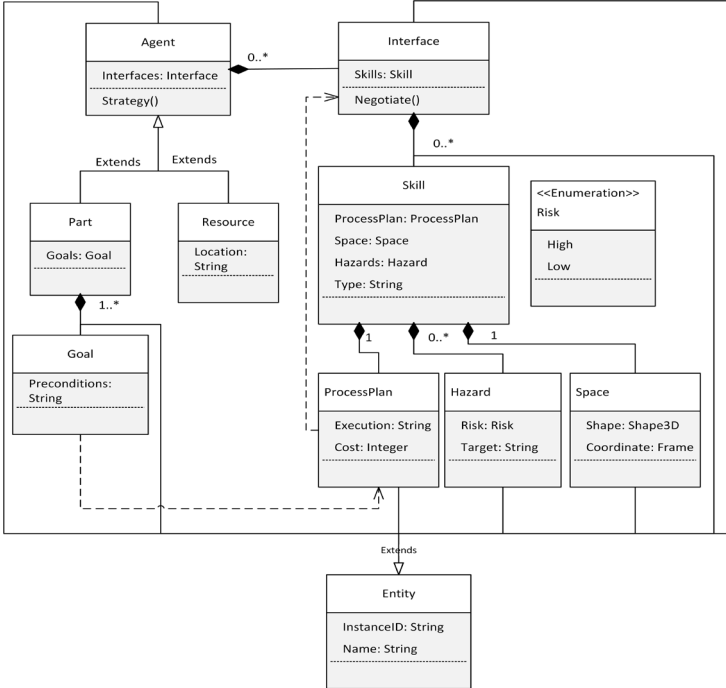


Figure 5 UML class diagram representing the C-MAS Plug & Produce ontology.

Class Agent has an attribute Interface of type Interface and the relationship between class Agent and class interface is a composition relationship of zero to many. This means that an agent can have zero to many interfaces. Also, class Agent has a method Strategy() and the algorithms proposed within this thesis are part of Strategy().

Classes Part and Resource have each an inheritance relationship with class Agent. Class Part extends class Agent with goals and a part can have one to many goals. This is implemented with one to many composition relationship with class Goal. Class Resource extends class Agent with its location.

Class Skill has composition relationships with classes ProcessPlan, Hazard, and Space and its attributes are based on these relationships. Additionally, this class has the attribute Type of type String. Class ProcessPlan has two attributes, Execution of type string and Cost of type integer. Execution is the Structured Text code of the process plan and Cost is a generic value that is used for optimisation e.g., energy consumption, time, or cost value. Class Goal uses process plans i.e., process plans as recipes to achieve the goal. Also, the class ProcessPlan uses interfaces i.e., the Structured Text code of the process plans includes interfaces. Class Hazard has two attributes, Risk and Target. Attribute Risk is of type Risk which a value from enumeration list of High and Low. Attribute Target is of type String, and it is used to detect if the hazard instance targets a specific skill. To detect this scenario, the attribute Target of a Hazard instance must match with the attribute Type of a Skill instance. Class Space has two attributes Shape and Coordinate. Shape is a representation of the operational space occupied by the skill during its execution and Coordinate decides along with the attribute Location of a Resource instance the location of the Space instance. It is worth noting that this type of representation of space is simplified within the scope of this thesis and the worthiness of further formulation is considered for future work.

All classes in the ontology, except Part and Resource, extend a class Entity and there is an inheritance relationship between all classes and class Entity. Class Entity has two attributes, InstanceID of type string to give a unique ID for each instance and Name of type string that is the name of the instance.

4.2 Emergent hazards identification and validation of plans safety

Composing the process plans and determining the sequence of goals are two main tasks of the process planner. The goals and process plans must be validated for emergent hazards and confirmation of safety is required from the process planner. To achieve this the process planner is presented with a hazard list related to the system's logical configuration. This is to permit the process planner to validate the production plans. The generation of a hazard list is done automatically using an algorithm that leverages the hazard models and identifies the emergent hazards. This algorithm is thoroughly described in paper B. The algorithm recursively checks all process plans to identify hazards. Figure 6 illustrates the data mapping from logical configuration, in the left column, to the algorithm functions, in the right column. The sequence of which the algorithm function is achieved can be seen under “Generation of hazard list”.

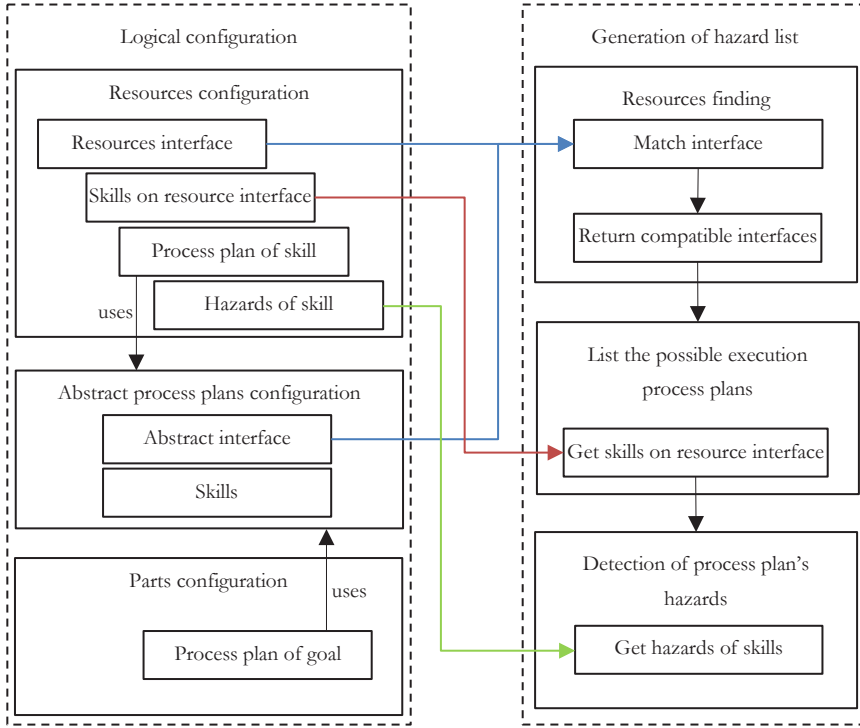


Figure 6 Data mapping and functions to automatically generate the hazard list of a Plug & Produce logical reconfiguration.

