

# Multi-view-Model Risk Assessment in Cyber-Physical Production Systems Engineering

Stefan Biffel<sup>1</sup>, Arndt Lüder<sup>3</sup>, Kristof Meixner<sup>2</sup>, Felix Rinker<sup>2</sup>,  
Matthias Eckhart<sup>2</sup> and Dietmar Winkler<sup>2</sup>

<sup>1</sup>Institute of Information Systems, TU Wien, Vienna, Austria

<sup>2</sup>CDL for Security & Quality Improvement in the Production System Lifecycle, TU Wien, Vienna, Austria

<sup>3</sup>Institute of Ergonomics, Manufacturing Systems and Automation, Otto-von-Guericke University, Magdeburg, Germany

**Keywords:** Model-based Risk Assessment, Multi-view Modeling in Systems Engineering, Cyber Physical Systems.

**Abstract:** The engineering of complex, flexible production systems, *Cyber Physical Production Systems* (CPPSs), requires integrating models across engineering disciplines. A *CPPS Engineering Network* (CEN), an integrated multi-domain multi-view model, facilitates the assessment of risks to CPPS and product designs, i.e., risks stemming from several engineering disciplines. However, traditional risk assessment, e.g., *Failure Mode and Effect Analysis* (FMEA), provides informal cause-effect hypotheses, which may be hard to test without interdisciplinary links through the CEN to CPPS data sources. This paper aims to improve the effectiveness of model-based cause identification and validation for risks to CPPS functions that come from modeling in several CPPS disciplines by introducing the *CPPS Risk Assessment* (CPPS-RA) approach for representing FMEA cause-effect hypotheses and linking them to a CEN. These links provide the basis to specify CPPS engineering and operational data required for hypothesis testing. We evaluate the CPPS-RA approach in a feasibility study on a representative use case from discrete manufacturing. In the study context, domain experts found the CPPS-RA meta-model sufficiently expressive and the CPPS-RA method useful to validate FMEA results.

## 1 INTRODUCTION

Industry 4.0 demands digitized industrial production calling for *Cyber-Physical Production Systems* (CPPSs). CPPSs use modern manufacturing methods and latest information technology to adapt to different conditions and interact with their environment. These CPPSs have to fulfill requirements regarding product quality, functional safety, and information security (Henning, 2013). CPPS engineering involves several engineering disciplines, such as mechanical, electrical, and software engineering, which design and use heterogeneous models and tools. Risk management in CPPS engineering, such as the *Failure Mode and Effects Analysis* (FMEA) approach (DIN60812, 2015), is well supported in single engineering disciplines,

but challenging to conduct across disciplines and may miss cross-discipline impacts when using discipline-specific, isolated models.

CPPS quality managers want to effectively and efficiently identify factors potentially leading to specific quality risks. However, knowledge on causes and impact relationships may come from different disciplines with their views on the system (Meier et al., 2019). Traditionally, quality managers do not use multi-view models for conducting risk assessments, making the results hard to validate, use in advanced analyses, replicate, and improve.

Identifying and assessing causes for risky effects is hard as (a) product failure modes may depend on several CPPS engineering disciplines, and (b) the heterogeneous models, data, and tools used are hard to integrate. These issues require an approach for multi-view modeling (Atkinson et al., 2015) that considers risks and their causes in *CPPS Engineering Networks* (CENs), i.e., integrated multi-domain multi-view models. Model-based risk assessment that relies on single-discipline models (Liu et al., 2013) does not link hypotheses to multi-disciplinary CPPS engi-

<sup>a</sup> <https://orcid.org/0000-0002-3413-7780>

<sup>b</sup> <https://orcid.org/0000-0001-6537-9742>

<sup>c</sup> <https://orcid.org/0000-0001-7286-1393>

<sup>d</sup> <https://orcid.org/0000-0002-6409-8639>

<sup>e</sup> <https://orcid.org/0000-0001-5125-4391>

<sup>f</sup> <https://orcid.org/0000-0002-4743-3124>

neering models and data. Data collection and analysis without hypotheses on cause-effect relationships often yield invalid cause-effect correlations and costly, but ineffective, changes to product and CPPS designs.

This paper focuses on functional risks represented in and possibly resulting from modeling in several CPPS disciplines, omitting information security risks that assume intentional wrongdoing. We elicited requirements for risk assessment (cf. Section 3) with CPPS engineers and introduce the use case *Screwing System* to illustrate challenges and core concepts. We investigate multi-view modeling for CPPS Risk Assessment to provide the basis for defining and analyzing cause-effect relationships, in particular causes of risks to assets, across disciplines. In particular, we investigate (1) what data elements are required to represent cause-effect relationships in a CEN and (2) how domain experts explore a CEN to identify and assess possible cause-effect relationships.

