Abschlussbericht, Fachbericht
Final Report, Technical Report

Reaktorsicherheitsforschung - Vorhaben-Nr.: 1501600D
Reactor Safety Research-Project No.: 1501600D

Vorhabentitel: „Evaluierung von Verfahren zum Testen der Informationssicherheit in der nuklearen Leittechnik durch smarte Testfallgenerierung – Plattformen, Produkte und Architekturen“ (SMARTEST2)
Project Title: „Evaluation of Testing Techniques for IT-security checks in automatic control software for nuclear power Plants – Platforms, Products and Architectures“ (SMARTEST2)

Autoren / Authors: Dr. Karl Waedt, Ines Ben Zid, Josef Schindler, Erkin Kirdan, Xinxin Lou, Ndeye Ndiaye, Romarick Yatagha, Natasha Edeh, Oumayma Mejri

Dienststelle des Autors / Performing Organisation: Framatome GmbH, ICCPS-G

Berichtsdatum / Publication Date: 2024-08-07

Berichts – Nr. / Report - No:.....
(Berichts- Nr. nur, wenn eine vom ZE/AN vergeben wird.)

Gefördert durch:

Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz unter dem Förderkennzeichen 1501600D gefördert.

Haftungsfreistellungsklausel

Diese Veröffentlichung wird durch das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV, SMARTEST2, Projekt-Nr. 1501600D), im Rahmen des Forschungsförderung für nukleare Sicherheit gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

1. Contents

List of Figures

List of Tables

1. Kurzfassung / Abstract

This section contains a German language and English language abstract of the SMARTEST2-FRA project, which is Framatome GmbH's part as partner in the SMARTEST2 R&D. The main content of this report is in English language, with the Summary section 1.2 also available in German language as section 1.1.

1.1. Kurzfassung

Das Verbundprojekt SMARTEST2 soll einen wesentlichen Beitrag dazu leisten, dass wichtige Sicherheitskontrollen für Digital Instrumentation & Control (I&C), wie sie in Kernkraftwerken (KKW) eingesetzt werden, eine adäquate Sicherheitslage erreichen können. Der SMARTEST2-F&E-Vorschlag wurde 2018 genehmigt und offiziell für den Start im Jahr 2020 genehmigt. SMARTEST2 ist eine Fortsetzung der SMARTEST R&D, die von 2015 bis 2019 durchgeführt wurde. Dieses Folgeprojekt wird in Kooperation von Hochschulen und Industrie gemeinsam durchgeführt, um Testmethoden zur systematischen Unterstützung bei der Erkennung von Sicherheitslücken vernetzter und softwarebasierter Prozessleitsysteme zu entwickeln. Dazu wird ein modellgetriebener Ansatz entwickelt, um die interne Struktur von Software, Kommunikationsnetzwerken, Netzwerkprotokollen und repräsentativen ausgewählten Teilen der Gesamtarchitektur der Leittechnik eines KKW zu untersuchen. Ein Hauptzweck besteht darin, intelligente ("intelligente") Angriffe unter genau definierten Testbedingungen zu generieren. Die drei deutschen Hochschulpartner stellen die notwendige wissenschaftliche Schlüsselexpertise aus den Bereichen Informationstechnologie (IT) Sicherheit, Software Engineering und Industrieautomation zur Verfügung. Der Industriepartner setzt die adressierten Safety I&C und Operational I&C Plattformen in Deutschland, der Schweiz und/oder anderen europäischen und weltweiten Neubau- oder Modernisierungsprojekten ein.

In Übereinstimmung mit den Einschränkungen der Ressourcen, z. B. für durchschnittlich einen Vollzeit-Doktoranden pro Hochschulpartner, müssen der technische Umfang und die Tiefe begrenzt und fokussiert werden. In Bezug auf das Technology Readiness Level (TRL), das häufig zur Beschreibung der Marktreife von Forschungsergebnissen auf einer Skala von 1 bis 9 (9, die auf eine Zertifizierung für die Massenmarktnutzung hindeutet) verwendet wird, werden die Ergebnisse voraussichtlich bei TRL 3 bis 5 liegen. Dementsprechend Nachfolgende Forschung wird notwendig sein, um den technischen Umfang zu erweitern, mehr Lebenszyklusphasen entlang der Lieferkette von Automatisierungsgeräten anzugehen, die konzeptionellen Ergebnisse selektiv umzusetzen und die erzielten Ergebnisse als Grundlage für Endbenutzerbibliotheken zu verfeinern, Tools, empfohlene Sicherheitsmaßnahmen, Verfahren und Anleitungen. Im Hinblick auf den sich entwickelnden FuE-Kontext sollte ein Folgeprojekt die TRL 4 bis 6 behandeln und KKW-Stilllegungen und verbrauchte nukleare Speicheranlagen als Teil eines angepassten oder erweiterten Anwendungsbereichs der FuE für Cybersicherheit im Nuklearbereich umfassen.

1.2. Abstract

Note: For a German language version, see subsection 1.1.

The aim of the collaborative research project, SMARTEST2, is to provide a major contribution towards demonstrating that important security controls for Digital Instrumentation & Control (I&C), as used in Nuclear Power Plants (NPPs), can achieve an adequate security posture. The SMARTEST2 R&D proposal was approved in 2018 and officially approved to start in 2020. SMARTEST2 is a continuation of the SMARTEST R&D which was carried out from 2015 until 2019. This follow-up project is jointly carried out through a cooperation of universities and industry to develop test methods for systematic support in detecting security vulnerabilities of networked and software-based process control systems. For this purpose, a model-driven approach is developed to examine the internal structure of software, communication networks, network protocols and representative selected parts of the overall architecture of the I&C of a NPP. A main purpose is to generate intelligent ("smart") attacks under well-defined test conditions. The three German university partners provide the necessary key scientific expertise from the domain of Information Technology (IT) security, software engineering and industrial automation. The industry partner deploys the addressed Safety I&C and Operational I&C platforms in Germany, Switzerland and/or other European and worldwide new-build or refurbishment NPP projects.

The approach is intended to be independent from automation system specific characteristics (e.g., specific network configurations, communication protocol characteristics, I&C platform features and I&C architecture and design details). The results should then be useful for testing of automation systems in the nuclear field as well as be applicable to other critical infrastructures.

The industry partner, identified as SMARTEST2-FRA, participated in the continuous exchange with the university partners with regards to the application of newest scientific approaches to representative NPP applications and the focus on representative I&C platforms that were agreed upon at the beginning of the project. The research project included a limited hardware budget for one of the new I&C platforms that is expected to be used in future NPP projects for the implementation of safety systems and safety-related systems. The research project also leveraged training for all partners on a specialized fuzz testing framework, which includes a new Software Development Kit (SDK) that can be deployed for selected SMARTEST2 network protocol modeling objectives. The industry partner also provided a dedicated lockable lab (with access-control) for the entire project duration. Additional laboratory equipment and software was provided by the university partners.
In line with the limitations on resources, for e.g., on average one full-time PhD candidate at each university partner, the technical scope and depth have to be limited and focused. In terms of the Technology Readiness Level (TRL) often used to describe the market readiness of research results, on a scale from 1 to 9 (9 indicating a certification for mass market use), the results are expected to be at TRL 3 to 5. Accordingly, subsequent research will be necessary in order to broaden the technical scope, to address more lifecycle phases along the supply chain of automation equipment, to selectively implement the conceptual results and to refine achieved results as a basis for end user libraries, tools, recommended security countermeasures, procedures and guidance. With regard to the evolving R&D context a follow-up project should address TRL 4 to 6 and include NPP decommissioning and spent nuclear storage facilities as part of an adjusted or extended scope of the cybersecurity R&D for the nuclear domain.

2. Objective

Advancement in technology has seen critical infrastructures, such as NPPs, increasingly adopting computer-based systems in favor of traditional analog systems. Whilst advantages realized from this change includes increased functionality, flexibility, economy and reliability, there are reasonable concerns regarding the significant risks to safety and security as introduced by the computer-based digital safety and operation control technology (hereon referred to as I&C systems).

As this project is a continuation of the SMARTEST R&D project, the objective is to refine a set of topics and initiate other new ones. In terms of test approaches, the objective for SMARTEST2 would be to cover a broader number of protocols used by the I&C of NPPs. In addition, the teams would work on deploying and addressing additional and more complex security test scenarios and algorithms. Another objective is to have more automated security tests which can be deployed by IT administrators.

To address this growing attack surface, the SMARTEST2 project sought to develop so-called "*smart*" testing procedures. The play on the word "smart" is used to not only indicate intelligent testing procedures, but to also highlight the purposefulness behind their approach and design. This project seeks to identify as many weak points as possible in selected I&C systems, with the overall aim to lower the risk of critical incidents. Attack scenarios are devised according to the presumed impact on confidentiality, integrity and availability. In this regard, formal attack models are constructed – these models include features of attackers, as well as the attack vectors against the target I&C systems. Besides the attack-model, a test model is envisaged to enable model-driven automatic testing, as well as to provide formal measurements of the testing coverage. A security model of the I&C systems and associated simulation environment are created to cover the following features:

- Model of I&C configurations (networks, systems, sub-systems, components), including all considered security artefacts
- Model of requirements and recommendations from security standards
- Semi-formal representation of security countermeasures
- Tool for the specification of security relevant relations
- Platform-independent/-dependent simulation environments
- Tools for analyzing and visualizing testing results
- Guidance and tools for partially automated attack tree analysis as a basis for the effective assignment of graded security controls

The following I&C platforms and products were considered in the project:

- TELEPERM XS (focus on TXS Core 4.0)
- Siemens PCS7
- SIMATIC S7-1500 (newer TIA portal starting 15.2)
- Qualified Display System (QDS)

- TXS Compact (initial analysis during R&D)

A demonstration system with real hardware/software for non-safety systems of future NPP projects is configured to verify and validate the developed testing approaches and results.

The above list of legacy, current and future (currently being developed) I&C platforms was agreed upon at the beginning of the Research and Development (R&D) project. The justifications for selecting these platforms include:

- to address legacy systems, like Siemens PCS7, that are already in use since many years and where previous versions were known to be susceptible to cyber-attacks (for example, Stuxnet);
- to address current systems, as these represent the state-of-the art: and
- to address recently developed systems, in order to propose potentially suited Security by Design concepts.

TELEPERM XS© is the Safety I&C platform that was initially developed by Siemens KWU (which later on became AREVA GmbH and then Framatome GmbH). It is one of a few worldwide Safety I&C platforms that is certified for use according to the most stringent nuclear I&C requirements (Cat. A according to IEC 61226 [1] and Class 1 according to IEC 61513 [2]).

Siemens PCS7 is one of the most common automation platforms. It is available worldwide in most industrial business domains and can be used for the implementation of I&C systems processing Cat. C functions according to IEC 61226 [1].

Siemens SIMATIC S7-1500 is currently one of the most popular automation platforms deployed in most business domain. While this platform claims performance and security improvements as compared to Siemens PCS7, it also deploys new concepts, like the Totally Integrated Automation (TIA) Portal, which allows web and cloud based configuration and software repositories.

Qualified Display System (QDS) is a specific automation platform of Framatome for safety-related user displays and limited user interaction. The QDS platform is available as an extension to TELEPERM XS 2nd generation and is also further developed, similarly to the Safety I&C – 3rd Generation. Accordingly, in this R&D project QDS is considered in the broader sense of a current and future display system platform that is able to meet high safety and security requirements.

TELEPERM XS© Compact is an automation system based on Field Programmable Gate Array (FPGA) technology that can be used with different modules from the TELEPERM XS portfolio for e.g. signal conditioning, TXS cabinet and installation infrastructure, power supply, etc. to implement safety I&C systems able to fulfill highest requirements of safety-related I&C systems in nuclear power plants. TELEPERM XS Compact offers a wide range of function block types that can be easily combined to implement typical NPP I&C functional requirements and safety functions. Safety I&C solutions on TELEPERM XS Compact contain no CPU and no software, but are entirely operated on configurable hardware logics in the FPGA and memory cells. Thus, it acts as a diverse automation platform, compared to TELEPERM XS Main Line CPU-based devices (such as SVE2/SVE3 application function processor). TELEPERM XS Compact enables the development of class 1 safety I&C systems according to IEC standards (IEC 61513, IEC 62566, IEC 60987; etc.) and to the system needs and functional requirements.

Note: As TELEPERM XS Compact will be an important future Safety I&C platform, further R&D on its FPGA based approach may be considered in a follow-up R&D project of SMARTEST2.