For each abstract process plan, abstract interfaces are mapped to matching real interfaces. An abstract process plan has a set of skills and variables that must exist on an abstract interface, the system uses these abstract interfaces to find compatible resources that have a matching interface with the same skills and variables demanded in the process plan. The search for compatible interfaces is done through a negotiation process between agents. This is a fundamental technique in agent systems [48]. This negotiation process is performed for each abstract interface in the process plan. The negotiation process will find all possible ways to execute a process plan, i.e., there could be several resources capable of performing the same skill, which implies that each process plan can be achieved with different combinations of resources. When all the possible execution orders of the process plan are determined and all participating resources are known, the third main activity is performed, which is the detection of process plan hazards.

The hazards list associated with the logical configuration is presented to the process planner. Figure 7 is an illustration of the output provided to the process planner in a scenario where a part's goal g is to load it into a machine. This goal

has a process plan $\pi_{g_{loadPart}}$ that includes the skill "*load*". The part demands the skill "*load*" and this demand is received by resources that have compatible interfaces. In this example, there are two resources with compatible interfaces, a gripper tool and a resource agent that represents a human operator. The gripper tool possesses the skill "*load*" that has a process plan $\pi_{load} = [pick, moveTool, place]$.

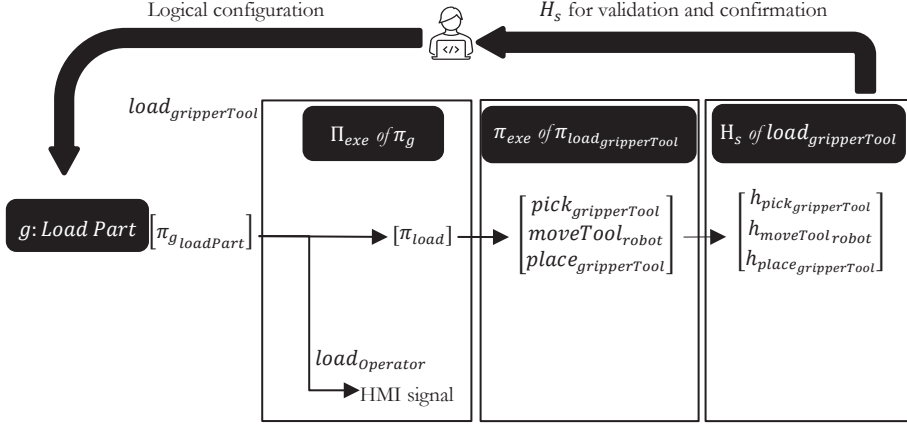


Figure 7 Illustration of the visualisation of a hazard list. The process planner inputs the system's logical configuration and receives the automatically generated hazard list H_s .

The C-MAS Plug & Produce can execute the process plan $\pi_{g_{loadPart}}$ in two ways. The first one is using the skill "*load*" of the gripper which implies that other skills of other resources will be used as well i.e., a robot for the skill "*moveTool*". This skill has hazards, and those hazards must be added to the total hazards of the plan. The other way for the system to execute the plan is by using the operator's skills. The skill "*load*" of the operator, if it is executed as intended, does not generate any hazard that harms other resources. Hazards that may be generated from a faulty execution of a skill will be handled by emergency stops controlled by the safety PLC. Handling these types of hazards is not a safety issue in Plug & Produce as they can be reduced by traditional safety methods. Thus, these hazards are not included in the scope of this thesis and the operator's skill is modelled without hazards.

The process planner receives a list of all hazards associated with all possible executions of the plans to achieve the goals. The process planner may use this information to implement some safety measures.

4.3 Automatic risk assessment and deployment of safety-aware control actions

At runtime, the part performs an automatic risk assessment to identify risk situations to make safety-aware decisions. To achieve its goals and support its safety-aware decision-making, the part agent is equipped with an algorithm that is thoroughly described in paper C. The algorithm can be summarized with the following steps:

Loop 1: For each goal g_p in the ordered set of goals G_p for part p :

Step 1: Retrieve all possible executable process plans for the selected goal g_p through the function *getAllExecutableProcessPlans*(g_p). These plans are stored in the set Π_g^{alt} .

Step 2: Choose the plan with the least production cost among the alternatives using the function *selectPlanWithLeastCost*(Π_g^{alt}). The selected plan is denoted as $\pi_{selected}$.

Loop 2: For each skill s in the selected plan $\pi_{selected}$:

Step 3: Conduct a risk assessment for the skill s using the function *riskAssessment*(skill: s). This assessment identifies pairs of interfaces and skills (IF^τ and S^τ) that are targeted by the hazards associated with the skill.

Step 4: Book the skill s and the targeted skills S^τ on the identified interfaces IF^τ in a specific state st using the function *book*(skill: s , interfaces: IF^τ , skills: S^τ , state: st)

The functions used in the algorithm are described as the following:

getAllExecutableProcessPlans(): This function generates all possible combinations of resources that can be involved in the execution of a specific goal g_p for a given part p . The result is a set Π_g^{alt} containing alternative executable process plans.

selectPlanWithLeastCost(): This function identifies and returns the executable process plan with the minimum production cost from the set of alternatives Π_g^{alt} .

riskAssessment(): Given a specific skill s , this function performs a risk assessment to identify potential hazards associated with the skill. The result

includes pairs of interfaces and skills IF^τ and S^τ that are targeted by these hazards.

book(): This function is responsible for booking a skill s along with the targeted skills S^τ on the identified interfaces IF^τ at a specific state st . It ensures that the booked skills are not available for allocation to other tasks at the same state, preventing conflicts and enhancing resource efficiency.

Figure 8 illustrates the logic of the algorithm for discovering a risk scenario. It is demonstrated using a process plan π_{load} for the skill “load” on a gripper tool. the process plan includes three skills, “pick”, “moveTool”, and “place”. For simplicity, the skill “moveTool” is chosen to further describe the part strategy.

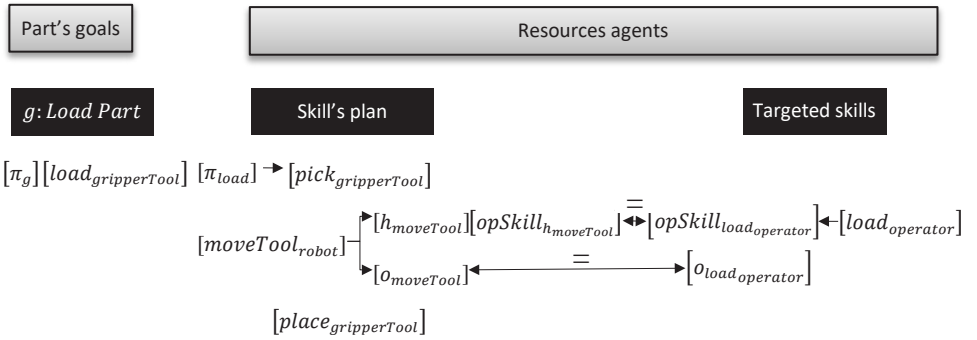


Figure 8 The discovery of a risk scenario that includes a robot and an operator. The equal sign (=) means that the value of the variables is the same.