We introduce the *CPPS Risk Assessment (CPPS-RA)* approach to elicit candidates for cause-effect hypotheses, in the multi-disciplinary CPPS engineering context. To this end, we introduce the *CPPS-RA meta-model* with core concepts for integrated multi-disciplinary engineering views for Risk Assessment and the *CPPS-RA method* to explore potential causes for risks in a multi-view graph. We describe the conceptual, technical design of prototype tool support for the CPPS-RA method, integrating engineering data based on *AutomationML (AML)* (IEC 62714, 2018). We evaluate the CPPS-RA approach in a feasibility study with the use case *Screwing System* from car manufacturing that is representative for discrete manufacturing processes and assets. For an extended report and further details, refer to (Biffel et al., 2020).

The remainder of the paper is structured as follows: Section 2 summarizes related work on multi-view modeling and risk assessment CPPS engineering. Section 3 introduces the research questions and approach. Section 4 introduces the representative use case *Screwing System* from the real-world CPPS engineering context – car manufacturing. Section 5 describes the CPPS-RA approach, the meta-model, and method steps. Section 6 reports on a feasibility study of the CPPS-RA approach. Section 7 discusses the results of the feasibility study regarding the requirements and the research questions. Section 8 concludes and motivates future work.

## 2 RELATED WORK

This section reports on multi-view modeling and risk management in CPPS engineering.

### 2.1 Multi-view Modeling in CPPS Eng.

CPPS life cycle digitization (Henning, 2013) is a trend to reduce costs and make production more flexible. Engineering process digitization supports this goal by improving process effectiveness and efficiency (Biffel et al., 2017). A major challenge is the exchange of engineering data. As the processes include multiple domains and models, data exchange requires the effective and efficient collection, integration, selection, and transformation of scattered and heterogeneous information.

Multi-view models (Atkinson et al., 2015) foster the collaboration in such multi-disciplinary environments. The engineering domain experts take decisions following their habits and represent the results of these decisions in Domain-Specific Languages. This results in *CPPS Engineering Networks (CENs)*, where Domain-Specific Languages express (discipline-internal) data models related to a single discipline and (discipline-crossing) data models related to several disciplines as a basis for the digitization of engineering data logistics (Lüder et al., 2019).

Risk management in CPPS engineering processes is essential (Foehr, 2013; Hopkin, 2018). While engineers ensure the quality within their discipline, there are limited capabilities for risk representation and evaluation involving several disciplines. The consideration of cross-discipline dependencies is renowned within CPPS engineering but hampered by data collection issues. Winzer *et al.* (Sitte and Winzer, 2010) presented an approach for matrix-based modeling of discipline-internal and discipline-crossing dependencies between system components. Foehr extended the approach with quality management strategies for a multi-model representation of quality dependencies crossing different disciplines like quality management and product & system design (Foehr, 2013).

A precondition for these methods is a sufficiently integrated multi-view system model, which is costly and error-prone to create from implicit knowledge. A multi-view system model over multi-domain elements with domain-specific links (Atkinson et al., 2015) can be represented in AML-based engineering data logistics, enabling common graph search algorithms.

### 2.2 Risk Assessment in CPPS Engineering with FMEA

Risk assessment in CPPS engineering focuses on identifying and analyzing product, process, and resource risks that might lead to defective products caused by inaccurate or defective processes or resources, omitting intentional wrongdoing. Risk as-

assessment builds the basis for the risks mitigation to prevent defects and avoid the recurrence of defects (Hopkin, 2018). In CPPS engineering, the *FMEA* approach is a common approach. It aims at systematically identifying CPPS assets, system elements related to the *System under Inspection (Sul)*, possible *Failure Modes* that may lead to unintended *Effects*, and (root) *Causes* for effects, as basis for risk mitigation (DIN60812, 2015; Stamatis, 2019) (cf. Table 1 for FMEA concepts). For more details on FMEA refer to (Biffel et al., 2020).

Model-based FMEA approaches (Kaiser et al., 2003; Liu et al., 2013) link effects through model connections to cause candidates, but typically for single-discipline models that do not represent risky dependencies across disciplines. For more details on model-based FMEA refer to (Biffel et al., 2020).

To address limitations of FMEA based on single-discipline models, this paper builds on CENs, integrated multi-domain multi-view CPPS engineering models, to represent and analyze cause-effect graphs linking cause candidates to risky effects under investigation, including cross-discipline dependencies.