3. Work Packages

The SMARTEST2 project consists of the following four work packages:

1. WP1: Analysis of security vulnerabilities with safety level considerations (HS-MD)
2. WP2: Hierarchical smart testing with basic attacks (OvGU-AMSL)
3. WP3: Systematic, attack-specific test procedures (FAU-SWE)
4. WP4: Tool-based smart testing (FRAM)

3.1. WP1: Analysis of Security Vulnerabilities with Safety-Level considerations (HS-MD)

The first work package is led by the university partner HS-MD and is based on the comprehensive approach detailed in SMARTEST. Modular structure of the work packages allows parallel processing, with interfaces for knowledge transfer among partners. Topics to be developed in the short and medium term are considered jointly with regard to their suitability. The relation between the different sub-work packages WP1.x and external WP (e.g. 4:x) is shown below.

All partners concomitantly contributed to the following sub-work packages:

- WP 1.1: Requirements analysis and definition for a static-dynamic modeling language
- WP 1.2: Evaluation of the modeling language and modeling tools in OvGU test environment
- WP 1.3: Evaluation of the modeling language and modeling tools in HS-MD test environment
- WP 1.4: Evaluation of the modeling language and modeling tools in FRAM test environment
- WP 1.5: Analysis and further development of the predefined modeling language
- WP 1.6: Attack models and attack scenarios in collaboration with OvGU

An overview of the WP1 and the different sub work packages and the involved partners in each item is summarized in Figure 1.

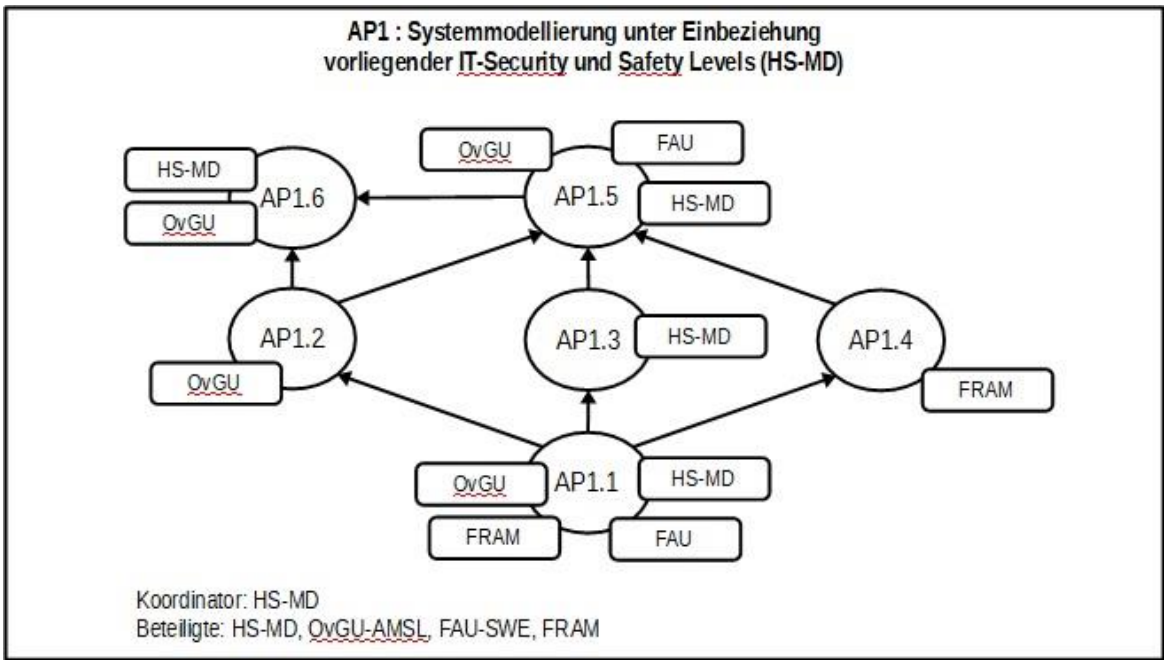

Figure 1- WP1 internal structure: Coordination of activities within WP1

3.1.1. WP 1.1: Requirements analysis and definition for a static-dynamic modeling language

The initial segment of WP1 contributes to the formulation of requirements for the desired modeling for Nuclear Power Plants, focusing on special features, various components and entities within existing demonstrators. General requirements for future modelling focus on aspects such as transitions between security zones and levels, protocol conversions and firewalls, process flows, communication structures and safety requirements.

The basis of the work is the refinement of the OvGU-AMSL demonstrator modelling, the INES-7 (Integrated Nuclear Evaluation System 7) whose design is based on findings from the project "IAEA CRP J02008 Enhancing Computer Security Incident Analysis and Response Planning at Nuclear Facilities - Subproject Incident Response, Forensic Readiness and Law-Enforcement for I&C of NPP”

Through collaborative reflection and analysis, the project partners endeavor to enable a realistic representation of control processes laying a solid foundation for its integration into various domains and applications, thereby facilitating more seamless and efficient operations in the future. Notably the joint sub-packages: WP 4.7: Modelling of Security Tests Relevant Artefacts and WP 4.9: Testing of Semi-formal Representation of Security Controls.

The current approach consists of manually generating the models. Since this is associated with an increased amount of time, the possibility of automated

exploration is explored as an additional modeling approach. The approach should have both passive and active exploration possibilities and generate models automatically via the demonstrator INES-7. As part of the cooperation, the need for a portable, targeted, customizable and freely available modeling tool emerged to ensure a better representation of the aspects to be modeled.

The concrete investigation of theses aspects took place within the framework of WP 1.2. Furthermore, working meetings are to be held with the partner HS-MD.

3.1.2. WP 1.2: Evaluation of the modeling language and modeling tools in OvGU test environment

WP 1.2 entails a Static Infrastructure Modeling approach of the INES-7 demonstrator within the OvGU-AMSL test environment, showcasing the possibilities for an automated exploration of a control engineering network as a basis for automated model creation.

The objective is to comprehensively understand and model the network infrastructure and behavior by using both passive and active exploration methods.

This involves producing modules for component and behavior modeling in order to passively extract information about devices and protocols from network packets. In this context, emphasis is placed on:

- Exploration of network components within the test environment for the existence of structural effects and forensic data types;
- Investigation of the creation of behavior and process models based on Modbus communication by the mean of automated modeling approach;
- Exploration of the possibilities for active network exploration methods to identify components not detectable through passive methods;
- Additionally, visualization of communication flows and potential data exfiltration within the network.

A consideration of different tools and an easy adaptation of these tools to the need for modeling (see WP 1.1) was also considered.

Following the evaluation of the modeling language, identification of possible limitations and necessary extensions should take place.

3.1.3. WP 1.3: Evaluation of the modeling language and modeling tools in HS-MD test environment

The primary objective of WP 1.3 is to rigorously evaluate the modeling language and associated tools within the HS-MD test environment in order to ensure their efficacy and integration in the model factory. The task also involves the

comprehensive application of the modeling approach developed in WP1.1 to the model factory with key considerations.

Following the evaluation of the modeling language, it is essential to identify any potential limitations and determine necessary extensions. A thorough analysis of the modeling language's performance within the HS-MD test environment is to be conducted, focusing on its ability to accurately represent physical processes with regard to control units and communication infrastructures. Any shortcomings or areas where the language fails to capture critical system and network behaviors must be documented. Based on these findings, recommendations for enhancements and modifications should be proposed to improve the modeling language's capability and ensure it meets the specific requirements of the test environment. This iterative refinement process aims to optimize the modeling tools for comprehensive system integration and future technological implementations.

Furthermore, for future testing, the system should be equipped with a Next Generation Firewall and Network Access Control, which are essential for securing the infrastructure and managing access. This setup allows for rigorous testing of security protocols and ensures that the system is robust against potential threats.

3.1.4. WP 1.4: Evaluation of the modeling language and modeling tools in FRAM test environment

Similar to WP1.2 and WP1.3, this work package involves applying and evaluating the modeling approach in the FRAM test environment to identify limitations and necessary improvements.

At Framatome, various prototype applications are intended to be modeled using tool-based Smart-Testing. Different tools, test environments and setups are deployed in the scope of the joint sub-packages WP 4.1, WP4.4, WP 4.6, WP 4.9. The evaluation of the modeling language and modeling tools thus includes a detailed analysis of safety and security-relevant artefacts modelled at the network protocol level together with the partner HS-MD (WP 4.1), the cybersecurity aspects of user interactions with control systems taken up in a semiformal and formal manner (WP 4.4), the I&C / Electrical Power Systems (WP 4.6) and the semi-formal (tool-readable) representations of security measures and controls (WP 4.9). Content of these works will be further discussed respectively in section 3.4.1, section 3.4.4, section 3.4.6 and section 3.4.9.

3.1.5. WP 1.5: Analysis and further development of the predefined modeling language

WP 1.5 focuses on the creation of an extended requirements catalog to optimize the modeling approach defined in WP1.1 and the expansion of the modeling

language described in WP1.1 based on the defined requirements catalog. All university partners were involved.

Three specific aspects are taken into account and need be covered:

- Modelling of the static infrastructure (mapping of the landscape);
- Modelling of the physical process (mapping of the process flow);
- Modeling of control engineering (mapping of dynamic behavior).

The subdivision into control technology and physical process is due to the fact that the modeling of the physical process focuses on sequences of physical states, associated logical conditions and actions initiated by these. The modeling of the control technology describes the implementation of these logical conditions and initiated actions by the concrete devices. Through these two types of modeling, a transfer of the logical conditions and initiated actions to the computing and communication processes within the control technology can be carried out. Here the sequence of condition and action is specifically mapped to the components of the control technology and a necessary communication process

These facets collectively depict the behavior of the entire INES-7 static landscape in which the dynamic actions are carried out.

An additional analysis of the various test environments using the expanded modeling language to identify any further need for improvement will also be conducted. The outcomes of this endeavor feed into WP 4.7: Modelling of Security Tests Relevant Artefacts and WP 4.9: Testing of Semi-Formal Representation of Security Controls.

3.1.6. WP 1.6: Attack models and attack scenarios (OvGU)

In WP1.6, the exchange between the project partners continuously examines different attack models as well as attack scenarios.

As part of the manual modeling approach, the aim is to consider possibilities for attack modeling. OvGU-AMSL supported the consortium partner HS-MD. This support was provided through agreements in digital meetings. Topics such as construction of demonstrators, identification of potential attack vectors and scenarios within the demonstrators, security enhancement by modeling and structural changes, and iterative review and adjustment of modeling approaches in accordance with revised regulations (e.g. IAEA) were discussed.

Research of Exemplary attacks are based on the attack model investigated in AP 1.1 - AP 1.5 which consists of typical attack techniques specified in NSS17T. Attack scenarios such as denial-of-service (DoS), ransomware, or exploitation of fuzzed identified zero-day vulnerabilities are analyzed to understand their influence and structural effects on hardware, software, and communication systems. These analyses aim to deepen the understanding of how such attacks can impact the

overall security and functionality of the systems being modeled.

3.2. WP2: Hierarchical smart testing with basic attacks (OvGU-AMSL)

Built on the insights and preliminary work from “Smartest,” this work package led by the university partner OvGU-AMSL, aims to develop approaches for conducting systematic, reproducible security investigations and implementing practical and experimental security testing for complex networked control environments (hardware, software, protocols, control processes, physical processes). Based on the three available independent test environments (OvGU, HS-MD, FRAM), the developed testing approaches will be continuously implemented, evaluated, and updated as needed, considering configuration heterogeneity. By applying these methods to three different test environments, the reproducibility and scalability of the developed procedures shall be ensured.

An overview of the WP2 is provided in Figure 2.