The skill “moveTool” that is achieved by a robot has a hazard $h_{moveTool}$ which is a high-risk hazard if it occurs. In addition, $h_{moveTool}$ is harmful to the operator. Based on that the hazard of the skill “moveTool” is configured as $h_{moveTool} = \langle high_{h_{moveTool}}, opSkill_{h_{moveTool}} \rangle$. To discover the risk scenario, the part’s algorithm instructs to check the risk level of the hazard, and in this case, it finds it is a high-risk hazard. Then, the algorithm checks if there is any other skill in the system that overlaps with the operational space of skill “moveTool”. Assuming the system is designed in a way that the operator’s skill “load” has operational space that overlaps with the skill “moveTool” of the robot. In this case, the part strategy instructs to check if the skill “moveTool” harms the operator while performing the skill “load”. The part finds that the skill “load” that is owned by the operator resource and has the type “opSkill” is targeted by the skill “moveTool” that is owned by the robot. Based on this information, the part books both skills “load” and “moveTool”. This means that the part not only uses the robot to achieve its plan but also prevents the operator from being

demand, by another plan execution, to perform the skill load. Note, that the operator is only prevented from doing a load and remains unrestricted in executing other skills.

5 Validation of results

This chapter outlines the approach to validate the proposed solution. Model checking is employed to achieve formal verification of the control algorithm. An ideal choice for representing the algorithm's control flow is a finite state machine. A Plug & Produce manufacturing scenario is introduced with different part types, goals, and resources.

5.1 Plug & Produce manufacturing scenario

The manufacturing scenario includes a part type p with three goals: preparation g_1 , loading into a machine g_2 , and machining g_3 . For simplicity, each goal has one process plan, and each plan includes one skill. The scenario includes four resources: two machines, one robot, and one operator. Each resource has one interface, and each interface has one skill. The robot interface has the “*load*” skill that loads the part into a machine, and each machine interface has the “*machineSkill*” skill that processes the part, and the operator agent interface has the “*prepare*” skill. To simplify, if each interface has one skill, the entire resource is considered as booked when that skill is booked for a part. The operational spaces of these skills overlap, and to count for unplanned operator actions, the operational spaces are monitored by safety sensors. In case the operator, in an unplanned manner, enters another resource’s space, the safety PLC enforces a safety stop. The abstract layout of the manufacturing cell is shown in Figure 9 where the resources are represented by black boxes and their respective physical spaces are in dotted and slashed areas.

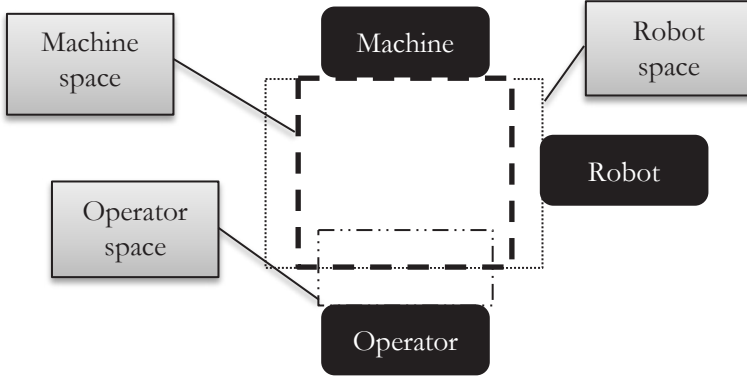


Figure 9 The abstract layout of the validation manufacturing cell. The resources are represented by black boxes and their respective physical spaces are in dotted and slashed areas.

Two configurations exist, each with a different machine. In Configuration 1, the robot and the first machine skill pose high risks to the operator, while Configuration 2 replaces the first machine with a low-risk second machine.

A part p is modelled by an extended finite-state machine EFSM [49]. An EFSM is an ordinary finite state machine, also called an automaton, where a set of variables V is also included. The total discrete state space of an EFSM is the combination of the locations (the states in an ordinary FSM) and the values of the involved variables. There are three variables controlled by the control algorithm, which are involved in location transition. The variables are $V_p \in \{R, Op, M\}$ and their transition in the next location is denoted with prime notation such in $V'_p \in \{R', Op', M\}$. Where R , Op and M are the variables representing a robot, an operator and a machine, in a specific configuration. The domain of each variable is $\{A, B\}$ where A means that the resource is available and B that it is booked.

Figure 10 shows the EFSM of part p in Configuration 1 in which the first machine is used. In this model, the locations q_1 , q_2 , and q_3 correspond to the goals and location q_4 corresponds to the final state in which the product has been produced. Location q_0 is the initial location and the conditional transition from q_0 to q_1 change the value of variable Op . The value of Op in the next location is represented with the variable $Op' = B$. This change in value of Op is due to operator skill "*prepare*" is used to achieve the plan of the first goal g_1 . The operator is made unavailable (booked) for goals g_2 and g_3 to not be able to interact with the hazardous skills of the robot and the machine. The model shows four conditional transitions and the final one is to the marked location q_4 at which

the event “*mc*” represents the completion of the skill “*machineSkill*”. This skill is performed by the first machine resource that is included in the plan of the third goal g_3 .

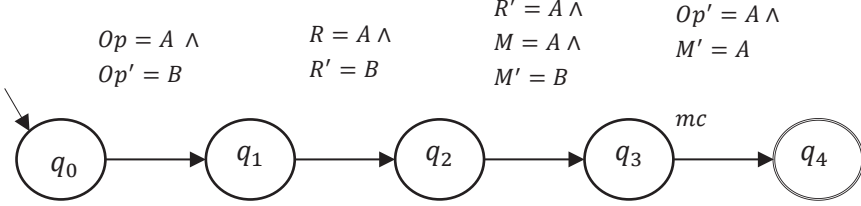


Figure 10 EFSM for a part p in Configuration 1.

Figure 11 shows the EFSM, of a part p in Configuration 2, in which the second machine is used. In this EFSM, it is shown that the operator skill “*prepare*” is available at location q_3 , $Op' = A$ and this is because the “*machineSkill*”, contrary to the first configuration, is not hazardous to the operator and the operator can interact with the machine. The event “*mc*” represents that the second machine has completed “*machineSkill*” and the part life cycle is completed.