### 3 RESEARCH QUESTIONS AND APPROACH

In the past, we conducted workshops with senior domain experts from a major CPPS integrator based in Europe, aiming to improve the quality of their CPPS engineering processes. A major concern was resolving issues with ineffective improvement activities. These issues resulted from invalid cause-effect correlations coming from machine learning projects on engineering data, that lacked links between engineering data and cause-effect arguments.

The domain experts provided the following **requirements Rx** for risk assessment.

**R11.** *Representation of FMEA elements* as a basis for reasoning on causes and effect considerations when conducting a FMEA. **R12.** *Representation of the CPPS Engineering Network (CEN)* to facilitate reasoning on connections in an integrated multi-view CPPS engineering model, e.g., an integrated AutomationML model (IEC 62714, 2018), for describing causes and effects across engineering disciplines. **R21.** *Representation of causes and hypotheses* to allow capturing informal causes early during FMEA and facilitate refining them to formal cause representations, linked via a hypothesis to an effect, as a basis for advanced risk analyses. **R22.** *Mapping of causes and effects to elements in the CEN* to root the risk assessment in the CPPS design, as a foundation for

realistic analyses with CPPS data. **R3.** *Representation and assessment of pathway from causes to effects in the CEN*, to validate the FMEA results, comparable to an attack graph in CPPS security.

From these requirements, we derived the following research questions (RQs).

**RQ1. CPPS-RA Meta-model.** *What data elements are required to represent cause-effect relationships in a CPPS Engineering Network (CEN) as a basis for risk assessment across discipline boundaries?* To address RQ1, this paper introduces the *CPPS-RA meta-model* to represent data elements and relationships required for conducting a FMEA with links to a CEN. The design of the meta-model is based on the standards underlying the FMEA method (DIN60812, 2015) and CPPS engineering data representation and exchange (Drath et al., 2008; Sitte and Winzer, 2010). Further, we compared the meta-model design to FMEA applications in CPPS engineering (Höfig et al., 2019) to facilitate a conceptualization consistent with these applications.

**RQ2. CPPS-RA Method.** *How can domain experts explore an integrated CPPS Engineering Network (CEN) to identify and assess possible cause-effect relationships for a failure mode/effect, even across discipline boundaries?* To address RQ2, this paper introduces the *CPPS-RA method* for identifying model elements to elicit and formalize cause-effect hypotheses that guide data selection and analysis. The CPPS-RA method refines the FMEA's cause analysis step by guiding experts to iteratively explore a CEN. It enables selecting effects, identifying assets potentially causing the effect, and building a cause-effect pathway across discipline boundaries in the CEN to substantiate a testable hypothesis. The risk analysis results provide the foundation for risk-based test scenarios and hypothesis-guided data collection and analysis.

For evaluation regarding the requirements Rx, we conducted a feasibility study with use case *Screwing System* from car manufacturing, building on a CEN (Biffel et al., 2019; Lüder et al., 2019). CPPS domain experts among this paper's authors conducted the CPPS-RA method. They discussed the results with senior domain experts from car manufacturing to compare the characteristics of CPPS-RA with those of their traditional method for risk assessment to analyze the strengths and limitations of the CPPS-RA approach.

