Towards A Knowledge Graph-based Framework for Integrated Security and Safety Analysis in Digital Production Systems

Sebastian Kropatschek[1,3,*], Kabul Kurniawan[2,3], Pusparaj Boshale[1], Siegfried Hollerer[1], Elmar Kiesling[2] and Dietmar Winkler[1,3,4]

[1]TU Wien, Institute of Computer Engineering, Vienna, Austria
[2]WU Wien, Institute for Data, Process and Knowledge Management, Vienna, Austria
[3]Austrian Center for Digital Production (ACDP), Vienna, Austria
[4]SBA Research, Vienna, Austria

Abstract

The increasing interconnection of Information Technology and Operational Technology in Industry 4.0 creates new challenges and requires new approaches to ensure that production processes are executed safely and securely. Production system safety and security have therefore become critical aspects as security incidents can lead to serious problems such as production failure, equipment damage, or human injury. This paper introduces a knowledge-graph-based framework for safety and security analysis that integrates prior work on product, process, and resources (PPR) as well as cause-effect modeling. To identify possible attack chains and their impact on safety issues, we leverage Bayesian Belief Networks to estimate failure probabilities and propagate them through the knowledge graph. We evaluate our approach by means of a real-world manufacturing use-case.

Keywords

Safety, Security, Knowledge Graph, Bayesian Network, CPPS

1. Introduction

Security in the production system domain is a critical aspect necessary to maintain reliability and ensure safety during the production process [1]. However, the convergence of Information Technology (IT) and Operational Technology (OT) and their connection in production systems have opened new attack vectors that make them more vulnerable to cyber-attacks [2]. IT infrastructure can increasingly serve as the initial point of attack and cause production system failures and safety issues (e.g., equipment/component damage and human injury).

For example, a Safety Instrumented System (SIS) may be attacked via exploiting IT-based vulnerabilities. As a result, the manipulated SIS cannot react when needed, or the execution of its safety function occurs in the wrong timeframe. This situation may cause people to be injured or harmed (e.g., while interacting with a machine) or damage the production facility or

ISWC 2023 Posters and Demos: 22nd International Semantic Web Conference, November 6–10, 2023, Athens, Greece
sebastian.kropatschek@acdp.at (S. Kropatschek); kabul.kurniawan@wu.ac.at (K. Kurniawan); pusparaj.boshale@tuwien.ac.at (P. Boshale); siegfried.hollerer@tuwien.ac.at (S. Hollerer); elmar.kiesling@wu.ac.at (E. Kiesling); dietmar.winkler@tuwien.ac.at (D. Winkler)

plant. Furthermore, it is possible to trigger safety functions intentionally. As a consequence, the attacked production line or machine line stops its operation, impacting the availability negatively while causing economic damage [3]. Additionally, cyber-attacks may be launched against user interfaces (e.g., web applications) controlling safety functions, potentially impacting human safety over this attack vector when exploited [4, 5]. Therefore and based on the examples, there is the need for a holistic view of safety and security.

Keeping track of the production system state and recognizing such unexpected attacks is an increasingly complex problem. This is due to the heterogeneous nature of resources and components as well as the isolated design of functional safety and security in production systems [1]. Furthermore, different views of engineering experts (e.g., mechanical and automation experts) increase the gap in safety and security coverage and consequently make security and safety analysis increasingly difficult. Several approaches exist to address safety and security [6, 7, 8]. However, there is a need to develop a standardized approach, generic tools, and a framework that effectively combines security and safety in a production system context while offering flexibility and feasibility [6]. In this paper, we therefore introduce a **Knowledge Graph (KG)-based framework for safety and security analysis in production system environments** (cf. Fig. 1). We build on prior work [7] and develop a standards-based model based on an RDF/OWL ontology to construct knowledge graphs ① ②. To analyze the generated KGs, we leverage Bayesian Belief Networks (BBNs) [6] ③ to identify possible failures and propagate them through the KG ④⑤.