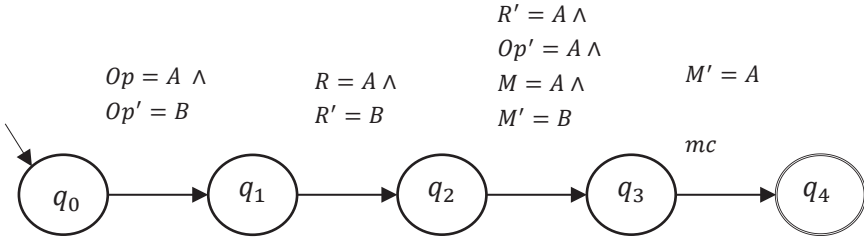


Figure 11 EFSM for a part p in Configuration 2.

5.2 Test results and discussion

The EFSM models were built using the formal model-checking software NuSMV [50] and the results were obtained from the simulation of the composition of two state machines of two parts, namely part i and part j .

In Configuration 1, which involves an unsafe machine, the reachability graph in Figure 12 illustrates that only safe states are reachable, with no instances of

reaching unsafe locations. An example of an unsafe location is the location q_{i1}, q_{j3} . This location is unsafe as it represents a state in which the skills “*prepare*” and “*machineSkill*” are concurrent. The scheduling of parts ensures a sequential production process, aligning with the imposed restrictions on concurrent activities.

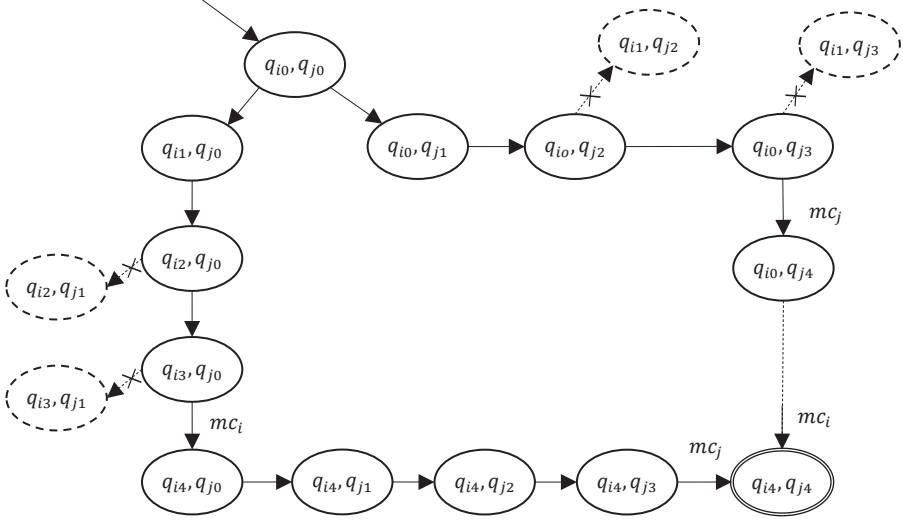


Figure 12 Reachability graph for two parts composition applying Configuration 1. The dashed states are unsafe states. mc is the event of “*machineSkill*” is completed and q_{i4}, q_{j4} is the final location where the production of parts is completed.

In Configuration 2, which involves a safer machine, the reachability graph in Figure 13 shows that safe states are scheduled, but with a higher number of reachable states compared to Configuration 1. As an example, the location q_{i1}, q_{j3} in this configuration is safe due to the safe skill “*machineSkill*”. Concurrent scheduling of skills is enabled in Configuration 2.

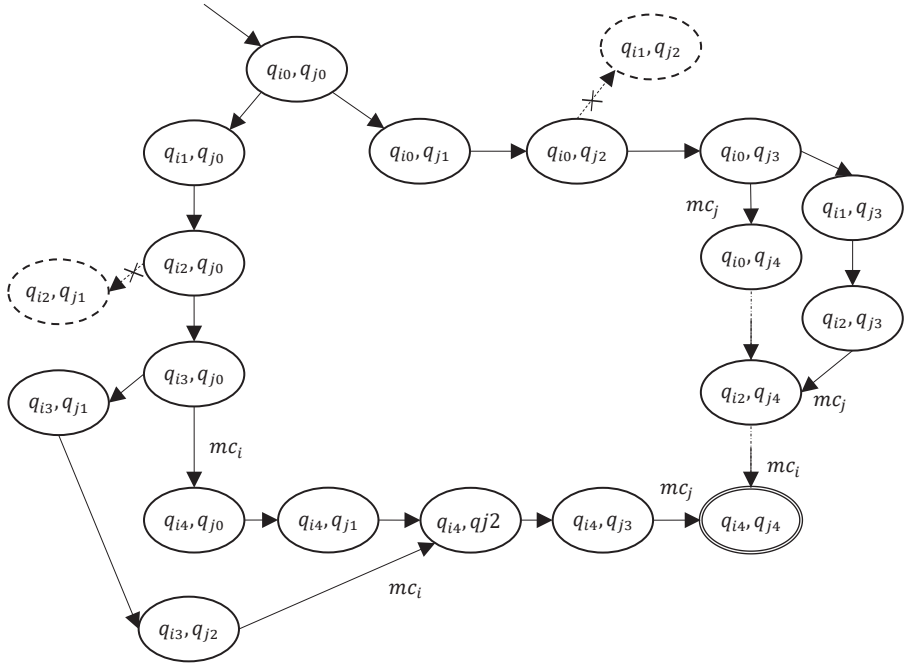


Figure 13 Reachability graph for composition of two parts applying Configuration 2. The dashed states are unsafe states. *mc* is the event of “*machineSkill*” is completed and q_{i4}, q_{j4} is the final location where the production of parts is completed.

In Configuration 1 risk avoidance is achieved by only scheduling the safe states including 16 reachable states. In Configuration 2, the safe states include 20 reachable states within the global state space. This is understandable as more restrictions are implemented by the controller in Configuration 1 due to the presence of more risks. In Configuration 2, as it is safe for the operator to work concurrently with the machine, a part plan may be scheduled to be parallel to another part.

6 Conclusion

In this thesis and the related papers, a hazard identification method aligned with safety standards has been introduced emphasizing skill-based hazard identification. The results showed the feasibility of modelling hazard information and potentially automating the proposed method. The automatic hazard identification method showed applicability after a logical reconfiguration of Plug & Produce. The method integrates hazard information into resource skills during the resource's logical configuration. The method employs an algorithm to identify hazards in all possible plan executions and shows a successful automatic generation of hazard lists.