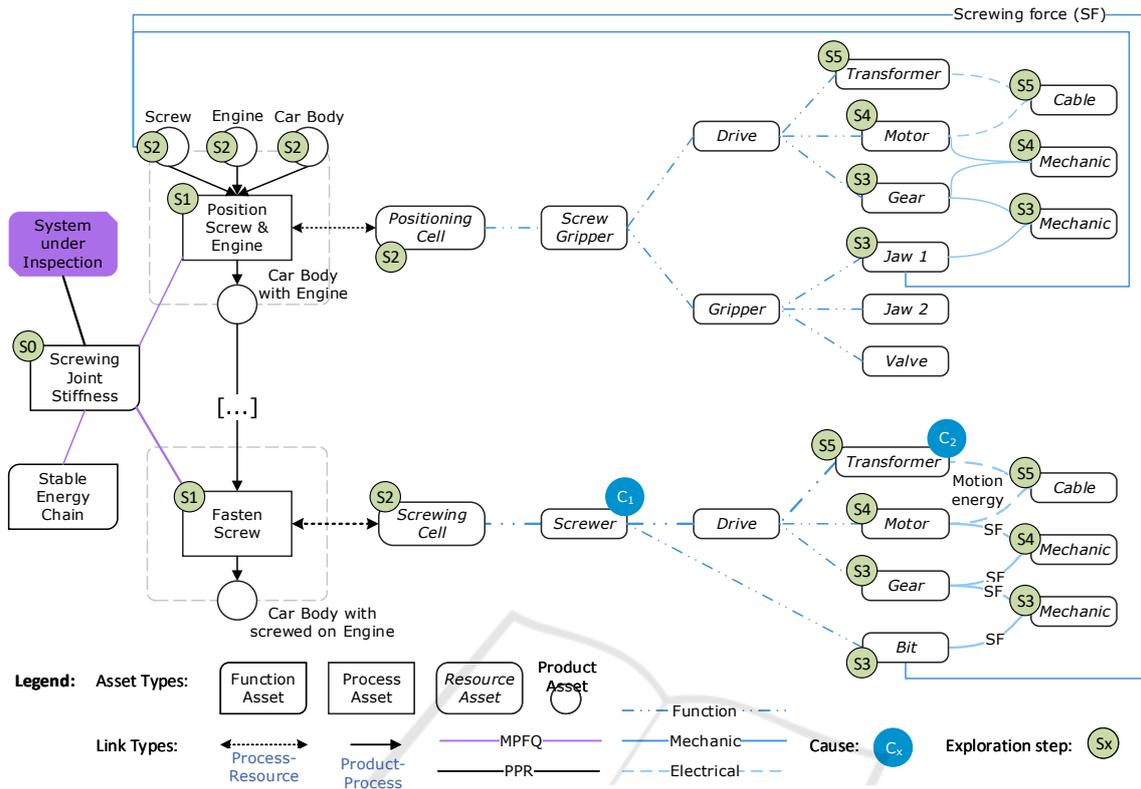


Figure 1: Multi-view sample from the CPPS Engineering Network (CEN) in the use case Screwing System.

#### 4 USE CASE SCREWING SYSTEM

This section introduces the use case *Screwing System* from the car manufacturing industry as an illustrative example for *position and joining* tasks. Such screwing systems contain 50 to 200 assets interlinked in various ways. The corresponding CPPSs are engineered using 15 to 35 different views, covering several engineering disciplines. Thus, engineering a screwing system requires multi-domain models, where common concepts represent shared, i.e., multi-view, assets. These assets are conceptual joining points between the discipline-specific views, resulting in interlinked views within the multi-view model.

The use case covers a screwing system that screws an engine block to a car body. This process is critical as it directly affects the car’s safety and usability. The correct position and stiffness of the screwing joints concern a significant risk in car manufacturing. A loose screw joint on an engine block can lead to cracks in the car body that weaken the car’s structural strength and violate safety regulations.

Figure 1 depicts a section of the aggregated CPPS engineering data model reached by the engineering of the screwing system exploiting the engineering

Table 1: Key concepts for Risk Assessment with FMEA in a CEN (cf. the meta-model in Figure 2).

Concepts	Concept Descriptions
$SuI$	<i>System under Inspection</i> , an <i>Asset</i> ; e.g., a <i>function asset</i> like screw joint stiffness.
$FM_x$	<i>Failure Mode x</i> of the $SuI$ , e.g., low screwing force, leading to an effect.
$E_{xx}$	<i>Effect xx</i> , e.g., a loose screwing joint.
$A; A_F, A_P, A_{P'}, A_R$	<i>Asset</i> ; a <i>Function (F)</i> , <i>Product or Material (P)</i> , <i>Process (P')</i> , <i>Resource (R)</i> Asset in a CEN.
$L_t(A_x, A_y)$	A <i>Link</i> of type $t$ between two <i>Assets</i> , $A_x$ and $A_y$ , e.g., a MPFQ relation, or mechanical, electrical, or information interface.
$C_x(A_y)$	<i>Cause</i> $C_x$ associated to asset $A_y$ , e.g., a wrong param. value leading to a FM.
$H_x(E_{xx}, C_x)$	Hypothesis, linking effect $E_{xx}$ to a set of causes $C_1, \dots, C_n$ via a pathway of assets and links in the CEN.

data logistics. The model shows relevant elements of the exemplary CPPS and is based on the engineering views of product engineering, quality management (MPFQ) (Foehr, 2013), and functional, mechanical, and electrical engineering. Table 1 summarizes the key concepts for FMEA in a CEN. For more details on the use case, refer to (Biffel et al., 2020).

We build on the *Screwing System* use case to illustrate examples for the CPPS-RA approach.

## 5 CPPS RISK ASSESSMENT APPROACH

This section introduces the CPPS-RA meta-model and method steps, and the conceptual design of a prototype to automate parts of the method.