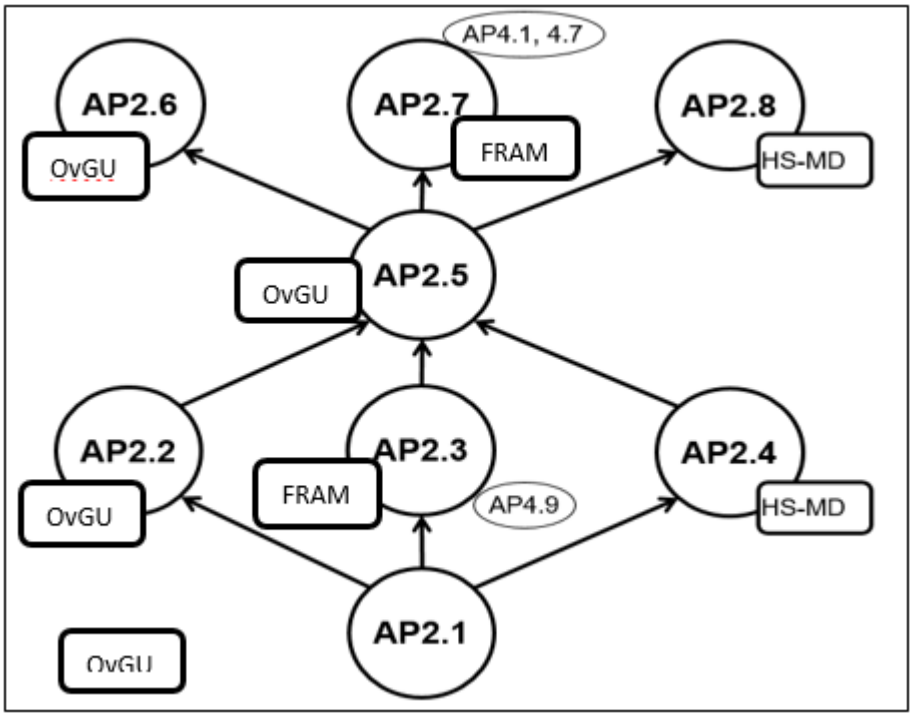

Figure 2- WP2 internal structure

3.2.1. WP2.1 Exemplary Attack Scenarios/Sequences (OvGU)

The adaptation and refinement of the exemplary attack scenarios selected in WP1.6 will take place, considering software, hardware, and network communication. Exemplary attack sequences will be defined as combinations of

basic attacks across all areas of analysis and all knowledge levels, taking into account the specific characteristics of the three test environments.

3.2.2. WP2.2 Demonstrative Implementation of Attack Sequences in the OvGU-AMSL Test Environment (OvGU)

The conceptual attack scenarios developed in WP2.1 will be demonstratively implemented in the OvGU-AMSL test environment. The goal is to identify the need for adjustments, extensions, and possible limitations considering the specific details of the test environment.

3.2.3. WP2.3 Demonstrative Implementation of Attack Sequences in the FRAM Test Environment (FRAM)

The conceptual attack scenarios developed in WP2.1 will be demonstratively implemented in the FRAM test environment. The goal is to identify the need for adjustments, extensions, and possible limitations considering the specific details of the test environment.

3.2.4. WP2.4 Demonstrative Implementation of Attack Sequences in the HS-MD Test Environment (HS-MD)

The conceptual attack scenarios developed in AP2.1 will be demonstratively implemented in the HS-MD test environment. The goal is to identify the need for adjustments, extensions, and possible limitations considering the specific details of the test environment.

3.2.5. WP2.5 Generation of Attack Scenarios and Sequences (OvGU)

Based on the findings from the demonstrative application of exemplary attack sequences, the generation of the attack scenarios will take place. The results and insights from the demonstrative application for all test environments from AP2.2-2.4 will be used to realize refinements and necessary adjustments to the knowledge levels and attacker/attack models. The goal is to implement the automatic generation of test cases and the automation of test sequences.

3.2.6. WP2.6 Validation of Automatically Generated Attack Sequences in the OvGU-AMSL Test Environment (OvGU)

The automatically generated attack scenarios will be evaluated for the OvGU-AMSL test environment. The goal is to identify the need for adjustments, extensions or limitations.

3.2.7. WP2.7 Validation of Automatically Generated Attack Sequences in the FRAM Test Environment (FRAM)

The automatically generated attack scenarios will be evaluated for the FRAM test environment. The goal is to identify the need for adjustments, extensions or limitations.

3.2.8. WP2.8 Validation of Automatically Generated Attack Sequences in the HS-MD Test Environment (HS-MD)

The automatically generated attack scenarios will be evaluated for the HS-MD test environment. The goal is to identify the need for adjustments, extensions or limitations.

3.3. WP3: Systematic attack-specific test approaches (FAU-SWE)

Motivated by the progress already achieved in the collaborative project SMARTEST, the partner FAU-SWE aims to extend its applicability to broader and more general attack scenarios with the overarching goal of creating a guideline that supports the identification and application of recommended test patterns for specified detectable vulnerability classes. For this purpose, this work package consists of the iterative sequence of the following steps(see Figure 3) :

- WP3.1: Mapping Between Classes of Vulnerabilities and Test Patterns
- WP3.2: Static Analysis Methods
- WP3.3: Dynamic Testing Methods

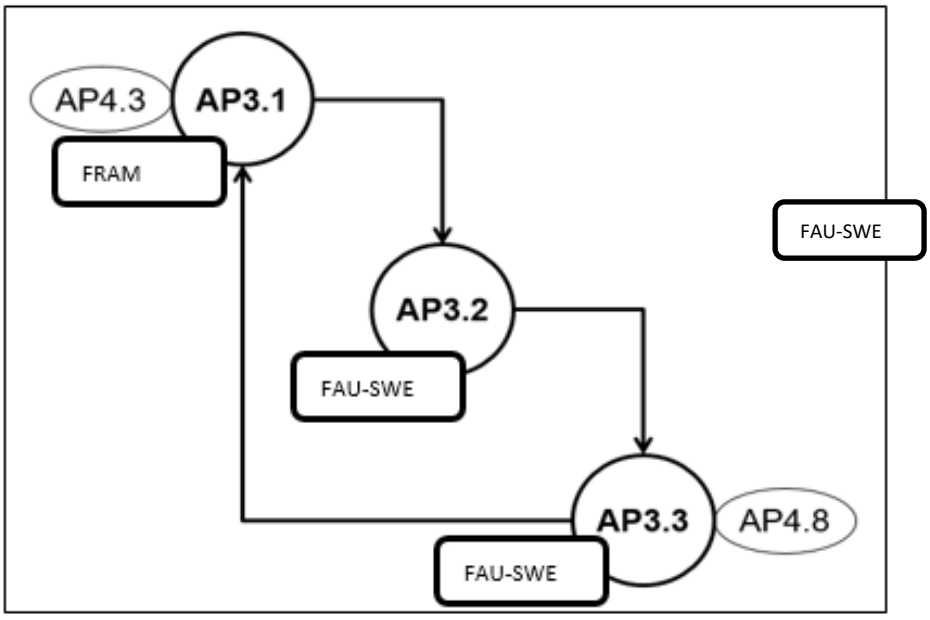

Figure 3- WP3 internal structure

3.3.1. WP3.1: Mapping Between Classes of Vulnerabilities and Test Patterns

In the first sub-package, existing partially divergent vulnerability taxonomies (e.g., [CWE]) will be examined and evaluated for relevance to nuclear facilities in cooperation with the industrial partner Framatome. The aim is to compile a catalog of selected and significant vulnerabilities, which will be further grouped based on commonalities regarding their activity in operation. According to their relevance, a new vulnerability class will be selected for further investigation. Upon completion of the static and dynamic analyses (see WP3.2 and WP3.3), this step is to be revisited to capture the determined test strategy as a test pattern and assign it to the considered and potentially additional vulnerability classes.

3.3.2. WP3.2: Static Analysis Methods

The vulnerability class last selected in the previous sub-work package will then be examined in terms of its static analyzability, i.e., the localization of all potential attack surfaces as automatically as possible. Such investigations have been successfully conducted for the attack class "Overlapping Machine Instructions" by identifying syntactically permissible memory-cell-shifted machine code interpretations, and for the attack class "Buffer Overflow" by determining instructions with buffer accesses. This investigation can be static, i.e., without executing the code to be examined; however, tools (so-called static analyzers) can be used for support. The limits of static analysis are apparent: all locations that might pose threats of the considered type are identified, but generally not the actual risk that may arise from them, which is often undecidable statically. Therefore, efforts are made to extract predicates from the static analysis that are necessary and sufficient for exploiting the vulnerabilities, as these predicates allow optimal control of the search for suitable test cases in the subsequent dynamic phase. For the attack class "Buffer Overflow," the static analysis was based on the so-called "Integer Constraint Analysis," which provides necessary and sufficient inequalities for the occurrence of a buffer overflow.

3.3.3. WP3.3: Dynamic Testing Methods

The attack surfaces and predicates extracted in the previous step now provide the basis for new test procedures, which are generally processed as multi-criteria search procedures. The predicates provide the criteria that a search procedure must meet. Due to the complexity of the underlying control and data flows, which may include loops with an unknown number of iterations, a systematic search for suitable test cases that meet all criteria is generally unachievable. In such cases, appropriate heuristics must be applied to the search problem, the quality of which, i.e., the degree to which the criteria are met – if not yet optimal – can be used to randomly generate new test cases using genetic operators. If the search is

successful, the found test cases can trigger the vulnerability; otherwise, suitable metrics for the search effort used can provide insights.

For the "Buffer Overflow" attack class, newly developed heuristic test generation procedures were successfully applied to three examples of increasing complexity, where the most complex example required a refinement of the heuristic based on global optimization by means of local optimization approaches/ a refinement of the global optimization-based heuristic using local optimization approaches.

3.4. WP4: Tool-based smart testing (FRAM)

WP4 is led by Framatome GmbH and it covers the following nine sub-work packages:

- WP 4.1: Security Testing of Industrial Network Protocols for Nuclear
- WP 4.2: New Hardware-based Security Solutions and Validation
- WP 4.3: Security Testing at the Source Code and Binary Code Level
- WP 4.4: Security Testing of User Interaction Relevant Parts
- WP 4.5: Forensic Readiness Testing
- WP 4.6: I&C / Electrical Power Systems
- WP 4.7: Modelling of Security Tests Relevant Artefacts
- WP 4.8: Security Testing of Formal Specifications
- WP 4.9: Testing of Semi-formal Representation of Security Controls

The relation between the different sub-work packages WP4.x

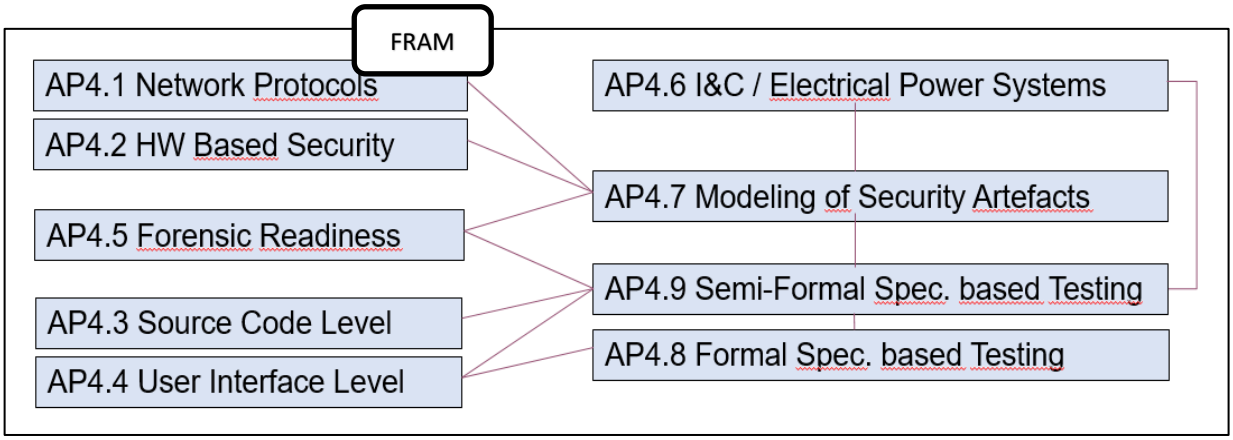

Figure 4- WP4 internal structure

3.4.1. WP 4.1: Security Testing of Industrial Network Protocols for Nuclear

In general, the research project SMARTEST2 focuses on the IT security of software-based control systems. One main goal is to identify suitable cybersecurity

protection measures for process control systems. For this purpose, the various communication protocols (MODBUS, PROFIBUS, PROFINET and OPC UA) of the current control systems must first be checked.

The communication protocols offer the automation components various functionalities that are required for control and regulation in nuclear power plants. However, current control systems from the automation environment are often equipped with only minor security countermeasures, as the systems were mainly designed to meet the performance requirements and security Countermeasures were provided outside the systems (for example, by physical protection) or system availability and real-time behavior could have been affected. But as networking progresses, this is no longer acceptable. To investigate the corresponding vulnerabilities, it is necessary to model all safety and security-relevant artifacts at the network protocol level. Thus, the effects of safety-relevant events on functional safety and nuclear safety can be evaluated and simulated.

For this purpose, risks can be assigned and prioritized in order to implement an effective and appropriate approach. In the approach, the attack scenarios are formulated and tested with the communication protocols.