Also, the thesis and the related papers introduce a C-MAS architecture represented by a UML class diagram for Plug & Produce ontology. This architecture models hazards on resource skills and additional safety information. The modelling of safety information is used to automatically identify risk scenarios. A development to the part agent strategy in the C-MAS controller is an algorithm to make safety-aware decisions autonomously. The control strategy is validated through a formal verification method. The results show the controller's ability to automatically avoid risk situations. The advantage is eliminating manual modifications to the safety controller when logical reconfiguration occurs. The presented approach emphasises proactive runtime safety-aware planning, and reduces reliance on physical barriers and emergency stops, thereby mitigating risks associated with agent autonomy.

6.1 Answers to the research questions

RQ1. How can a generic hazard identification method that identifies emerging hazards and supports safety-aware planning and validation for a Plug & Produce system be formulated?

This thesis formulates a hazard identification method as an answer to RQ1 according to the following conclusive steps: I, obtain the safety knowledge of resources by conducting a hazard analysis achieved by the resource's suppliers; II, construct a domain ontology facilitating the reuse of safety knowledge across a variety of applications; III, configure resources with hazard knowledge that is seamlessly integrated into the model, either by the process planner or the resource supplier; IV, enable automatic detection of emergent hazards within the plans for each logical configuration using a developed algorithm. The outcomes of this

method provide the process planner with safety awareness to validate their plans. Furthermore, these results are a starting point for a system controller with safe awareness, thereby contributing to addressing RQ2. The developed method demonstrates its adaptability for automation across various applications, which is a contribution to the field.

RQ2. How can a Plug & Produce system control strategy automatically perform risk assessment and satisfy control requirements for safety?

This thesis describes an approach to formulate a control strategy to answer RQ2. This control strategy includes the following steps. I, integration of the generic risk assessment method into the control logic of a Plug & Produce system. Given the part-oriented control structure of Plug & Produce, each part agent performs an automatic risk assessment, thereby enabling the discovery of risks associated with the execution of its plans. II, Subsequently, the identified risks are addressed, ensuring that each part executes its plans while averting all potential safety concerns. This new control strategy aligns with the primary objective of providing support for planning processes and reduces the safety responsibilities placed on the process planner. Moreover, it accomplishes the objective of ensuring reliable control within the Plug & Produce environment.

6.2 Recommendations for future research

Several recommendations are proposed for future work. These recommendations are the following.

Industrial testbed and laboratory implementation

The laboratory implementation will allow to evaluate the effectiveness of the proposed Plug & Produce control strategy and the feedback from a real-world scenario. This permits the discovery of further research to achieve industrial acceptance and in a longer perspective industrial implementation.

Design of complete Plug & Produce system lifecycle

In this thesis, the starting point towards Plug & Produce safety lifecycle was established. It included the roles of different stakeholders and the activities in different phases. It is required to integrate the safety lifecycle with the system lifecycle to identify the roles and activities. This will establish a framework to adapt Plug & Produce to the organization's production system.

Usability test of the user interface

In this thesis, a safety validation tool was proposed. The validation is a user interface that requires further investigation for its usability in real-world manufacturing. Usability testing is a method used to evaluate a software product by testing it with actual users to determine how user-friendly and effective it is. The goal of usability testing is to identify any usability issues, gather feedback on the user experience, and make improvements to enhance the overall usability of the software.

Investigate if STPA can be used for Plug & Produce

Systems-Theoretic Process Analysis, STPA, is a hazard analysis technique that is based on system theory that identifies the unsafe control actions and analyses the control structure of a system to identify the hazards. The STPA is commonly used in aerospace, automotive or healthcare systems. This thesis has presented an approach that focuses on identifying hazards of the control system and investigating STPA can lead to improvement to the proposed solution.

Human-robot collaboration based on large language models that understand the ontology

Human-robot collaboration has been widely studied in recent years and the safety analysis of these systems has been standardised in the ISO/TS 15066:2016. The new advances in this field include large language models that enhance human-robot collaboration. It allows the robot system to understand natural languages permitting novel ways of combined human-robot decision making. It is interesting to investigate the safety issues related to integrating such kind of decision making into the control structure of Plug & Produce.

Define an ontology that goes beyond a simple 3d definition

The hazard and risk identification in the proposed solution mostly focuses on the temporal aspect of the control flow. The spatial considerations were simplified by a simple 3d definition of the skills workspace. There is a need to further research the definitions of the workspaces and their representations in the ontology. This will increase the accuracy of the hazard and risk identification.

7 Summary of appended papers

Paper A presents a method for hazard identification in Plug & Produce systems, which is derived from ISO safety standards and guidelines. This method specifically focuses on addressing emergent hazards that arise after system reconfiguration, which were unforeseen during the initial system design. The paper contributes to answering RQ1 and provides insights into the necessary domain of support that needs to be developed to support safety-aware planning.

Paper B builds upon the knowledge obtained in paper A, using it to establish its objectives. It primarily focuses on presenting a novel approach to automating hazard detection, leveraging the foreseen hazards initially identified on individual resources. Additionally, paper B approaches RQ1, as it advances the method for identifying emerging hazards after logical configuration, incorporating a model-based approach. Additionally, it contributes to answering RQ2 by introducing an algorithm capable of automating the extraction and analysis of safety data and generating a list of hazards based on the Plug & Produce different reconfigurations.

Paper C presents a broader study by extending the learnings of paper B. Paper C expands the scope of knowledge representation initially established in paper B. It contributes to answering RQ2 by presenting a method that leverages C-MAS control of Plug & Produce to execute model-based risk analysis. This approach enables the generation of control actions that guarantee compliance with safety requirements throughout the production process.

7.1 Paper A

A Framework for Hazard Identification of a Collaborative Plug & Produce System

Aim

The paper aims to find a framework for the application of ISO safety standards and guidelines to ensure the safety of Plug & Produce systems.

Description

To achieve the aim, the applied research method includes an analysis of safety standards and relevant literature. ISO standards outline a three-step approach to

achieve safety, hazard identification, risk assessment, and subsequent risk reduction, both at the singular component and system levels.

To deal with the challenges posed by the frequent logical and physical reconfiguration in the Plug & Produce system, the paper proposes a hazard identification method aligned with safety standards. The proposed hazard identification method involves identifying hazards based on the skills of the resources involved. The proposed method also involves determining system reconfigurations, which include both physical and logical aspects.

The paper includes the formation of a case study to understand the applicability of ISO standards within the Plug & Produce context. The proposed method for hazard identification is then applied to this case study, and the results are collected and analysed to enhance the understanding of its effectiveness.