### 5.1 CPPS Risk Assessment Meta-model

The *CPPS-RA meta-model* focuses on the connection of core concepts for FMEA, a *CPPS Engineering Network (CEN)*, and hypotheses that link effects to causes in the CEN, even across discipline boundaries. The meta-model abstracts concepts and relationships from the FMEA standard (DIN60812, 2015) and previous work on ontologies and meta-models for applying FMEA to hypothesis building in specific areas (Höfig et al., 2019).

Figure 2 shows the core concepts of the CPPS-RA meta-model divided into three areas: 1. *FMEA* concepts (in violet), 2. *CEN* concepts (in green), and 3. *Cause-Effect Hypothesis* concepts (in light-blue). All data elements have a unique identifier and can have properties, e.g., for annotations. For details on the meta model concepts refer to (Biffel et al., 2020).

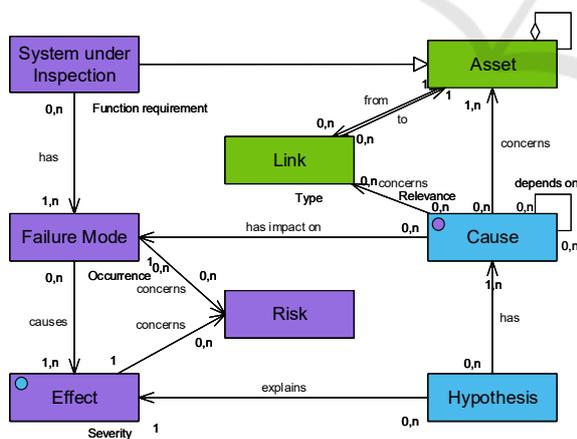


Figure 2: CPPS-RA core concepts meta-model (see concepts in Table 1).

### 5.2 CPPS Risk Assessment Method

The CPPS-RA method follows three steps:

**Step 1. FMEA: Identify risk and informal cause candidates.** In this step, the quality manager (QM)

and the domain expert (DE) follow the FMEA process with a specified goal and scope to define the SuI and identify and prioritize candidate failure modes, effects, and risks. For a selected effect  $E$ , the QM and DE build on engineering knowledge in the project to elicit, e.g., with *Fault Tree Analysis*, a list of informal cause and hypothesis candidates, such as "Effect  $E_{12}$  may be caused by Causes  $C_1$  and  $C_2$ ."

**Step 2. CPPS-RA with CEN exploration.** In this step, the QM and DE iteratively explore the CEN (see Section 5.3) linking informal cause candidates  $C_x$  to assets  $A_y$ . The CEN can, e.g., be modeled in AML following the CPPS-RA meta-model (see Section 5.1). These links serve as the basis for formalizing causes and identifying possible pathways between the causes and the selected effect, which consists of assets  $A_x$  and technical links  $L_t(A_x, A_y)$ . Based on formalized causes, cause-effect pathways, and informal hypothesis candidates, the QM specifies hypotheses  $H_x$  linked to CEN asset data elements as the foundation for testing these hypotheses with CPPS data.

**Step 3. Collect and analyze data based on CPPS-RA results.** In this step, a data analyst uses the CPPS-RA results, i.e., the hypotheses linked to CEN assets, to define data elements for collection and analysis. Based on the collected data, the analyst can test the hypotheses with CPPS engineering and operation data and report hypothesis test results. Finally, the QM and DE can interpret the CPPS data as a strong foundation to address likely causes for important risks.

For an extended report on CPPS-RA method steps refer to (Biffel et al., 2020).

### 5.3 CPPS Eng. Network Exploration

Figure 3 shows the steps 2.x of the CPPS-RA method in IDEF0 notation to iteratively explore likely causes with limited resources for risk assessment. Starting point is an effect with an informal cause candidate, such as "effect *loose screw* may come from wrong *parameter setting in screw motor control*."

**Step 2.1 Explore CEN** In this step, the QM and DE identify assets that are relevant to represent informal cause candidates. Typically, the DE will start in the CEN from the asset that represents the SuI and iteratively explore assets in the neighborhood. Therefore, the DE follows selected links between assets, e.g., mechanical or communication links, potentially related to the effect type. The step results in a set of links between causes and assets and their possibly updated/added representing domain knowledge relevant for the cause-effect argumentation.