Assuming that maintaining integrity is a crucial role in restricting and even avoiding the manipulation of communications, possible solutions are reviewed to determine their benefits. Recent advances in cryptographic protection for critical infrastructure have contributed to the development of light-weight MAC security solutions. The solutions support time-critical communication with significantly reduced resource requirements. As part of the SMARTEST2 research project, these solutions are also extensively investigated, implemented and tested for critical infrastructures. An expected project result is the development of a secure switch that supports the MAC-based protection measures and offers the functionality of secure key exchange. The overall goal is to maintain the integrity of network communication to eliminate misuse or manipulation, as well as increase the trustworthiness of communication over the network. These protocols currently used in nuclear power plants, the protocols used in new automation systems and the light-weight approaches are subjected to in-depth security tests.

3.4.2. WP 4.2: New Hardware-based Security Solutions and Validation

As part of the SMARTEST R&D project, it was determined that certain hardware-related protection measures as well as security mechanisms implemented in HW are required in addition to the testing of software configurations and software tests. For example, there were specific questions from Preussen Elektra and EnKK about secure hardware configurations due to known misconfigurations in the Intel Management Engine (ME), which will be implemented in Intel processors from 2006. The ME runs with its own operating system either on a dedicated controller, PHC (Intel Platform Controller Hub) or in the SoC (system-on-chip).

The focus of SMARTEST2 is less on the security aspects of these processor manufacturers specific hardware-related solutions but on the possibilities, the current processors regarding secure design and support of virtualization on hardware level offer. This goes hand in hand with "software defined hardware" applications and "software and hardware co-design", which are possible with newer hardware and corresponding software tools. This is seen as a complement to ASICs (Application Specific Integrated Circuit), which are widely used as the preferred solution with optimized, non-changeable HW components in assemblies of security control solutions.

3.4.3. WP 4.3: Security Testing at the Source Code and Binary Code Level

The static analysis on source code can help to avoid security vulnerabilities, for example by avoiding buffer overflows or deadlocks. Especially with programming languages (such as C/C++) which are used in automation due to their good performance characteristics, corresponding language constructs are missing. Static analysis tools such as synopsys coverity can be used to identify safety-critical quality defects. The tool also tests secure coding. Another tool is Polyspace, which can find a particularly weak point in interfaces (application programming interface) in boundary areas, starting from a virtual source code execution in a multidimensional variable space.

Furthermore, domain knowledge could be introduced to support the static analysis of the source code. For example, we assume the limitation to rotation speed (< 500 per minute) as a predefined safety-relevant rule. A certain sequence of code sections that can set the rotation speed higher than 500 means one or more potential security gaps. Additional security testing at the binary level can also help identify the vulnerabilities based on specific programming languages or even detect injected malicious code.

To increase the reliability and robustness of a system, the security analysis at source code level and binary level is necessary. With such security tests, security gaps can be found as early as possible, ideally even before the system integration tests.

3.4.4. WP 4.4: Security Testing of User Interaction Relevant Parts

Within the framework of SMARTEST, graphical user interfaces were part of the consideration of qualified display systems (QDS). As part of the research project SMARTEST2, the analyses are to be extended and deepened, since the human component can be the weakest link in a safety chain on the one hand, but on the other hand can also make the appropriate decisions for adequate protection.

Human Machine Interfaces (HMIs)" play a key role in any industrial control system. These interfaces are used to visualize process information, highlight critical states, condense information, monitor and document accident consequences, among others orders. The latter is usually not permitted for the highest safety requirements in current power plants (this is done via conventional control switches), but will also be required for the highest safety levels in the future.

HMIs are among the most critical attack vectors. In addition to the confidentiality and availability of an HMI, integrity is critical. It is expected that on HMIs the displayed data is authentic without ambiguity or ambiguity being understood by the operator. To achieve this, a specific new approach is evaluated for HMIs. First, the HMIs are modeled as assets, analyzed and necessary countermeasures are implemented. Then, tool-supported appropriate security tests can be performed to improve the status of the HMI and verify the integrity of the process information displayed in the control room. As a prerequisite for the use of tools, a corresponding modeling of the relationships (AP4.7) as well as semi-formal representation of the application security controls (AP4.9) is required.

3.4.5. WP 4.5: Forensic Readiness Testing

Security measures to detect manipulations are particularly important for critical infrastructures. In accordance with the attacks to be assumed (Design Basis Threat), internal perpetrators must also be assumed. The physical security measures (Preventive Security Controls) do not apply here. Measures for a secure detection of manipulations are required (Detective Security Controls).

As part of the research project SMARTEST, the tool SLogVIZ was developed. For SMARTEST2, it was planned to further evaluate and improve SLogVIZ. The tool can work with public or commercial so-called "Security Information and Event Management (SIEM)" to correlate the results if manipulated log files are affected. With intentional manipulated log files, the quality of SLogVIZ could be checked and further developed. In addition, an independent or web-based user interface of SLogVIZ was developed to use the tool in forensic readiness training. Detailed security tests and forensic analysis on operational control systems are carried out.

With SMARTEST2 the logging information was especially considered with the hardware based security solutions (WP 4.2), as part of an embedded data diode.

The semi-formal description of security measures for Digital Electronic Artifacts (Forensic Digital Evidence) is investigated in conjunction with WP 4.9.

3.4.6. WP 4.6: I&C / Electrical Power Systems

As part of the cybersecurity tests of a nuclear power plant, the functionalities and weaknesses of the power supply systems ("Electrical Power Systems" EPS) must also be taken into account. EPS is required for both ongoing operations and emergencies. Cyber-attacks could disrupt the ongoing operation of a nuclear power plant, even if redundant EPS is present. Therefore, the security-by-design concepts must be applied both for the control technology and for EPS.

As part of the SMARTEST research project, basic threat scenarios were developed so that potential weaknesses in control systems as well as their impact and consequences can be identified and investigated.

In the SMARTEST2, security tests to find the weak points are to be extended to EPS, for example with regard to the temperature monitoring of transformers, generator switches and busbar switching systems in substations. Corresponding system platforms used in German and Swiss nuclear power plants are SIPROTEC, SCOUT and SENTRON in different versions in conjunction with SIMATIC S7.

3.4.7. WP 4.7: Modelling of Security Tests Relevant Artefacts

A typical nuclear power plant contains hundreds of digital systems, in particular critical digital units (CDAs in English "Critical Digital Assets") required for the overall operation and safety/security of the plant. In order to identify CDAs, the entire structure of a power plant, its equipment, communication systems and the networks with the security protection measures as well as supporting systems that are security-relevant are recognized. Experts from different areas are required to build the security baseline for systems. The goal of the security analysis is that as many as possible convert the security requirements to quantitative descriptions and measurements in order to iteratively minimize the remaining cybersecurity risks.

In order to evaluate the resilience to cyber-attacks at power plant level, the modeling must be extended accordingly. The security-relevant artifacts at different levels of abstraction and associated CDAs must be considered in the model.

The modeling of the control systems with the Automation Markup Language (AutomationML) can help to represent the information that is generated, exchanged and used within the processes of the control systems. The latest Industry 4.0 approaches of modeling are applied and extended for the nuclear domain, especially with regard to test coverage metrics and the prioritization of the analysis of paths along attack trees.

3.4.8. WP 4.8: Security Testing of Formal Specifications

This package is going to analyze the system (Refueling Machine)/controller (Siemens S7-1500) vulnerabilities base on the formal specification. Formal Methods (FM) are considered can greatly increase our understanding of a system by revealing inconsistencies, ambiguities, and incompleteness that might otherwise go undetected. Knowing the system well is the foundation of performing safety and security analyses. If we even do not precisely know how the system should work, or what is the behavior of the system under certain situations, how can we know whether some abnormal events happened. We will not be able to know whether there is a possibility that detrimental things happen until they really occur. Thus, to know the system well as early as possible, and to try to find out as many vulnerabilities as we can, is a better and more cost-effective choice than performing an analysis after an incident happened. Formal Methods (FM) have been and are considered as a reliable approach to verify the system vulnerabilities and give counterexamples (if the specified properties are not satisfied), especially find out the weakness of system in design stage. However, though the FM approach is reliable, it is not as popular as some other semi-formal methods in the industrial domain, the main reason is that it is not so practical.

In SMARTEST2, we will try to apply formal method to analyze the vulnerabilities of system, and provide a practical approach to fill the gap between the formal methods' advantage and its practicality. This approach will be easy to use, reliable and effective. The functional specification is written in a formal language, for example, First Order Logic (FOL), Hoare Triple, combine with AI planning techniques together, to get a correctness and completeness specification. Safety and security analysis will be deployed base on the functional specification. Model checking (use model checker e.g. SPIN) is one of the available ways to check the safety and security properties. The safety and security properties will be specified based on the Framatome experts enrich experience in this domain.

3.4.9. WP 4.9: Testing of Semi-formal Representation of Security Controls

Numerous security measures (security controls) are used for the various components of the control technology platforms, which were considered within the scope of SMARTEST. For complex systems, it is not enough to describe them only on paper and then manually evaluate all connections. In the SMARTEST-FRA project proposal, this was indicated as an option, but for resource reasons, it could only be considered as a starting point. One basis should be the standard ISO/IEC 27034-1 already mentioned in the SMARTEST project application, whereby further parts of this standard series have now been published. The security measures must be defined in a machine-readable, e.g., XML and/or JSON format so that tools can start on it. The concept of "Level of Trust" is based on the security level used in the nuclear sector. Implementing Security Degrees. The relationship between the

security measures shall be indicated. Relations with power plant employees must be specified according to the RACI model. In principle, the verification and validation (security test) procedures must be specified for all security measures, so that the implementation is also checked after the "security by design". For resource reasons, however, this should only be investigated for exemplary security measures. Security measures can not only be additional components (for example for authentication) but also, for example, properties of a source code module. This semi-formal description is related to several other APs, in particular AP4.1 (network protocols), AP4.2 (HW based security), and AP 4.5 (forensic readiness). Important here are also metrics for the tool-based evaluation, which also requires the relationship to the modeling, so which Application Security Controls (ASCs) are used at which points in the model.

4. Preconditions and research context

4.1. Know-how of project team

4.1.1. Relevant Know-how at Framatome GmbH

On one hand, Framatome brings its practical know-how into the structure and the provision of a realistic simulation environment and the necessary attack sequence generation. In addition, various activities (for example in WP1) of the other partners with know-how on productive nuclear control systems are significantly supported. Furthermore, Framatome brings know-how from worldwide projects, standardization and from a platform development context.

4.1.2. Relevant Know-how at project partner HS-MD

HS-MD, with its previous knowledge of industrial automation technology, is also instrumental in providing the simulation environment and in coordinating the final exemplary application of the elaborated solutions.

4.1.3. Relevant Know-how at project partner OVGU-AMSL

OVGU-AMSL mainly designs and accompanies the definition, design and application, etc. of the attack scenarios in the context of security attack and attacker modeling.

4.1.4. Relevant Know-how at project partner FAU-SWE

FAU-SWE contributes its know-how in formal modeling, specifically for a compact and formal recording of the attack scenarios using appropriate modeling languages and defining the required model-based test approaches.

4.2. Infrastructure at Framatome GmbH

Framatome owns test-bays and several test facilities, offices and IT infrastructure in Erlangen and Karlstein. During the project, infrastructure was available to PhD students.

4.3. Test facilities

4.3.1. Test facilities at FRA

Framatome GmbH owns several test facilities. This includes a test lab in Erlangen, Paul-Gossen-Str. 100, Building 10. This test lab contains TELEPERM XS and Siemens automation equipment, as well as Electrical Power Systems (EPS) equipment (SIPROTEC) and IT systems, typically used in NPPs and critical infrastructure. The test lab and offices also include scalable software development environments for isolated software development, intranet software development

and web development. The TELEPERM XS Monitoring and Service Interface (MSI) test, which was earlier performed by Framatome GmbH, was reviewed by SMARTEST PhD students. The MSI test is performed on FRA products, by sending and recording manipulated frames (layer 2) to the system under test (SUT).