Paper's outcome

A better understanding obtained from the results shows the feasibility of modelling hazard information and highlights the need for automation of the proposed method. The study also leads to the idea of implementing safety measures through logic first and considering generic physical barriers as secondary measures. Furthermore, it leads to a notion of proactive methods to prevent risks, thus reducing reliance on implementing physical barriers.

7.2 Paper B

Online hazard detection in reconfigurable Plug & Produce systems.

Aim

The paper aims to propose an automatic method for hazard identification, of a system configuration, to support the planning within Plug & Produce.

Description

Paper B presents a method for hazard identification of Plug & Produce systems and validation of plans. It provides the hazard list of all possible executable alternatives of the abstract plans automatically. The presented method in the paper is divided into two phases, the configuration phase, and the validation phase. The former includes the activities of configuring the plans which are made by the process planner. The activity of configuring the plans resembles the production design in traditional manufacturing. These plans are abstract plans that don't specify what resources will participate, they only specify the skills

needed. The validation phase includes the conversion of the abstract plans into executable ones using the available resources.

The proposed method adds to the configuration phase the activity of adding the hazard information to resources' skills. This is based on the identified hazards of individual resources including determining the set of skills that the resource can perform and identifying the hazards associated with each of the resource's skills. Hazards of resources are identified according to ISO standards, for example, machines ISO 12100 and robots ISO 10218. This can be done by the supplier of the resources or can be done internally by the process planner.

When the reconfiguration phase is done. The system figures all possible executions, with different resources, of each plan. For this, the paper presents an algorithm that identifies all the hazards associated with every possible execution of each plan in this configuration. Furthermore, a conceptual software tool was developed to present to the process planner all the discovered hazards. Based on this information the process planner confirms that the hazards are covered by traditional safety measures.

Paper's outcome

Modelling the hazards associated with skills allows for including this safety-related information within the system configuration and allows for the reusability of this information when the skill is demanded in the online execution of a process plan.

A benefit of the proposed solution is that it allows the process planner to be aware of the effect on operational safety due to changes in the control structure i.e., the system plans, which allows for safety-aware planning.

Another benefit is that the system is aware of the set of hazards associated with each logical reconfiguration of the Plug & Produce. This is a point of departure to autonomous decision-making and to choosing the safe execution of the production.

7.3 Paper C

Model-based reasoning and decision-making for safe operation in a Plug & Produce environment.

Aim

Paper C aims to synthesize a control strategy within the multi-agent controller of Plug & Produce that automatically discovers the risk scenarios and autonomously

generates control actions that enable the execution of the plans avoiding the occurrence of risks.

Description

Paper C focuses on the autonomous decision-making in the Plug & Produce system. Autonomous decision-making raises a safety challenge due to control actions that may generate risk situations during the execution of the plans.

This paper presents a C-MAS architecture represented by a UML class diagram for the Plug & Produce ontology. The class diagram includes modelling hazards on skills of resources, in line with the work in paper B. In addition, it models further safety information that enables to identification of a complete risk scenario. This includes the modelling of risk levels of the harm caused by the hazard, the space in which the skill is performed, and the agent that may be harmed by the hazard. The model is used for reasoning in the runtime phase.

During runtime, the safety decision-making is the C-MAS controller's responsibility. In this paper, an algorithm is developed to enable safety decision-making in the controller. The controller runs the algorithm to perform an automatic risk assessment and discover if a certain skill that harms a certain agent is taking place in a location where the agent of interest is performing its skills. The algorithm reasons if that scenario is high risk and if so, the algorithm makes a schedule that prevents this hazardous scenario from happening.

This algorithm was tested with a simulated manufacturing scenario that includes producing more than one part concurrently and the result of the algorithm was validated using a formal verification method.

Paper's outcome

This paper presented an approach that has the advantageous effect of eliminating the need for manually modifying the safety-related part of the control system. The presented approach incorporates an automatic risk assessment with the C-MAS controller, that pre-emptively averts emergency stops rather than reactively responding to them. This significantly reduces the reliance on physical barriers and emergency stop mechanisms. The benefit of this approach is it enables runtime planning of operations, by the controller, effectively mitigating safety concerns associated with agent autonomy.

8 References

- [1] T. Arai, Y. Aiyama, Y. Maeda, M. Sugi, and J. Ota, “Agile Assembly System by ‘Plug and Produce,’” *CIRP Annals*, vol. 49, no. 1, pp. 1–4, 2000, doi: 10.1016/S0007-8506(07)62883-2.
- [2] T. Arai, Y. Aiyama, M. Sugi, and J. Ota, “Holonc assembly system with Plug and Produce,” *Computers in Industry*, vol. 46, no. 3, pp. 289–299, 2001, doi: 10.1016/S0166-3615(01)00111-7.
- [3] R. W. Brennan, M. Fletcher, and D. H. Norrie, “An agent-based approach to reconfiguration of real-time distributed control systems,” *IEEE Transactions on Robotics and Automation*, vol. 18, no. 4, pp. 444–451, 2002, doi: 10.1109/TRA.2002.802211.
- [4] A. Rocha *et al.*, “An agent based framework to support plug and produce,” in *12th IEEE International Conference on Industrial Informatics*, Porto Alegre, Brazil: IEEE, Jul. 2014, pp. 504–510. doi: 10.1109/INDIN.2014.6945565.
- [5] P. Leita, J. Barbosa, A. Pereira, J. Barata, and A. W. Colombo, “Specification of the PERFoRM architecture for the seamless production system reconfiguration,” in *42nd Annual Conference of the IEEE Industrial Electronics Society*, Florence, Italy: IEEE, Oct. 2016, pp. 5729–5734. doi: 10.1109/IECON.2016.7793007.
- [6] T. Arai, H. Izawa, Y. Maeda, H. Kikuchi, H. Ogawa, and M. Sugi, “Real-time task decomposition and allocation for a multi-agent robotic assembly cell,” in *Proceedings of the IEEE International Symposium on Assembly and Task Planning, 2003.*, 2003, pp. 42–47. doi: 10.1109/ISATP.2003.1217185.
- [7] M. Onori, N. Lohse, J. Barata, and C. Hanisch, “The IDEAS project: Plug & produce at shop-floor level,” *Assembly Automation*, vol. 32, no. 2, pp. 124–134, 2012, doi: 10.1108/01445151211212280.
- [8] M. Bennulf, “A Control Framework for Industrial Plug & Produce,” Ph.D. dissertation, University West, Sweden, 2023.
- [9] A. Nilsson, F. Danielsson, M. Bennulf, and B. Svensson, “A Classification of Different Levels of Flexibility in an Automated Manufacturing System and Needed Competence BT - Towards Sustainable Customization: Bridging Smart Products and Manufacturing Systems,” A.-L. Andersen, R. Andersen, T. D. Brunoe, M. S. S. Larsen, K. Nielsen, A. Napoleone,

and S. Kjeldgaard, Eds., Cham: Springer International Publishing, 2022, pp. 27–34.