Figure 1 shows an abstract CEN from the use case with assets linked by different link types. These

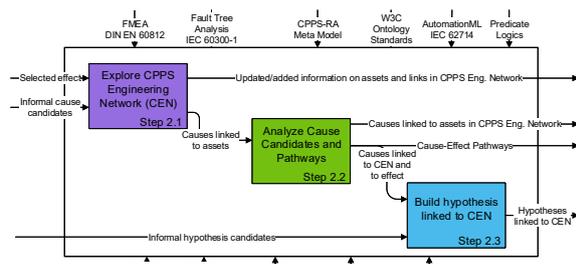


Figure 3: CPPS-RA Step 2: CEN Exploration (IDEF0).

links represent the model views, e.g., mechanical networks, and quality-process networks (see Section 4 and links in Figure 1). The network also allows annotating impact pathways between assets, e.g.  $S_0$  to  $S_5$ . CPPS resources are linked to other resources and sub-resources via mechanical, electrical, and communication interfaces building a resource network. The network includes automation devices that are often causes of engineering errors and failures.

For the iterative exploration, the *asset neighborhood* can be defined by a neighborhood function (starting asset, link types to use, stopping condition, e.g., number of steps, or condition of the asset found, e.g., asset type *automation device*). These functions enable systematically exploring asset neighborhood following the CEN to identify assets and paths likely to lead to a specified effect. Alternatively, the DE can identify relevant asset instances in the CEN and try to find relevant paths between these asset instances.

The effective and efficient iterative exploration of large or complex CENs requires tool support to browse, search, and visualize the integrated multi-view model. Typical CEN browser functions for CPPS-RA include: Overview of related assets, browsing assets and their relationships, filtering assets and relationships according to neighborhood functions, and annotating the relevance of assets and links, e.g., for specifying a cause-effect relationship.

**Step 2.2 Analyze cause candidates and cause-effect pathways.** In this step, the QM and DE analyze causes linked to CEN elements to define at least one *Cause-Effect Pathway* that links the effect  $E$  to one or more causes, as a foundation for substantiating cause constructs with data from CPPS engineering results. A *Cause-Effect Pathway* consists of links between causes, causes and assets, and between assets, including the SuI.

**Step 2.3 Build hypothesis linked to the CEN.** In this step, the QM specifies a formal hypothesis based on the set of causes linked the CEN and the *Cause-Effect Pathway*. The hypothesis consists of the effect, e.g.,  $E_{12}$ , and the list of causes linked to the CEN, e.g.,

$C_1, C_2$ . Figure 1 shows a *Cause-Effect Pathway* that links causes  $C_1$  and  $C_2$  to, e.g., effect  $E_{12}$  by referring to assets and technical links in the CEN. If there is more than one cause in a hypothesis, the hypothesis requires a function that specifies the relationship of the causes to the effect, by default a logical AND function, e.g.,  $H_1(E_{12}; C_1 AND C_2)$ . Therefore, the hypothesis is well defined and linked to CPPS data elements, as the basis for data collection and hypothesis testing (see Section 5.2, Step 3).

**CPPS-RA Conceptual Prototype.** For details on the conceptual prototype, refer to (Biffel et al., 2020).

The CPPS-RA conceptual prototyping results provided a solid basis for the evaluation of the method and for the discussion with domain experts to guide further prototype development priorities.

## 6 FEASIBILITY STUDY

We evaluated the CPPS-RA method’s feasibility with the representative *Screwing System* use case (cf. Section 4) from CPPS engineering. The study built on a CEN that contains function, product, process, and resource assets and selected links between the assets, e.g., functional and qualitative interfaces (cf. Figure 1). CPPS domain experts among the authors of this paper conducted the CPPS-RA method steps. They discussed the results, focusing on the effect *loose screwing joint*, with three senior domain experts from car manufacturing to compare the characteristics of CPPS-RA and their traditional method for risk assessment.

In the following, we summarize the discussion of the main results of the CPPS-RA method steps.

**Results of Step 1: Identify risk and informal cause candidates.** For the risk *loose screwing joint*, the domain experts identified *insufficient screwing force* or *wrong screw positioning* as informal cause candidates.

**Results of Step 2.1: Explore CPPS Engineering Network.** The domain experts reviewed CEN elements relevant for *insufficient screwing force* and structured their CEN exploration as *exploration steps*,  $S_i$ . They characterized the steps by the set of starting elements, neighbourhood functions to select further elements, and termination rules that limit the search scope (see Figure 1 for examples of exploration steps, labeled  $S_i$ ). For more details on the exploration results, refer to (Biffel et al., 2020).