Figure 5. Initial TELEPERM XS Equipment in Framatome Test Lab

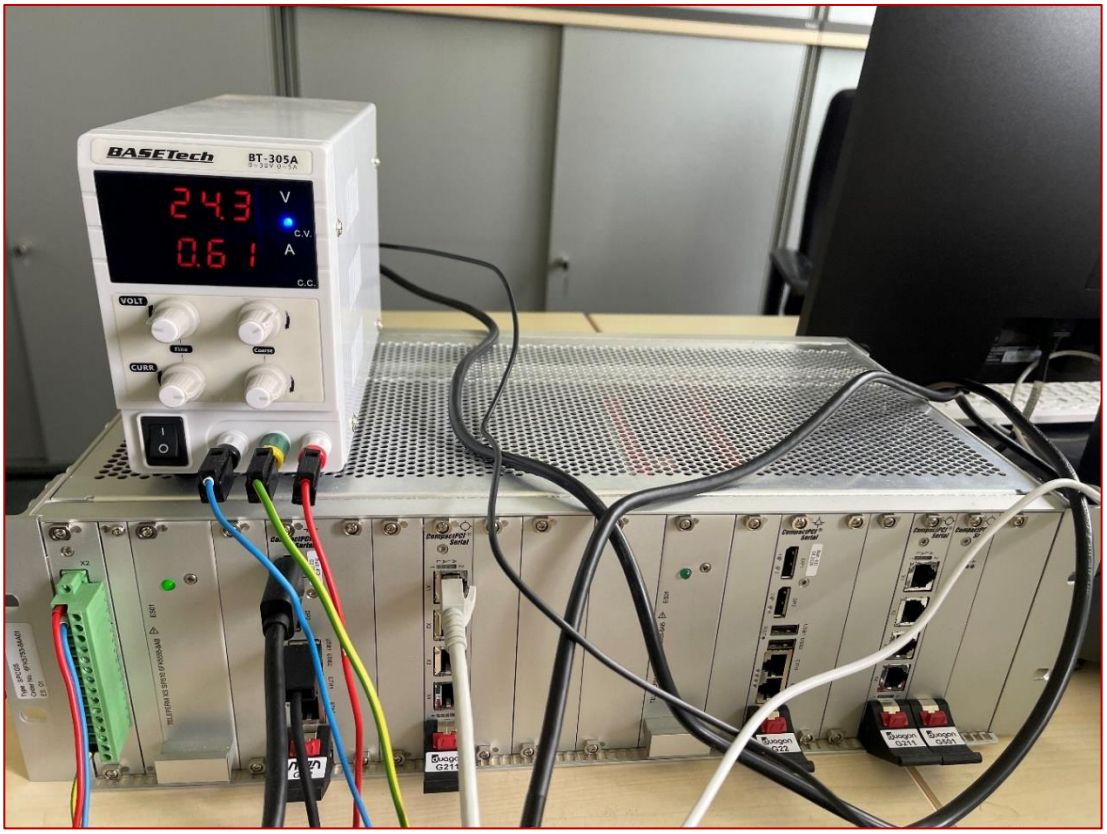

Figure 6. New SPCGS rack of the TELEPERM XS Equipment in Framatome Test Lab

Figure 7. S7-1500 Equipment in Framatome Test Lab

4.3.2. Test Facilities at HS-MD

At the university partner HS-MD, several labs are available for research projects. The major lab for automation technology that is used for the research project SMARTEST is a Model Factory for Engineering Technology “Modellfabrik-ET” as shown in Figure 8. The lab is located in Building 17 in the campus of Magdeburg-Stendal University of Applied Science.

Figure 8. Model Factory for Engineering Technology of Partner HS-MD

In this lab, different SIMATIC S7 controllers, like S7-300, S7-1200 and S7-1500 are connected through variants of Profibus (FDL, PMS and DP) or PROFINET. The control computer can be accessed through a gateway linked to the university network.

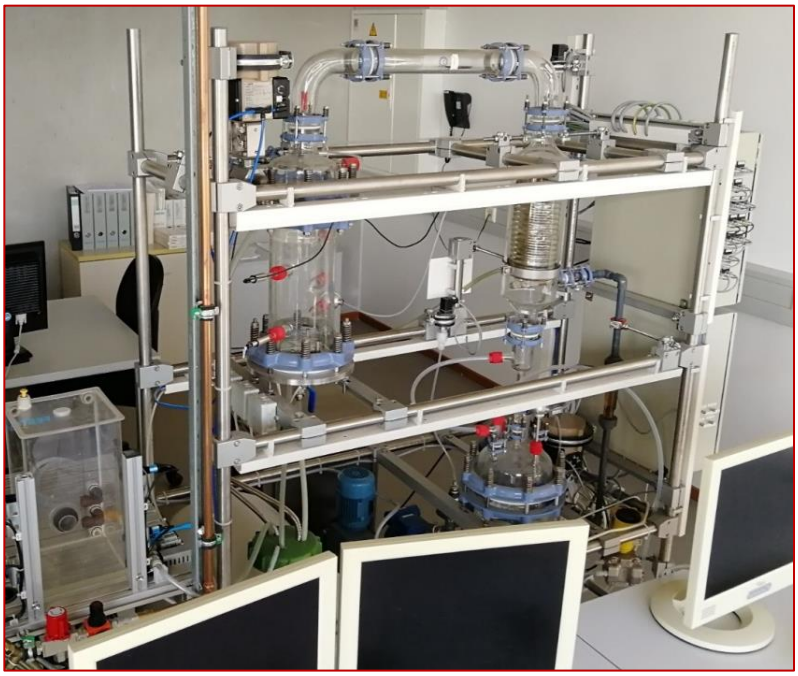

Figure 9. Refinery Process Part of the Model Factory ET

The Distillation unit as shown Figure 9 is a part of the ”Modellfabrik-ET” lab. It can be seen as a simplified model implementation of a steam generator used in NPPs. The distillation is controlled by a programmed S7-1200 controller.

Figure 10 shows a metal pressing and stamping testbed “Stempelanlage”. The system connects 2 S7-1200 PLC and one control computer. It works with a part separator (2) and an optic sensor. In the case a part is detected by the sensor, the PLC will continuously send a signal to the control computer to inform it a part exists, and it will be displayed on the UI program. When the part is removed, no signal will be sent the computer anymore so the UI displays that no parts have been detected or connected.

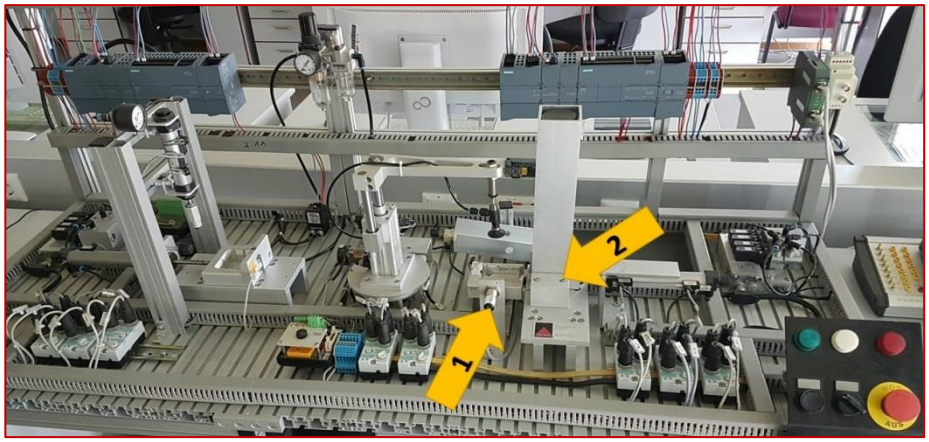

Figure 10. Metal Pressing and Stamping Testbed at Partner HS-MD

4.3.3. Test facilities at FAU-SWE

The Software Engineering department of partner FAU is equipped with main computer workstations, as well as software tools available for faculty members.

4.3.4. Test facilities at OVGU-AMSL

Within the scope of Smartest, PLC test facilities of the OvGU were used for test setups. The test setup for Smartest (OvGU-Security-Demonstrator) is based on a PLC and implements a control for signaling states and a button at a digital input. In addition, the configuration application and HMI software suitable for the firmware version of the PLC have been used. In order to evaluate the possibilities and effects of attacks, communication was examined on the basis of network recordings and then specifically influenced. Open source software in combination with a passive network tap was used to create the network recordings.

4.4. Associated partners

Beyond the SMARTEST2 R&D partners from three German universities, Framatome cooperates with other companies, including Siemens AG in Erlangen (without subcontracting). Furthermore, cooperation (without subcontracting) is established with universities where SMARTEST2 PhD students are completing their thesis. These universities include the University of Siegen, University of Bielefeld.

4.5. Existing research networks

Framatome, including PhD candidates involved in the SMARTEST and SMARTEST2 R&D provided extensive support to German standardization and is involved in the development of new standard IEC 63096 (Security Controls for NPPs).

Note: In recent years the 250+ pages IEC 63096 is widely adapted in countries that deploy nuclear energy. It is even translated to national versions, e.g. in France, Germany and China.

In addition, Framatome cooperates with and attend research events and conferences in Computer Science Society (Gesellschaft für Informatik – GI), International Conference on Nuclear Engineering (ICONE) and the Annual Meeting on Nuclear Technology (AMNT).

5. Planning and implementation of the project

5.1. Planning

This project is planned together with three University partners: Institute for Elektrotechnik, University of Applied Science Magdeburg-Stendal* (HS-MD), Department of Software Engineering (Informatik 11), University of Erlangen-Nuremberg (FAU-SWE), and AG Multimedia and Security, Otto-von-Guericke-University Magdeburg (OVGU-AMSL). Each university planned to hire one PhD student for the project, whereas Framatome GmbH, as the industry-partner, intended to hire six PhD students in order to address security testing of Safety I&C and Operational I&C, the different I&C platforms and the current and new I&C platforms. The staff in Framatome working on the SMARTEST2 project was initially represented by two full time employees and 3 PhD students. Towards the end of the project this number increased to include a total of 4 full time employees as well as 5 PhD students. Due to specific project topics, it took longer than planned to hire PhD students with proper background – students were hired as early as 2021 and as late as Q1/2024. All project partners planned to perform security testing on different I&C platforms currently installed in nuclear power plants and new platforms used in other industry domains and expected to be used in future projects for NPPs. Reaching technology readiness levels TRL 3 to TRL 5 is planned.

Concerning trainings, during the SMARTEST2 project, Framatome contributed to a training preparation at the IAEA headquarters. IAEA planned to offer these cybersecurity trainings at their location in Seibersdorf, near Vienna, to a number of about 1000 participants per year.

During the SMARTEST2 project, the purchase of new hardware was limited to the purchase of DELL XPX 17 notebooks used as a powerful tool for testing. In addition, a TELEPERM XS representative HW in the form of a rack which combines both the TXS Service Unit (SU) and TXS Gateway (GW) have been acquired.

Concerning the dissemination of project results, it was planned to have little or no overlapping with regards to the national, European and international conferences where scientific papers will be submitted as well as the participation of Framatome at the it-sa fair in 2022 and 2023.

In autumn 2024, Framatome will present selected cybersecurity solutions at the it-sa 2024.

5.2. Implementation of the project

The implementation of the R&D project is described in the following two sections, first for the overall implementation with the partners (5.2.1) and then for the SMARTEST2-FRA part in (5.2.2).

5.2.1. Overall implementation of the project

The overall project coordination was assumed by partner HS-MD, who had already coordinated a smaller previous project on nuclear safety with participation of Framatome GmbH. Also partner HS-MD had already cooperated with the head of the department of Software Engineering at the Friedrich-Alexander University Erlangen and the University of Applied Science Magdeburg Stendal is located close to the Otto-von-Guericke University Magdeburg.

From the very beginning, the project was conceived to rely on ongoing workshops and regular meetings and teleconferences of the project partners. The first joint two days meeting was held virtually due to the implemented COVID-19 restrictions.

As can be seen from the definitions of the work packages, the lead is taken by each of the university partners HS-MD, OvGU-AMSL and FAU-SWE for each of the work packages WP1, WP2 and WP3 respectively while Framatome took the lead for work package WP4.

The partners had discussed the selection of the I&C hardware to be purchased as part of the R&D project from the very beginning and had also considered guidance by senior staff from GRS involved in the external funding. Existing HW that was purchased for the SMARTEST project was taken into account while making this estimation. As the focus from SMARTEST was on the purchase of Operational I&C Hardware, it was preferred to acquire a Safety I&C Hardware by the SMARTEST2-FRAM. Due to the fact that the Safety I&C is usually isolated via physically unidirectional optical data diodes and/or physically isolated networks which, by design, some of the attack vectors that could be exploited by threat agents with different capabilities were excluded.

The results for the work packages WP1 and WP2.1 and WP2.2 were elaborated and published as described in more detail in the respective sections of this report. Important steps towards these results were determined through several meetings and teleconferences in which the grading of the capabilities of threat agents was discussed for all lifecycle phases, but especially for the Engineering and Integration and the plant operation and maintenance.

A key part of the SMARTEST2 project is the “smart” (as model based) security tests. Fuzzing was and still is currently “the most effective and efficient vulnerability discovery solution” [5]. However, the fuzzing solutions available for IT and to a lesser extent, for Industrial Automation, vary broadly, with brute force dumb fuzzing on the lower end and commercial or proprietary fuzzing solutions for selected network protocols at the high end. Even the brute force approaches may rely on tools that collect network traffic over a given time period, e.g., one hour, and then tailor the attack datagrams according to heuristics and the intelligence derived from listening to the network traffic on selected network segments.