2. Our Approach

In prior work [7], we introduced the *PPR Model* which establishes links between Product, Process, Resource (PPR) in a production system environment and *Failure Cause-Effect* relationships. The PPR model comprises three fundamental concepts in production environments and their connections within a production network, i.e., *(i) Products*, such as input or output as resulting from the production process, *(ii) Processes*, such as activities performed to accomplish a certain task, and *(iii) Resources*, such as components utilized by the process to execute tasks. The *Cause-Effect* network represents the existing knowledge of cause-effect relationships curated by experts.

Example Scenario. Fig. 2 depicts a *Collaborative Robot (Cobot) Hazard* scenario [7] represented in a *Cause-Effect-PPR Model*. It involves the risk of a cyber-attack causing harm to humans working with robots in a car part production environment. Therefore, the *Products* produced in this scenario are car parts. The production systems involve several resources including *OT resources* (e.g., cobot, force sensor, and a light-barrier), *Control/IT resources* (e.g, workstations and a process engine/PLC) and *Human resources* such as operators and security engineers. These resources perform tasks in the production *Processes*, such as *"unloading parts"* (performed by a cobot) and a *"human inspection"* – which is carried out by the operator. Finally, the *Cause-Effect* part of the model represents production knowledge pertaining to production and security-related causes and effects.

Safety and Security Issues. In our example scenario, a security incident occurs because the attacker successfully compromises the workstation by uploading malicious software. It allows

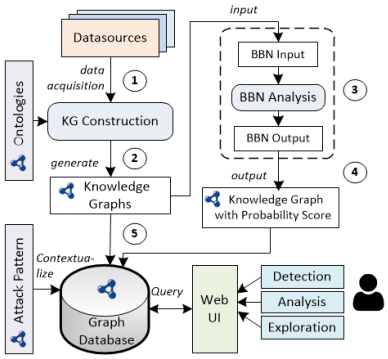

Figure 1: KG-Based SafeSec Framework Architecture.

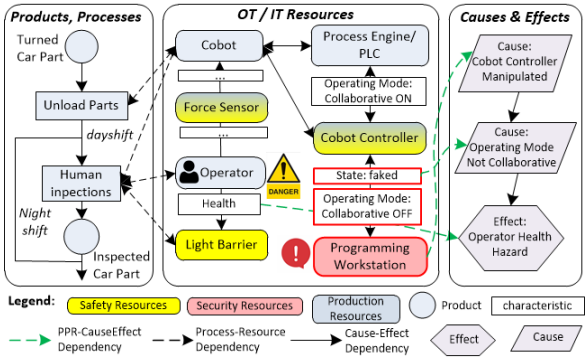

Figure 2: Cobot Hazard Scenario represented in Cause-Effect-PPR Model.

the attacker to manipulate the *Cobot Controller* and change the collaborative mode to ”inactive” while displaying a manipulated state message (”ON” mode). Given that the cobot controller is connected to the cobot, this raises a high risk of an incident wherein the operator can be struck by the cobot and sustain injuries.

Model Conceptualization and KG-Construction. To represent the relevant *Cause-Effect-PPR* knowledge, we developed an ontology based on RDF/OWL. To this end, we followed established ontology engineering practices [9]. We first conducted a survey of existing ontologies and identified [10] as a candidate for cause-effect modeling and the VDI 3268[1] standard as a basis for our PPR representations. Fig. 3 shows our integrated Cause-Effect-PPR ontology. To link knowledge from these domains and coordinate investigations, we introduced a common general concept, i.e., *Characteristic*, which defines characteristic values from both Cause-Effect and PPR elements. It has a self-dependency link identified by the *hasCharacteristic* property and a dependency link to the *FailureMode* concept. Due to space constraints, we do not explain the full ontology in detail but refer the interested reader to the related documentation[2]. Listing 1 shows an excerpt of RDF instance constructed from the proposed ontology.