- [10] A. Klose *et al.*, “Building Blocks for Flexible Functional Safety in Discrete Manufacturing and Process Industries,” *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, vol. 2021-Sept, 2021, doi: 10.1109/ETFA45728.2021.9613608.
- [11] C. A. Ericson, *Hazard Analysis Techniques for System Safety*. Wiley, 2005. doi: 10.1002/0471739421.
- [12] S. Gradel, B. Aigner, and E. Stumpf, “Model-based safety assessment for conceptual aircraft systems design,” *CEAS Aeronautical Journal*, vol. 13, no. 1, pp. 281–294, 2022, doi: 10.1007/s13272-021-00562-2.
- [13] C. H. Koo, S. Schröck, M. Vorderer, J. Richter, and A. Verl, “A model-based and software-assisted safety assessment concept for reconfigurable PnP-systems,” *Procedia CIRP*, vol. 93, pp. 359–364, 2020, doi: 10.1016/j.procir.2020.03.076.
- [14] A. Joshi, M. P. E. Heimdahl, S. P. Miller, and M. W. Whalen, “Model-based safety analysis,” 2006.
- [15] A. Baklouti, N. Nguyen, F. Mhenni, J.-Y. Choley, and A. Mlika, “Dynamic Fault Tree Generation for Safety-Critical Systems Within a Systems Engineering Approach,” *IEEE Systems Journal*, vol. 14, no. 1, pp. 1512–1522, 2020, doi: 10.1109/JSYST.2019.2930184.
- [16] O. Lisagor, T. Kelly, and R. Niu, “Model-based safety assessment: Review of the discipline and its challenges,” in *ICRMS'2011 - Safety First, Reliability Primary: Proceedings of 2011 9th International Conference on Reliability, Maintainability and Safety*, IEEE, 2011, pp. 625–632. doi: 10.1109/ICRMS.2011.5979344.
- [17] Y. Koren, X. Gu, and W. Guo, “Reconfigurable manufacturing systems: Principles, design, and future trends,” *Frontiers of Mechanical Engineering*, vol. 13, no. 2, pp. 121–136, 2018, doi: 10.1007/s11465-018-0483-0.
- [18] A. Hanna, “Risk Assessment and Safety Measures for Intelligent and Collaborative Automation.” Ph.D. dissertation, Mälardalen University, Sweden, 2023.
- [19] K. Säfsten and M. Gustavsson, *Research Methodology For Engineers and Other Problem-Solvers*. Studentlitteratur AB, 2020.
- [20] L. Svensson, P.-E. Ellström, and G. Brulin, “Introduction—on interactive

- research,” *International journal of action research*, vol. 3, no. 3, pp. 233–249, 2007.
- [21] H. Altrichter, S. Kemmis, R. McTaggart, and O. Zuber-Skerritt, “The concept of action research,” *The Learning Organization*, vol. 9, no. 3, pp. 125–131, Jan. 2002, doi: 10.1108/09696470210428840.
 - [22] J. E. Van Aken, “Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules,” *Journal of Management Studies*, vol. 41, no. 2, pp. 219–246, 2004, doi: 10.1111/j.1467-6486.2004.00430.x.
 - [23] A. Chakrabarti and L. T. M. M. Blessing, *DRM: A Design Research Methodology*. Springer London, 2009.
 - [24] J. Woodcock, P. G. Larsen, J. Bicarregui, and J. Fitzgerald, “Formal Methods: Practice and Experience,” *ACM Computing Surveys*, vol. 41, no. 4, pp. 1–40, 2009.
 - [25] M. Bortolini, L. Botti, F. G. Galizia, and C. Mora, “Safety, Ergonomics and Human Factors in Reconfigurable Manufacturing Systems,” no. 2019, pp. 123–138, 2020, doi: 10.1007/978-3-030-28782-5_6.
 - [26] C. Digmayer and E.-M. Jakobs, “Developing Safety Cultures for Industry 4.0. New Challenges for Professional Communication,” in *2019 IEEE International Professional Communication Conference (ProComm)*, 2019, pp. 218–225. doi: 10.1109/ProComm.2019.00045.
 - [27] O. Jaradat, I. Sljivo, I. Habli, and R. Hawkins, “Challenges of Safety Assurance for Industry 4.0,” *Proceedings - 2017 13th European Dependable Computing Conference, EDCC 2017*, pp. 103–106, 2017, doi: 10.1109/EDCC.2017.21.
 - [28] D. Etz, P. Denzler, T. Fruhwirth, and W. Kastner, “Functional Safety Use Cases in the Context of Reconfigurable Manufacturing Systems,” *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, vol. 2022-Septe, 2022, doi: 10.1109/ETFA52439.2022.9921448.
 - [29] D. Hillen *et al.*, “Plug-and-Produce... Safely! BT - Model-Based Safety and Assessment,” in *Model-Based Safety and Assessment. International Symposium on Model-Based Safety and Assessment 2022. LNCS, vol 13525.*, C. Seguin, M. Zeller, and T. Prosvirnova, Eds., Cham: Springer International Publishing, 2022, pp. 83–97.
 - [30] Y. Lu, Q. Li, Z. Zhou, and Y. Deng, “Ontology-based knowledge modeling for automated construction safety checking,” *Safety Science*, vol.

79, pp. 11–18, Nov. 2015, doi: 10.1016/J.SSCI.2015.05.008.