The SMARTEST2 approach is to deploy fuzzing as a core technology for testing network protocols based on a comprehensive, systematic and scalable approach suited for complex I&C systems and transferrable to the critical infrastructure industry domain.

Comprehensive approach

In the context of this R&D project, a comprehensive approach means that the whole I&C architecture of a nuclear power plant is addressed. This includes all Safety I&C systems, all Operational I&C systems and all independent or supporting IT systems and subsystems. This is a wide scope, and it includes most of the digital equipment available in the main control room of a nuclear power plant.

Note: Some important digital equipment, like the digital devices for EPS of NPPs or the physical protection specific digital devices of NPPs are not explicitly in the scope of this R&D. They could be addressed as part of a subsequent R&D.

The representative reference architecture, agreed upon during the SMARTEST project, contains components that are typical for the nuclear domain, including different types of physically unidirectional gateways, at ISO/OSI layer 2 and at ISO/OSI layers 3 and 4 with specific application layer software at both ends of a unidirectional connection.

The reference architecture also considers the concepts of security grading and security zones, which implies meeting graded security requirements including graded requirements and effort on security testing.

Systematic approach

The systematic approach on applying fuzz testing technology started with an in principle analysis of all relevant network protocols that are in the scope of the R&D, as well as appropriate fuzz testing tools available on the market.

It became clear that some network protocols used in the nuclear domain are proprietary. Thus no free or commercial fuzz testing tools supporting the fuzzing of these protocols are available. Accordingly, the decision was to deploy a fuzzing test framework that includes a Software Development Kit (SDK) or an Application Programming Interface (API) that can be configured or extended in order to prepare smart fuzzing test suites for partially known proprietary protocols.

Scalable approach

A scalable approach means that the developed algorithms and procedures are not just applicable for a single network or logical interface, and do not heavily depend on manual interaction or configuration.

Accordingly, tools and software libraries are needed to support this. The first part towards scalability is a semi-formal representation of the relevant part of a complete I&C architecture. The relevant part has to include all security artefacts and all digital and process engineering assets that are needed in order to perform overall risk assessments and to support the assignment of fuzz testing approaches and a graded effort for achieving security test metrics.

In order to achieve scalable representations, the focus is on the semi-formal representation of the needed model, as well as the support of linking between digital and process engineering assets with security controls. In order to support this linking, the existing or planned countermeasures (security controls) are represented as Application Security Controls (ASCs) [7], as the basis for this semi-formal representation is already provided by ISO/IEC 27034-5-1 [8] in an extendible way (based on XML or JSON file formats).

In order to support the analysis by security experts in some cases, 3D representations are used, especially when plant sites, plant facilities, plant floors, plant rooms, I&C cabinets, hardware sub-racks, hardware modules are involved together with their components, like the front and back doors of an I&C cabinet. Beyond providing an adequate view and navigation support for security experts, this approach avoids maintaining multiple 2D views that could become inconsistent over time. Nevertheless, 2D representations are preferred where appropriate, e.g., for logical network diagram representations.

Based on these semi-formal representations, including the description of network interface configurations for communication processors, gateways, switches and firewalls, appropriate “smart” test cases can be generated.

Transferrable approach

The semi-formal representation of security artefacts and related assets is a minimum requirement as a basis for tool support. In order to make the semi-formal representations transferrable to other business domains, the concepts, data structures and annotations (metadata) have to be based on standardized exchange formats that are known and applied by the different business domains.

Accordingly, Automation ML [4] was selected as a standardized representation of assets, including physical assets and dynamic aspects (process engineering part) and even the expression of automation logic (e.g., processing of analog signals from sensors). While Automation ML is based on multiple formats that are already

standardized, none of these are specifically designed to represent security artefacts. However, as these formats are extendible (XML-based) the information that has to be added by SMARTEST tools can be inserted into the existing structures. This includes the links towards ASC instances, which are standardized as aforementioned.

This semi-formal approach based on the latest Industry 4.0 concepts and formats (like Automation ML) will also support the calculation of metrics on the current security posture based on assigned ASCs and on validation results achieved from security testing. Each ASC can be associated with validation procedures (including automated fuzz testing configurations) specific to the targeted security degree (target security level).

5.2.2. Implementation of the SMARTEST-FRA part of the project

This section addresses the SMARTEST-FRA part of the R&D project implementation, especially:

- the cooperation with the project partners,
- the cooperation with further university partners,
- the project staffing and organization,
- the dissemination of results and
- the exploitation of results.

Cooperation with project partners

A detailed overview of the cooperation between Framatome and the university partners is provided in Section 3. Framatome had the opportunity to convey to the university partners the domain-specific industry requirements and needs, along with representative architectures and designs and different levels of detail. For this purpose, the newest applicable standards, guidance and publications related to cybersecurity in the nuclear domain were evaluated.

For more specific requirements and architectures of modern NPPs, Framatome provided the project partners reference to selected parts of the new Evolutionary Power Reactor (EPR) either directly or in a condensed and streamlined version. According to the national regulation in France and UK, comprehensive parts of the technical EPR descriptions are available for comments by the public. Especially the EPR documentation for the Hinkley Point C (HPC), the EPR project is well suited as a basis, because the documents that are available to the public are in English language, while the public document extracts for the Flamanville 3 (FA3) EPR project are available in French. As explained in other sections of this report, it had proved more effective to agree on a representative I&C architecture for the purpose of the SMARTEST2 R&D investigation.

For some investigations by the partners, more detailed resources were required, partially similar to the resources that are not available to the public put presented on demand e.g., for evaluation by the Office for Nuclear Regulation (ONR) in UK. In order to avoid any licensing or non-disclosure issues, the provided source code examples contained mainly source code generated by code generators for simulation environments. Such code sections were e.g., provided to the SMARTEST2-FAU partner as one basis to investigate the code complexity, the possibility of buffer overflow vulnerabilities or unsecure handling of character strings. The provided source codes examples were not complete programs and accordingly they could not be compiled into executable programs without extensions by the project partner.

Note: The source code generators that come for example, with the TELEPERM XS platform, generate e.g., ANSI C source code (by using only a subset of the programming language, in accordance with strict programming guidelines, as mandated by the tools section of IEC 60880 [9] for Cat. A software). This source code is mostly static and contains many constant initialization parts and no dynamic heap allocation for the embedded software. This is possible, as the source code is generated based on semi-formal graphical specifications of interconnected functional diagrams and function blocks that are not changed during plant operation. Accordingly, additional source code from non-official (but representative) simulation examples were provided to the project partners on demand. Software in line with IEC 62138 [10] has to meet less stringent requirements. In order to meet IEC 62138 Cat. C software requirements especially, solutions based on off-the-shelf industry software can be leveraged. These topics were discussed with project partners at different meetings in order to explain the restricted nuclear context.

The university partners provided consulting guidance based on lectures for graduate students and workshops for industry partners (as are held regularly by OVGU University, especially for the automotive domain). For example, the network tap devices for use with RJ45 Ethernet interfaces with up to 100 Mbit/s bandwidth were purchased on recommendation of OVGU, where such network taps were already in use.

Regular joint workshops at different partner facilities, teleconferences and some joint conference were organized as part of the SMARTEST2 project.

Cooperation with further university partners

Due to the number of PhD candidates involved in the FRAMATOME-FRA project part, there was a need for having further German universities with security related departments involved in the mentoring of the PhD candidates. This was achieved by support of the University of Siegen, Friedrich-Alexander-University Erlangen-Nuremberg, the University of Bielefeld and the Technical University of Munich. This support was in parallel to the SMARTEST2 project execution, as the SMARTEST

project had already started when the cooperation between Framatome GmbH and these universities commenced for individual PhD candidates. The relatively early cooperation assured that only outstanding PhD candidates, with appropriate skills as considered by both, Framatome and the university partner, were accepted.

This cooperation with further university partners was also beneficial due to the consideration of technology and solutions available at the respective departments and due to recommendations on newest articles by the respective professors. However, while we are very grateful for this support, in this report, these consulting contributions will be considered only implicitly, via the results coming from the mentored PhD candidates participating in SMARTEST-FRA.

Project staffing and project organization

Figure 11 provides an overview of the SMARTEST-FRA R&D project organization

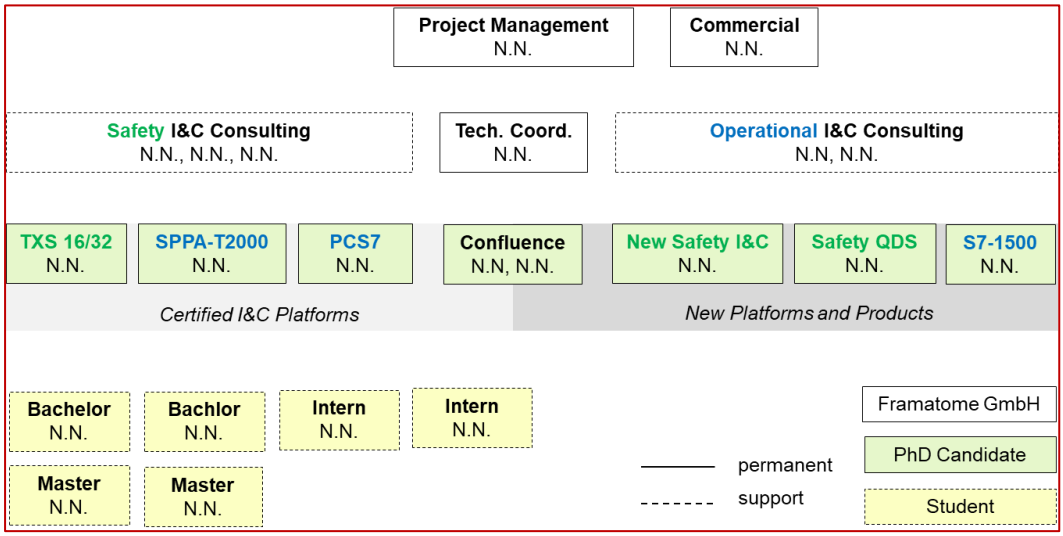

Figure 11. SMARTEST2-FRA R&D project organization.

Except for the PhD candidates, all other staff members indicated in Figure 11 were not working full-time on the SMARTEST2-FRA R&D project. While the Technical Coordinator worked mainly on SMARTEST2, the further selected Framatome GmbH subject matter experts were happily providing focused consulting on demand for Safety I&C platforms and Operational I&C platforms.

The Bachelor, Master and Intern students indicated in Figure 11 were supporting the PhD candidates in achieving faster progress towards the implementation of parts of the tools described in the planning section.

Note: The Bachelor, Master and Intern students were funded by two Framatome departments and were not covered by the SMARTEST2-FRA budget. To some

extent this provided more momentum towards the implementation of the SMARTEST2-FRA part.

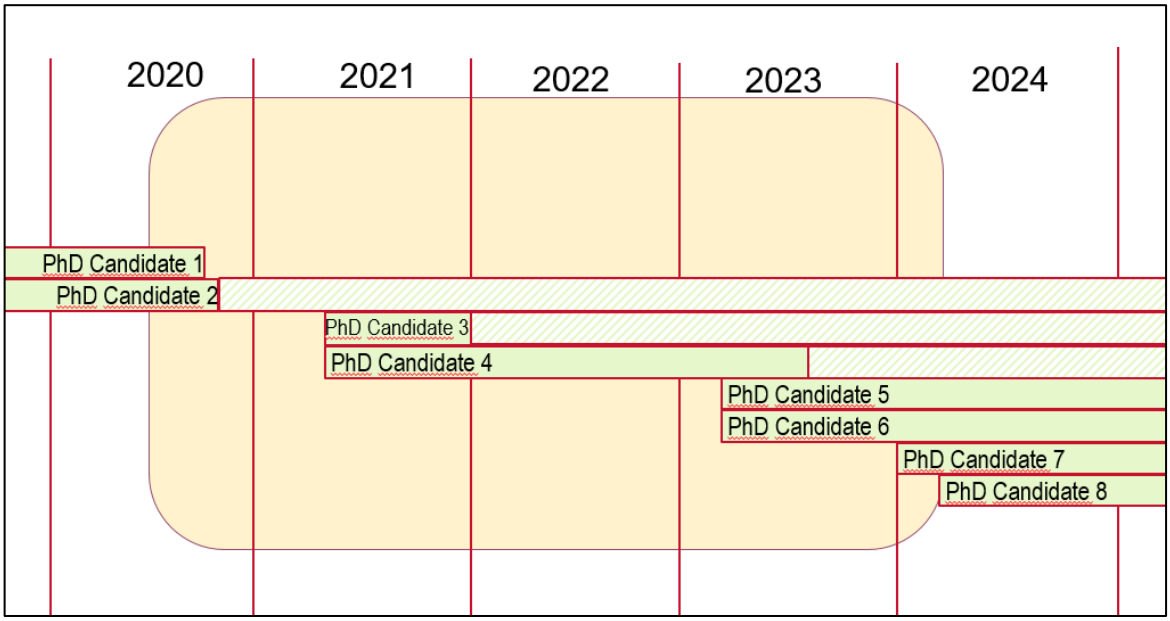

Figure 12. Gradual hiring of PhD Candidates for SMARTEST-FRA

As indicated in Figure 12, Framatome gradually hired the agreed number of PhD students. Each PhD student performed research on an assigned platform and/or the “confluence” topic, indicated at the center of Figure 11. The “confluence” topic is the basis for the tool based semi-formal approach of SMARTEST2. As each I&C platform has its own set of proprietary tools (diagram editors, simulation environments, and so forth) that are not suited for interoperability with the tools and frameworks from other platform, an abstraction layer which focuses on the security assets and the related assets is needed. Accordingly, the PhD students working on the “confluence” part of the project are also supporting the platform specific parts, as it is necessary to represent the key aspect of each platform in a confluent representation.