**Results of Step 2.3: Build hypothesis linked to the CEN.** The domain experts used a simple restricted language to express their hypotheses based on cause candidates linked to CEN elements (see Table 1), e.g.,

$H(E_{12}; C_1 \text{ or } C_2)$ , where  $E_{12}$  represents the effect *loose screw joint in car body position X*,  $C_1$  is weak screwing force of *Screw*  $S$ , and  $C_2$  is a wrong parameter setting in *Transformer T*.

As a result, the domain experts could collect evidence on these causes by checking the associated engineering plans or by collecting data from a simulation or an operational CPPS.

## 7 EVALUATION AND DISCUSSION

This section discusses the results of the feasibility study regarding requirements, research questions, and research limitations.

### 7.1 Evaluation

We evaluated the research results in a feasibility study with domain experts regarding the requirements  $R_x$  (cf. Section 3). We investigated common use cases for automotive component assembly processes to better understand the knowledge that domain experts refer to when discussing risk assessment scenarios. We discussed assembly steps, associated assets, and links from the automotive domain similar to the use case *Screwing System* (cf. Section 4, Figure 1). Furthermore, we compared the CPPS-RA method with their traditional risk assessment approach, the discussion of causes for an effect using the discipline-specific models. These models are typically integrated mentally by the domain experts who rely on considerable implicit domain knowledge.

In Table 2, columns list the risk assessment approaches and the rows list the requirements ( $R_x$ , cf. Section 3). The table cells show the evaluation results based on a 5-point Likert scale. The signs + (++) indicate the risk assessment approach to satisfy the requirements (very) well, O indicates partial fulfillment, and - (--) indicate (very) low fulfillment of the requirement by the risk assessment approach.

The representation of the cause-effect pathway in the CEN is a good foundation for selecting data for advanced analyses as the CEN data elements are related to measurable data points during testing, simulation, and operation of the CPPS. For more details on the evaluation refer to (Biffel et al., 2020).

### 7.2 Discussion

The main result of RQ1 on *what data elements are required to represent cause-effect relationships in a CEN as a foundation for CPPS risk assessment are*

Table 2: Capabilities of risk assessment approaches in CPPS engineering.

Requirement	Approaches	
	Traditional	CPPS-RA
R11. FMEA concepts	+	+
R12. CEN concepts	-	++
R21. Causes and Hypotheses	-	+
R22. Mapping Causes & Effects to CEN	-	+
R3. Cause-Effect Path	--	+

CPPS-RA meta-model elements that represent core concepts of FMEA, the CEN, and Cause-Effect hypotheses, including links between these concepts. The meta-model introduced in Section 5.1 addresses the requirements  $R_x$  elicited from practitioners (cf. Table 2).

The main outcome of RQ2 on *how a domain expert can explore a CPPS Engineering Network to identify and assess candidate cause-effect relationships for a failure mode/effect* is the CPPS-RA method. The method allows exploring a CEN to identify and annotate assets and links related to a cause-effect pathway that links likely causes to an FMEA effect. The CPPS-RA method introduced in Section 5.2 addresses the applicable requirements R22 and R3. In the feasibility study (see Section 6), domain experts found the results of the CPPS-RA method understandable and applicable to a typical use case in car manufacturing.

**Limitations.** The feasibility study focused on a single use case in a large car manufacturing company. This may introduce bias due to the specific selection of model types in the CPPS engineering network, the types of effects and causes considered, as well as the roles or individual preferences of the domain experts. The evaluation highlighted that the proposed representation of domain expert knowledge and the CPPS-RA method for risk assessment in discrete manufacturing are promising. However, they should be evaluated in further studies with several engineering organizations and use cases. For details on lessons learned and limitations refer to (Biffel et al., 2020).

## 8 CONCLUSION AND FUTURE WORK

The assessment of risks in CPPS engineering usually requires input from several engineering disciplines. In this paper, we built on a CEN, a multi-domain multi-view CPPS engineering model, to assess risks to the

CPPS and products.

We introduced the *CPPS-RA* approach for linking effects and causes to assets in a multi-view CEN to validate informal Cause-Effect hypotheses and explore potential causes for risks to the CPPS and products, even across discipline boundaries. The CEN model elements provide the foundation for specifying the engineering and operational data required for testing the hypotheses. We defined the *CPPS-RA meta-model* to represent core concepts for integrated CPPS engineering views for risk assessment. We evaluated the CPPS-RA approach in a feasibility study with a conceptual prototype with the use case *Screwing System*, which is representative for discrete manufacturing.