- [31] S. Sonfack Souchio, B. Kamsu-Foguem, and L. Geneste, “Construction of a base ontology to represent accident expertise knowledge,” *Cognition, Technology & Work*, 2023, doi: 10.1007/s10111-023-00724-8.
- [32] J. I. Single, J. Schmidt, and J. Denecke, “Ontology-based computer aid for the automation of HAZOP studies,” *Journal of Loss Prevention in the Process Industries*, vol. 68, 2020, doi: 10.1016/j.jlp.2020.104321.
- [33] S. Mao, Y. Zhao, J. Chen, B. Wang, and Y. Tang, “Development of process safety knowledge graph: A Case study on delayed coking process,” *Computers and Chemical Engineering*, vol. 143, 2020, doi: 10.1016/j.compchemeng.2020.107094.
- [34] B. Zhong and Y. Li, “An Ontological and Semantic Approach for the Construction Risk Inferring and Application,” *Journal of Intelligent and Robotic Systems: Theory and Applications*, vol. 79, no. 3–4, pp. 449–463, 2015, doi: 10.1007/s10846-014-0107-9.
- [35] C. Wu, Q. Ouyang, S. Yu, C. Deng, X. Mao, and T. Hong, “The development and application of the ontology for tractor fault diagnosis,” *International Journal of Computational Science and Engineering*, vol. 15, no. 1–2, pp. 112–122, 2017, doi: 10.1504/IJCSE.2017.086010.
- [36] J. Siegert *et al.*, “Model-based Approach for the Automation and Acceleration of the CE-Conformity Process for Modular Production Systems: Future Requirements and Potentials,” in *Proceedings of the Conference on Production Systems and Logistics*, 2021, pp. 177–190. doi: 10.15488/11273.
- [37] M. Webster *et al.*, “Toward Reliable Autonomous Robotic Assistants Through Formal Verification: A Case Study,” *IEEE Transactions on Human-Machine Systems*, vol. 46, no. 2, pp. 186–196, 2016, doi: 10.1109/THMS.2015.2425139.
- [38] T. Koch, “Approach for an automated safety configuration for robot applications,” *Procedia CIRP*, vol. 84, no. March, pp. 896–901, 2019, doi: 10.1016/j.procir.2019.04.280.
- [39] M. Askarpour, L. Lestingi, S. Longoni, N. Iannacci, M. Rossi, and F. Vicentini, “Formally-based Model-Driven Development of Collaborative Robotic Applications,” *Journal of Intelligent & Robotic Systems*, vol. 102, no. 3, p. 59, 2021, doi: 10.1007/s10846-021-01386-2.
- [40] N. W. Chi, K. Y. Lin, and S. H. Hsieh, “Using ontology-based text

classification to assist Job Hazard Analysis,” *Advanced Engineering Informatics*, vol. 28, no. 4, pp. 381–394, Oct. 2014, doi: 10.1016/J.AEI.2014.05.001.

- [41] G. Bakirtzis, T. Sherburne, S. Adams, B. M. Horowitz, P. A. Beling, and C. H. Fleming, “An ontological metamodel for cyber-physical system safety, security, and resilience coengineering,” *Software and Systems Modeling*, vol. 21, no. 1, pp. 113–137, 2022, doi: 10.1007/s10270-021-00892-z.
- [42] A. Aziz, S. Ahmed, and F. I. Khan, “An ontology-based methodology for hazard identification and causation analysis,” *Process Safety and Environmental Protection*, vol. 123, pp. 87–98, 2019, doi: 10.1016/j.psep.2018.12.008.
- [43] V. Ebrahimipour, K. Rezaie, and S. Shokravi, “An ontology approach to support FMEA studies,” *Expert Systems with Applications*, vol. 37, no. 1, pp. 671–677, 2010, doi: 10.1016/j.eswa.2009.06.033.
- [44] D. P. Pereira, C. Hirata, and S. Nadjm-Tehrani, “A STAMP-based ontology approach to support safety and security analyses,” *Journal of Information Security and Applications*, vol. 47, pp. 302–319, 2019, doi: 10.1016/j.jisa.2019.05.014.
- [45] A. Carniel, J. D. M. Bezerra, and C. M. Hirata, “An Ontology-Based Approach to Aid STPA Analysis,” *IEEE Access*, vol. 11, pp. 12676–12696, 2023, doi: 10.1109/ACCESS.2023.3242642.
- [46] R. Awad, M. Fechter, and J. Van Heerden, “Integrated risk assessment and safety consideration during design of HRC workplaces,” *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, pp. 1–10, 2017, doi: 10.1109/ETFA.2017.8247648.
- [47] A. Nilsson, F. Danielsson, and B. Svensson, “Customization and flexible manufacturing capacity using a graphical method applied on a configurable multi-agent system,” *Robotics and Computer-Integrated Manufacturing*, vol. 79, no. July 2022, p. 102450, 2023, doi: 10.1016/j.rcim.2022.102450.
- [48] I. Kovalenko, E. C. Balta, D. M. Tilbury, and K. Barton, “Cooperative Product Agents to Improve Manufacturing System Flexibility: A Model-Based Decision Framework,” *IEEE Transactions on Automation Science and Engineering*, vol. 20, no. 1, pp. 440–457, 2023, doi: 10.1109/TASE.2022.3156384.
- [49] S. Mohajerani, R. Malik, and M. Fabian, “A framework for compositional nonblocking verification of extended finite-state machines,” *Discrete Event*

Dynamic Systems: Theory and Applications, vol. 26, no. 1, pp. 33–84, 2016, doi: 10.1007/s10626-015-0217-y.

- [50] A. Cimatti *et al.*, “NuSMV 2: An opensource tool for symbolic model checking,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2404, pp. 359–364, 2002, doi: 10.1007/3-540-45657-0_29.

Planning and Control of Safety-Aware Plug & Produce

The Plug & Produce manufacturing system is a visionary concept that promises to facilitate the seamless integration and adaptation of manufacturing resources and production processes. The Plug & Produce control system allows for the automatic addition and removal of manufacturing resources, minimizing human intervention. However, the reconfigurability and autonomous decision-making features of Plug & Produce control systems pose challenges to safety design and control functions.

In contrast to conventional manufacturing systems with fixed layouts and processes, ensuring safety in Plug & Produce systems is complicated due to the complex risk assessment process, the difficulty of implementing non-restrictive safety measures covering all possible hazards, and the challenge of designing a reliable controller for consistent safe operation.

This thesis addresses these challenges through various contributions. It introduces an automatic hazard identification method, considering emergent hazards after reconfiguration. A novel domain ontology is developed, incorporating safety models specific to Plug & Produce systems. The work also proposes a generic, model-based, and automatic risk assessment method, along with a method for the safe execution of plans based on the results of the risk assessment.

The results of this research offer benefits to process planners, who are responsible for coordinating the manufacturing processes with product design in the Plug & Produce system. The proposed solution provides tools for process planners to validate their plans and reduces their safety-related responsibilities. The proposed safety assurance method seamlessly integrates into the multi-agent control of Plug & Produce, providing the control system with risk scenarios associated with process plans. This enables proactive and reliable control, effectively avoiding potential risks during system operation.



Bassam Massouh

Received a B.Sc. degree in control and automation from Damascus University, in 2015 and an M.Sc. degree in robotics and automation from University West, Sweden in 2019. He joined the production technology research group at University West in 2020 and his research includes Plug & Produce manufacturing, multi-agent systems, industrial safety, robotics and automation.

ISBN 978-91-89325-66-1 (printed)

ISBN 978-91-89325-65-4 (pdf)