With regards to the project staffing, the following list provides an overview of the initial background of the PhD candidates involved in the SMARTEST-FRA project.

PhD candidate 1 holds a Bachelor in Electronic Information Engineering and A Masters in Electronic Engineering in Chang'an University in China. After contributing to SMARTEST and a few months to SMARTEST2, the candidate was focusing on a novel formal cybersecurity analysis approach on safety-critical systems, which take Siemens S7-1500 PLCs as main controllers for one year at safety I&C and cybersecurity project at a German university, before completing the PhD with a Dr.-Ing. degree (Summa Cum Laude grade).

PhD candidate 2 holds a master of engineering degree in industrial informatics from the National school of electronics and telecommunication in Tunisia. The previous studies combined automation, programming and AI as technical topics.

Currently working on security engineering and analysis for safety-related end-user interfaces in critical infrastructures. This PhD candidate was hired by Framatome GmbH in October 2020 and continued to support the SMARTEST2 project, including for the preparation of this final R&D report.

PhD candidate 3 switched from the DECENT R&D to the SMARTEST2 R&D in 2021 Q2, was hired by Framatome GmbH beginning of 2022 and continued to support the SMARTEST2 project, including for the preparation of this final R&D report.

PhD candidate 4 switched from the DECENT R&D to the SMARTEST2 R&D in 2021 Q2, was hired by Framatome GmbH in 2023 and continued to support the SMARTEST2 project, including for the preparation of this final R&D report.

PhD candidate 5 holds dual master's degrees in Telecommunications (network security) and in Informatics respectively from the National School of Electronics and Telecommunications in Tunisia and the Deutsch-Französische Hochschule Multimedia Distributed Pervasive Secure Systems PhD-Track Program (INSA Lyon-University Passau). The doctoral thesis, which began in March 2023, was interrupted due to visa issues and resumed in 2024. Research focuses on joint consideration of 3rd generation Safety and Security, cybersecurity testing, and AI-based risk management. She also supported the preparation of this final R&D report.

PhD candidate 6 holds a Bachelor of Science in Combined Mathematics and Computer Science and a Master of Science in Computer Network and Distributed Services. Throughout the project, he has focused on developing a monitoring and anomaly detection system, implementing data collection processes from the S7 1500 PLC, and enhancing the display of monitoring results on the TP2200 HMI. This research applies advanced computational and network principles to real-world systems, setting a strong foundation for innovative contributions in the field of system monitoring and anomaly detection.

PhD candidate 7 holds a Bachelor of Electrical and Electronics Engineering (Control) from the University of East London and a Master's of Science degree in Information Systems. The doctoral thesis of PhD candidate 7 was supposed to begin in 2023 but due to visa issues started in January 2024.

PhD candidate 8 holds a master degree of science in Artificial intelligence and software from ewha womans university in south korea. After master degree, the candidate had a work experience in a Korean company for two years, working as an AI researcher, mostly focusing on developing AI guidelines and standards for AI in healthcare, recruitment, autonomous and general AI. Currently the PhD candidate is supporting other R&D projects within the company.

Note: As some of the PhD candidates started late in the SMARTEST2 R&D, they are ideally positioned for supporting R&D in a follow-up project.

Dissemination of results

During each year of the SMARTEST2 project execution, several papers were submitted to different international conferences, as can be seen from the list of own publications, which includes papers jointly prepared by two or three project partners. The IAEA cybersecurity activities substantially increased over the last years, both with regards to cybersecurity specific conferences and tracks on cybersecurity as part of major nuclear safety and security conferences. Furthermore, as compared to the initial planning, more papers were submitted in the context of the annual “Gesellschaft für Informatik” (GI) conferences as these include a workshop track on Industrial Automation and Control Systems and participation at the conferences is cost-effective, as they are held in Germany mostly. Similarly, a paper was submitted in the nuclear specific International Conference on Nuclear Engineering (ICONE), in Japan 2019 . ICONE is the leading global conference on nuclear reactor technology. The Japan Society of Mechanical Engineers (JSME), American Society of Mechanical Engineering (ASME) and Chinese Nuclear Society (CNS) are the main organizers of ICONE. Over the years, they have also adopted the sessions for cybersecurity in nuclear specific domain in the conference.

Framatome GmbH participates actively in consultancy and technical meeting organized by the IAEA, where some of the following topics are addressed:

- addressing the design and application of computer security controls to I&C systems at nuclear power plants (NPPs);
- discussing other collaborating organizations efforts on computer security for I&C systems at NPPs; and
- supporting the IAEA in defining future activities in the field of secure system designs for I&C systems at NPPs.

Framatome assisted in the delivery of the presentation entitled “Development of a new IEC Standard on Cybersecurity Controls for I&C in Nuclear Power Plants - IEC 63096 (SUPPLY CHAIN ASPECTS)”. Here, we shared the efforts of the SMARTEST and SMARTEST2 R&D project, as a contribution to deploying advanced testing techniques to assure secure systems along the supply chain.

Exploitation of results

Typically, the results of an R&D project are towards the dissemination, the contribution to standardization and the industrial or institutional exploitation. Accordingly, for Framatome, the project implementation must assure that the results can be deployed in the relevant industry domain. As indicated in the project plan section, the targeted Technology Readiness Level is TLR 4 to TLR 5 on a scale from 1 to 9. Accordingly, no direct market readiness is intended, but instead, a solid foundation for further research and finally applicable concepts, procedures

and tools. Additionally, one major benefit for all staff involved in the project implementation is their more in-depth understanding of cybersecurity aspects of key I&C platforms deployed in the nuclear domain, as well as the proficiency in some of the most advanced security testing techniques. This expertise is beneficial as augmentation and support to all NPP units that have their local cybersecurity staff in place, but cannot afford in-depth specialists for each platform or for specific testing techniques. This is in line with the assumption that “security is a process not a product” [11].

6. Science and technology state-of-the art related to security testing in 2020

6.1. 2018 state of science and technology according to standardization efforts

The ISO/IEC 27000-series known as the ISMS family entitled “Information technology — Security techniques — Information security management systems — Overview and vocabulary”, supports organizations in securing information assets. The series contain information security standards published jointly by the International Organization for Standardization (ISO) and the International Electro Technical Commission (IEC). Bringing information security intentionally under management control constitutes a key principle in the ISO/IEC 27000 standards. ISO/IEC 27001 is the well-known standard in the family, offering requirements for an information security management system (ISMS). Published in September 2013, it replaces ISO/IEC 27001:2005, assisting small, medium and large businesses in different sector securing their information assets. An ISMS is a precise method for managing and securing sensitive company information; it is a management system comparable to those recommended by other ISO standards, such as ISO 9000 and ISO 14000. It takes account of people, processes and IT systems by applying a risk management process. The standard primarily defines the purpose of an ISMS deployed in order to manage information security risks and controls within an organization. On the other hand, ISO/IEC 27002 offers best practice recommendations on information security management responsible for initiating, implementing or maintaining ISMS, and is used as a reference for deciding on controls within the process of implementing an ISMS based on ISO/IEC 27001. Information security is defined within the standard in the context of the C-I-A (Confidentiality –Integrity-Availability) triad.

ISO/IEC/IEEE 29119-4:2015 “Software and systems engineering -- Software testing -- Part 4: Test techniques” was published in December 2015. It defines test design techniques that can be used during the test design and implementation process that is defined in ISO/IEC/IEEE 29119-2. ISO/IEC/IEEE 29119-4:2015 is intended for, but not limited to, testers, test managers, and developers, particularly those responsible for managing and implementing software testing.

ISO/IEC/IEEE 29119-5:2016 “Software and systems engineering -- Software testing -- Part 5: Keyword-Driven Testing” was published in November 2016. ISO/IEC/IEEE 29119-5:2016 defines an efficient and consistent solution for Keyword-Driven Testing by:

- providing a reference approach to implement Keyword-Driven Testing;
- defining requirements on frameworks for Keyword-Driven Testing to enable sharing of test cases, test data, keywords, or complete test specifications;
- defining requirements for tools that support Keyword-Driven Testing (e.g., test automation, test design and test management tools);

- defining interfaces and a common data exchange format to ensure that tools from different vendors can exchange their data (e.g., test cases, test data and test results);
- defining levels of hierarchical keywords, and advising the use of hierarchical keywords;
- providing an initial list of example generic technical (low-level) keywords, such as "inputData" or "checkValue" that can be used to specify test cases on a technical level.

Beyond the recommendations for some programming languages in [13], new languages, like TypeScript, are available that support avoiding and early detection of many error classes. TypeScript is described as a superset of JavaScript (or, JavaScript is a subset of TypeScript). The main contribution of TypeScript is its addition of (data) types, which provides static code analysis and improves code readability ad maintenance [17]. A major benefit of this is that it enables Integrated Development Environments (IDEs), such as Eclipse, to provide a richer environment for recognizing common errors as the code is being typed. For instance, the IDEs are able to use the TypeScript types descriptions to spot errors such as passing a numeric type to an Object constructor function and to infer types which are not explicitly declared. TypeScript also facilitates easier code debugging to uncover code errors before the final application is executed. The overall result is the development and deployment of more robust software.

The introduction to the draft standard of ISO/IEC 27019:2017 [16] from November 2017 states:

"At the focus of application of this document are the systems and networks for controlling and supervising the generation, transmission and distribution of electric power, gas and heat in combination with the control of facilitating processes. This includes control and automation systems, protection and safety systems and measurement systems, including their associated communications and telecontrol applications."

Information security management presents fundamentally the same risk management challenges in all contexts, but the real-time nature of process control systems and the safety and environmental criticality make some of the challenges particularly extreme for organizations in the energy industry. The standard therefore provides additional, more specific guidance on information security management than the generic advice provided by ISO/IEC 27002, tailored to the specific context of process control systems used by the energy utility industry for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, gas, oil and heat, and for the control of associated supporting processes.

IEC 62859:2016 "Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity" was published. This standard specifically focuses on the issue of requirements for coordinating safety

and cybersecurity provisions for I&C programmable digital systems and architectures. It defines both generic principles and guidance for practical situations to integrate cybersecurity requirements in nuclear I&C architectures and systems, fundamentally tailored for safety. Technical, as well as conceptual, organizational and procedural aspects, is covered. It is intended that this standard be used by designers and operators of NPPs (utilities), systems evaluators, vendors and subcontractors, and by licensors.

IAEA is working on publishing NST 45 (ongoing) and NST 47 (ongoing), while IAEA Nuclear Security Series (NSS) 33-T [18] was published mid-2018.

ISO/IEC 27021:2017 “Information technology -- Security techniques -- Competence requirements for information security management systems professionals” The new ISO/IEC 27021:2017 provides a list of knowledge and skills professionals must acquire in relation to the topic of IT security according to their specific tasks. The required competences include the understanding of IT security frameworks, regulations and standards as well as the ability to implement them. Professionals shall be able to determine the security risks and put in place processes capable to treat such risks.

Professionals shall have the competences to perform monitoring, measurement (metrics), analysis, evaluation and (internal and external) auditing. Since maintaining a continual improvement process and keeping up with technological improvements is crucial, skills for balancing the benefits of corrective actions against effort, analyzing the operations impacts of emerging technologies, etc. shall be acquired.