The CPPS-RA approach provides the following benefits: (1) Causes linked to CPPS engineering data elements in a CEN facilitate the automated evaluation of hypotheses based on data, even across discipline boundaries; and (2) the CEN allows validating the cause-effect pathway, i.e., to what extent a CEN element linked to a cause is connected to the CEN element linked to an effect.

**Future Work.** *Combination of model- and data-driven CPPS risk assessment.* Building on the CPPS-RA results of hypotheses linked to a CEN, we plan to explore the combination of model- and data-driven CPPS analysis based on data from CPPS engineering and operation.

*Security and Countermeasures.* Going beyond product quality concerns, we plan to combine the risk assessment regarding functional quality and information security aspects with iterative cause-effect analysis to address the risk for large CPPSs that are part of the critical infrastructure. We plan to extend the CPPS-RA approach to represent countermeasures that address weaknesses of assets or links to mitigate risks to a CPPS or product. For more details on future work refer to (Biffel et al., 2020).

## ACKNOWLEDGEMENTS

The financial support by the Christian Doppler Research Association, the Austrian Federal Ministry for Digital and Economic Affairs and the National Foundation for Research, Technology and Development is gratefully acknowledged.

## REFERENCES

Atkinson, C., Tunjic, C., and Möller, T. (2015). Fundamental realization strategies for multi-view specification

environments. In *2015 IEEE 19th Int. Enterprise Distributed Object Computing Conf.*, pages 40–49.

Biffel, S., Lüder, A., and Gerhard, D., editors (2017). *Multi-Disciplinary Engineering for Cyber-Physical Production Systems*. Springer.

Biffel, S., Lüder, A., Meixner, K., Rinker, F., Engelbrecht, C., Eckhart, M., and Winkler, D. (2020). Multi-View-Model Risk Assessment for Positioning and Joining Simulation (Case Study). Technical Report CDL-SQI 2020-05 CDL-SQI-2020-05, CDL-SQI, Institute for Information Systems Engineering, TU Wien. <https://qse.ifs.tuwien.ac.at/cdl-sqi-2020-05/>.

Biffel, S., Lüder, A., Rinker, F., Waltersdorfer, L., and Winkler, D. (2019). Engineering data logistics for agile automation systems engineering. In *Sec. and Quality in Cyber-Physical Sys. Eng.*, pages 187–225. Springer.

DIN60812 (2015). Din en 60812:2015-08: Failure mode and effects analysis (fmea).

Drath, R., Lueder, A., Peschke, J., and Hundt, L. (2008). Automationml-the glue for seamless automation engineering. In *Emerging Tech. and Factory Automation. ETFA 2008. IEEE Int. Conf.*, pages 616–623. IEEE.

Foehr, M. (2013). *Integrated consideration of product quality within factory automation systems.* dissertation, Otto v. Guericke Universität, Germany.

Henning, K. (2013). *Recommendations for implementing the strategic initiative INDUSTRIE 4.0.* acatech–National Academy of Science and Engineering.

Höfig, K., Klein, C., Rothbauer, S., Zeller, M., Vorderer, M., and Koo, C. H. (2019). A meta-model for process failure mode and effects analysis (pfmea). In *2019 24th IEEE Int. Conf. on Emerging Tech. and Factory Automation (ETFA)*, pages 1199–1202. IEEE.

Hopkin, P. (2018). *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management.* Kogan Page, 5th edition edition.

IEC 62714 (2018). Engineering data exchange format for use in industrial automation systems engineering – automation markup language. *Int. Standard, Second Edition, Int. Electrotechnical Commission, Geneva, 2.*

Kaiser, B., Liggesmeyer, P., and Mäkel, O. (2003). A new component concept for fault trees. In *Proc. Wsh. on Safety critical sys. and sw.-Volume 33*, pages 37–46.

Liu, H.-C., Liu, L., and Liu, N. (2013). Risk evaluation approaches in failure mode and effects analysis: A literature review. *Expert sys. with app.s*, 40(2):828–838.

Lüder, A., Pauly, J.-L., Rinker, F., and Biffel, S. (2019). Data exchange logistics in engineering networks exploiting automated data integration. In *IEEE ETFA*, pages 657–664. IEEE.

Meier, J., Klare, H., Tunjic, C., Atkinson, C., Burger, E., Reussner, R., and Winter, A. (2019). Single underlying models for projectional multi-view environments. In *Proc. MODELSWARD*, pages 119–130. SciTePress.

Sitte, J. and Winzer, P. (2010). Demand-compliant design. *IEEE Trans. on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 41(3):434–448.

Stamatis, D. (2019). *Risk Management Using Failure Mode and Effect Analysis (FMEA).* Quality Press.