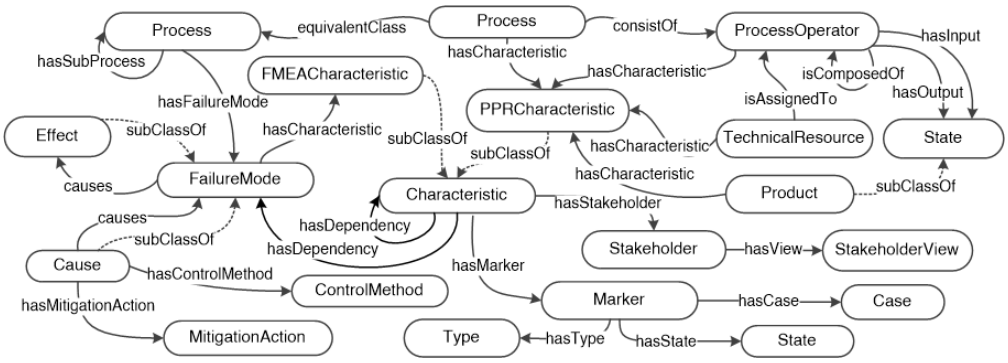

Figure 3: Integrated Cause-Effect-PPR Ontology.

[1]VDI 3682: VDI guideline 3682: Formalised process descriptions (2005)
[2]Ontology Representation: http://w3id.org/acdp/onto/fpi

Listing 1: an Excerpt of RDF instance.

```
@prefix fpi : <http://w3id.org/acdp/onto/fpi#> .
@prefix     : <http://w3id.org/acdp/res#> .
:PLC-1 a fpi:ControlResource, fpi:TechnicalResource;
         fpi:hasCharacteric      :OperatingMode;
         fpi:hasFunctionalLink   :Cobot-1.
:Cobot-1 a fpi:OperationalResource; ...
```

Listing 2: RDF Instance with BBN probability.

```
@prefix bbn : <http://w3id.org/acdp/onto/bbn#> .
@prefix     : <http://w3id.org/acdp/res#> .
:PLC-1 a bbn:Node.
<< :PLC-1 bbn:fail true >> bbn:probability 0.7 .
<< :PLC-1 bbn:fail false >> bbn:probability 0.3 .
:Cobot-1 a bbn:Node; ...
```

KG-based Bayesian Belief Network (BBN) propagation. BBNs are probabilistic models that represent and analyze relationships between variables through conditional probability distributions. They have been investigated extensively in academia and adopted in industry as a method to tackle safety and security challenges in manufacturing [6]. We propose to combine KGs' ability to represent safety- and security-relevant domain knowledge with the ability of BBNs to capture probabilistic relationships. By propagating probability information throughout the KG structure, we leverage BBNs for probabilistic reasoning in knowledge graphs. Integrating BBNs into KGs offers several advantages: (i) By making BBNs queryable, they can be enriched and contextualized with domain knowledge from the KG, (ii) BBNs enhance KGs by providing advanced probabilistic reasoning and inference capabilities. In this context, BBNs can support a KG in analyzing the potential impact of safety and security issues, and finding root causes. Listing 2 depicts an example of such a BBN-KG integration. Here, the probability of `:PLC-1` failing is quantified through RDF-star statement as `<< :PLC-1 bbn:fail true >> bbn:probability 0.7 .` Throughout the KG network, these probability scores are propagated.

3. Preliminary Evaluation and Conclusions

Use-Case Evaluation. Following the scenario described in Section 2, an analyst may need to identify the root cause of a safety incident. Our approach enables the analyst to start the root cause analysis by formulating a SPARQL query as shown in Listing 3. The query traces backward through the KG via `^fpo:hasFunctionalLink*` starting from the identified *Operator Health Hazard*. To find relevant node chains associated with the safety issue, a filter can be applied to trace back and filter the desired nodes with high probability, e.g., `<< ?o bbn:fail true >> bbn:probability ?val2.` and `filter (?val >= 0.5 \&\& ?val2 >=0.5)`. Fig. 4 shows a sub-graph representing the identified and selected nodes chaining associated with the safety incident (note that different node colors show different types of resources). It shows that an attacker managed to bypass the *corporate firewall* ① and launch *malicious software* that compromised the *cobot programming software* on the workstation ②. From there, the attacker gains access to the *cobot* ③ via a *switch* connected to *PLC* and manipulates them ④.

Conclusion and Outlook. In this paper, we introduce a method that represents, constructs and analyzes safety and security in production systems by means of a KG and BBN method. The evaluation result shows high practical relevance as the proposed approach effectively performs safety and security analysis. For future work, we plan to evaluate our approach in a real-world setting and link the identified attack to the existing attack pattern.

Listing 3: SPARQL Query - Backward Search.

```
PREFIX bbn: <http://w3id.org/acdp/onto/bbn#> .
PREFIX fpi: <http://w3id.org/acdp/onto/fpi#> .
PREFIX    : <http://w3id.org/acdp/res#> .
CONSTRUCT {?s ?p ?o}
   WHERE {:Operator ^fpi:hasFunctionalLink* ?o.
          ?s ?p ?o.
          << ?s bbn:fail true >> bbn:probability ?val.
          << ?o bbn:fail true >> bbn:probability ?val2.
   FILTER (?val >= 0.5  && ?val2 >=0.5)}
```

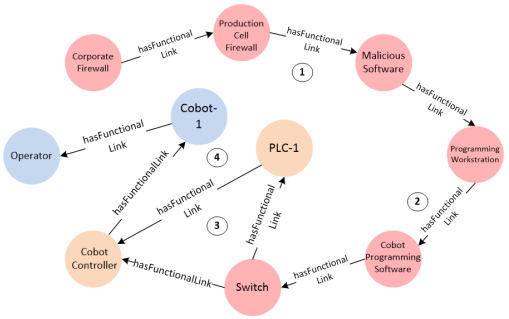

Figure 4: Constructed Graph Visualization.

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. This work has been partially supported and funded by the Austrian Research Promotion Agency (FFG) via the Austrian Competence Center for Digital Production (CDP) under the contract number 881843 and SBA Research. This work has also received funding from the Teaming.AI project in the European Union's Horizon 2020 research and innovation program under grant agreement No 95740.

References

[1] A. Ustundag, E. Cevikcan, B. C. Ervural, B. Ervural, Overview of cyber security in the industry 4.0 era, Industry 4.0: managing the digital transformation (2018) 267–284.

[2] M. M. Alani, M. Alloghani, Security challenges in the industry 4.0 era, Industry 4.0 and engineering for a sustainable future (2019) 117–136.

[3] Jin-woo Myung ; Sunghyuck Hong, ICS malware Triton attack and countermeasures., in: International Journal of Emerging Multidisciplinary Research, 2019.

[4] M. Wolf, D. Serpanos, Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems, Proceedings of the IEEE 106 (2018) 9–20. doi:10.1109/JPROC.2017.2781198.

[5] S. Hollerer, C. Fischer, B. Brenner, M. Papa, S. Schlund, W. Kastner, J. Fabini, T. Zseby, Cobot attack: a security assessment exemplified by a specific collaborative robot, Procedia Manufacturing 54 (2021) 191–196. doi:https://doi.org/10.1016/j.promfg.2021.07.029.

[6] S. Pirbhulal, V. Gkioulos, S. Katsikas, Towards integration of security and safety measures for critical infrastructures based on bayesian networks and graph theory: A systematic literature review, Signals 2 (2021) 771–802.

[7] S. Kropatschek, S. Hollerer, D. Hoffman, D. Winkler, A. Luder, T. Sauter, W. Kastner, S. Biffl, Combining Models for Safety and Security Concerns in Automating Digital Production, in: 2023 INDIN, 2023.

[8] K. Kurniawan, A. Ekelhart, E. Kiesling, G. Quirchmayr, A. M. Tjoa, Krystal: Knowledge graph-based framework for tactical attack discovery in audit data, Computers & Security 121 (2022) 102828.

[9] N. F. Noy, D. L. McGuinness, et al., Ontology development 101: A guide to creating your first ontology, 2001.

[10] Z. Rehman, C. V. Kifor, An ontology to support semantic management of fmea knowledge, International Journal of Computers Communications & Control 11 (2016) 507–521.