New IEC 62443-x-x parts (published 2016 or later) are a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.

6.2. 2018/2019 State of science and technology according to publications

The references section contains several indications of publications from 2016 to 2018/2019. These will not be repeated here. The number of publications and the broad list of topics addressed by the publications shows that still a lot of development is going on in the critical infrastructure security domain and in the nuclear cybersecurity domain.

6.3. 2018/2019 State-of-the-art of commercial products

As mentioned in previous sections, the project adopts a “smart” testing approach in its security analysis of the selected I&C systems. In this sense, the intention is not to bombard these systems with brute force testing to uncover vulnerabilities. Instead, intelligent and purpose-driven attack scenarios are designed to achieve

specific outcomes (e.g., buffer-overflow, Denial-of-Service (DoS), and so forth). As a part of this effort, the SMARTEST project employs the use of tools and methodologies that follow similar smart analysis, for example, Synopsys® Defensics® for fuzz-testing.

Synopsys® Defensics® is observed as a fuzzing solution that follows the smart fuzzing approach. It is described as a multi-protocol, environment-variable smart fuzzer that can understand the overall system and test individual elements dynamically [19] [20] [21]. The Defensics® engine provides a comprehensive, powerful, and automated black box solution that enables organizations to effectively and efficiently discover and remediate security weaknesses in software. By taking a systematic and intelligent approach to negative testing, Synopsys® Fuzz Testing allows organizations to ensure software security without compromising on product innovation, increasing time to market or inflating operational costs [22]. The Defensics® engine is programmed with knowledge on input type, whether it is an interface, protocol or file format. Because the engine has a deep understanding of the rules that govern communication within the input type, it can deliver targeted test cases that exploit that input type's inherent security weaknesses. Defensics® offers advanced test suites for 250+ standard network protocols, file formats, and other interfaces, and provides a Software Development Kit (SDK) that allows users to develop their own test suites (hereon referred to as custom suites) [22].

There are similarly highly competitive smart fuzzing solutions, such as beSTORM® by Beyond Security® and Peach Fuzz® from PeachTech®. A comparative analysis of beSTORM and Defensics® is given in [23], where it is highlighted that for the various fuzz-testing needs, beSTORM® is the favorite solution. This report goes on to state that beSTORM® can be used against a wider variety of test targets than Defensics®, and that the beSTORM test cases number in the thousands to billions per protocol and that users can extend these with their own custom test cases and attack vectors. In [24], PeachTech® also highlights the advantages of Peach Fuzz® in comparison to Defensics®. Noteworthy statements from this report include where it is declared that the fuzzing engine of Peach Fuzz® contains over 60 mutation algorithms that can generate millions of intelligent test cases, and that Peach Fuzz® is product life-cycle-aware, which allows it to integrate with a target at different stages of its life cycle development [24].

7. Science and technology state-of-the art related to security testing in 2024

7.1. 2024 state of science and technology according to standardization efforts

The IAEA Nuclear Security Series No. 17 () “Computer Security at Nuclear Facilities “provides comprehensive guidance on computer security measures for nuclear facilities. The NSS 17 document outlines various methodologies to safeguard against cyber-attacks, including penetration testing, fuzz testing, and denial-of-service attacks. It emphasizes the importance of continuous monitoring, updating security protocols, and ensuring that all components of the nuclear facility's digital infrastructure are resilient against potential cyber threats.

A major evolution since the IAEA NSS No.17-T, Computer Security at Nuclear Facilities was revised in 2021. With interfaces with the State/CA (NSS 42-G) and I&C (NSS 33-T) previously published, revision IAEA NSS No.17-T.2021 “Computer Security Techniques for Nuclear Facilities” [25] follows the lifecycle of facility and provides guidance on CS Risk Management Program (facility & systems), Defensive Computer Security Levels and Zones and Policies and Procedure. The released technical guidance applies to the implementation and management of computer security for nuclear security purposes by addressing all digital assets associated with a nuclear facility, including the facility’s I&C systems. Thus, additional guidance on specific computer security considerations for the facility’s I&C systems that provide safety, security or auxiliary functions is provided.

The new parts of the IEC 62443-x-x series, published from 2016 onwards, provide standards, technical reports, and related information on electronically securing Industrial Automation and Control Systems (IACS). These documents offer detailed procedures and guidelines for various stakeholders involved in the IACS value chain. Recent revisions include updates to existing standards to address new cybersecurity threats and technologies.

- 62443-2-4” Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers” specifies a comprehensive set of requirements for security-related processes that IACS service providers can offer to the asset owner during integration and maintenance. The 2023 update to IEC 62443-2-4 focuses on enhancing the cybersecurity requirements for Industrial Automation and Control Systems (IACS) service providers [26]. Key additions include Enhanced Security Program Requirements, Lifecycle Security, Alignment with Latest Standards. These updates aim to improve the overall security and resilience of IACS environments.
- 62443-3-3 “Security for industrial automation and control systems – Part 3-3: System Security Requirements and Security Levels” provide detailed technical security requirements for IACS systems, in order to protect them against cybersecurity threats. An official German version is adopted as DIN EN IEC 62443-3-3:2020-01, also known

as VDE 0802-3-3:2020. This version aligns with the IEC 62443-3-3:2013 and includes corrigenda and amendments to ensure up-to-date guidelines on IT security for industrial networks [27]. The national versions ensure that the global standards set by the IEC are localized to meet specific regional requirements and are available in various languages, facilitating broader accessibility and implementation.

The IEC 62541 standardize the OPC Unified Architecture (OPC UA), an essential protocol for modern industrial automation. This series of standards defines in detail the fundamental concepts, address space model, information model, server services, protocol mappings, standardized profiles and security mechanisms. OPC UA facilitates interoperability between various industrial systems and equipment, enabling secure and reliable communication. It specifies flexible data models, advanced services such as data read/write, and robust security features to protect sensitive information. By standardizing these aspects, OPC UA contributes to operational efficiency, simplified system management, and reduced development and maintenance costs. These standards are crucial to industry, guaranteeing robust and secure communications, thus meeting the growing demands for connectivity and security in advanced industrial automation environments.

The standards saw a series of significant updates in 2020 and 2021 declined in 14 parts. Part 14 (IEC 62541-14:2020) specifies the OPC Unified Architecture (OPC UA) PubSub communication model. It outlines an OPC UA publish-subscribe (PubSub) pattern that enhances the client-server model described in IEC 62541-4 Services. PubSub enables the dissemination of data and events from an OPC UA information source to interested parties within a device network as well as to IT and analytics cloud systems. IEC TR 62541-1 provides a comprehensive overview of both models (IEC 62541-14 vs IEC 62541- 4) and their unique applications [28].

The Common Criteria (CC) Framework, application of ISO/IEC 15408, has recently undergone the first major revision in 2022 since Version 3.1 Release 5 [29]. The latest version involves modifications in three key areas: the introduction and general model, security functional requirements, and security assurance requirements. Thus it now consists of five parts to address various aspects of IT security evaluation comprehensively, enhancing cybersecurity and privacy protection. These updates ensure that the criteria remain relevant and effective for evaluating the security features and capabilities of IT products on a global scale (Corsec Security, Inc.®) (Common Criteria Portal).

Additionally, the European Union Agency for Cybersecurity (ENISA) has introduced the European Cybersecurity Certification Scheme on Common Criteria (EUCC) [30]. This scheme, adopted in early 2024, is based on the existing Common Criteria framework and aims to unify and elevate the cybersecurity standards across EU member states. It provides a structured and voluntary assessment process for ICT products, allowing suppliers to demonstrate compliance with EU-wide cybersecurity standards (ENISA).

7.2. 2024 State of science and technology according to publications

The references section contains several indications of publications from 2016 to 2024. These will not be repeated here. The number of publications and the broad list of topics addressed by the publications shows that still a lot of development is going on in the critical infrastructure security domain and in the nuclear cybersecurity domain.

8. Cooperation with partners

There is an ongoing exchange with the partners of the SYNTHESIS R&D project that started in 2020, also targeting the nuclear domain. There is still ongoing international exchange with the former partners of the European funded IAEA Coordinated Research Projects (CRP) on Enhancing Computer Security Incident Analysis at Nuclear Facilities (IAEA CRP J02008). Cooperation with some of the former IAEA CRP J02008 partners in the context of a new IAEA CRP, related to cybersecurity for Small Modular Reactors (SMRs), is currently being investigated. Cooperation with several German university partners was and is ongoing based on mentored PhD candidates or currently ongoing Master/Bachelor thesis.

9. I&C test platforms and security test tools

FRA TELEPERM XS

TELEPERM XS is Framatome's I&C platform which is eligible for safety-critical systems used in nuclear power plants (NPPs) [31].

The platform is suitable for new plants, as well as for the upgrading and modernization of existing NPPs of virtually all types and from all main suppliers. The first TELEPERM XS systems were put into operation more than ten years ago, and have been working very reliably ever since [31].

Redundant design can be implemented with TELEPERM XS system to achieve a very high reliability required by nuclear facilities. The hardware production of TELERPERM XS system is monitored and managed by Framatome. In Germany, TELEPERM XS cabinets will be installed and tested within its test-bay in Erlangen before delivery to customers.

The software tools developed for TELEPERM XS software provide an integrated environment for design, simulation, code generation and system maintenance. Together with project management tools suggested by Framatome, the full life-cycle management of safety-critical system from design to operations guarantees the compliance to strictest nuclear safety/security standards.

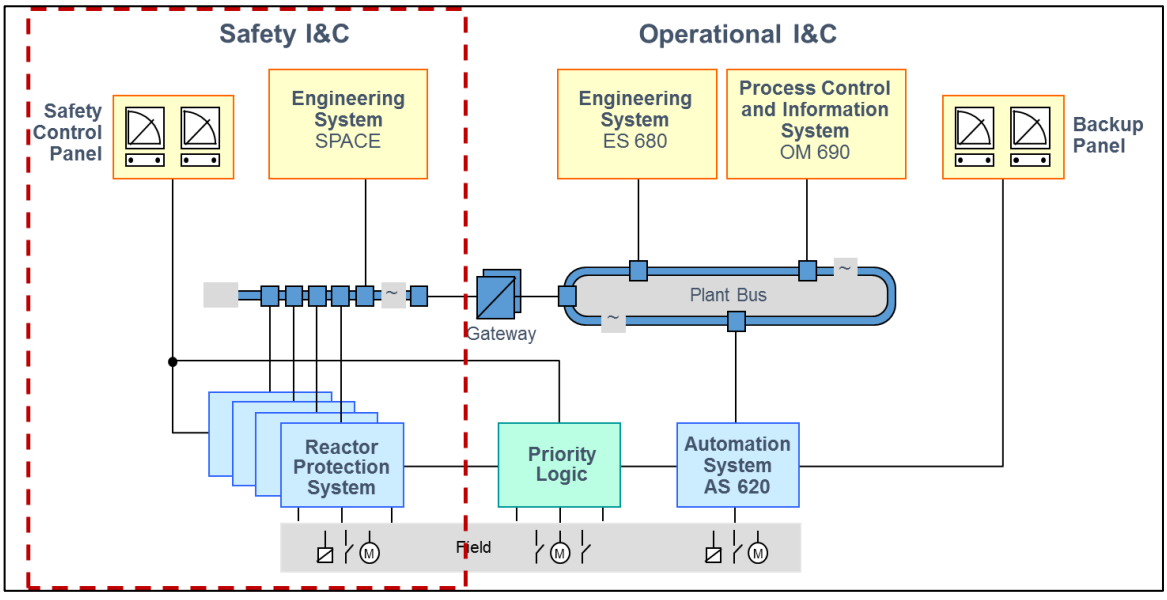

Figure 13. Simplified Example of Safety I&C for Nuclear [31]

As part of the SMARTEST2 R&D budget a single TXS SPCGS rack containing a TELEPERM XS Service Unit (TXS SU) and a TELEPERM XS Gateway (TXS GW) were purchased at the beginning of the project. This safety I&C hardware is used for hardware in the loop tests, where parts that are not available in the Cybersecurity Lab are simulated in real-time. This hardware in the Cybersecurity Lab is also used for porting and checking cybersecurity results from one TXS Core Software version to a subsequent version,

especially when the tests showed that the layout of messages at the ISO/OSI application layer changed.

Siemens PCS7-400

PCS7 is a current generation automation system for process industry from SIEMENS. Standard components include PC, controller, communication and distributed peripherals. It is used in process industries such as chemical industry, pharmaceutical industry and food industry for the management of the main production process, but also for side, upstream or downstream processes such wastewater treatment and energy distribution. It also delivers data to higher-level ERP systems [32].

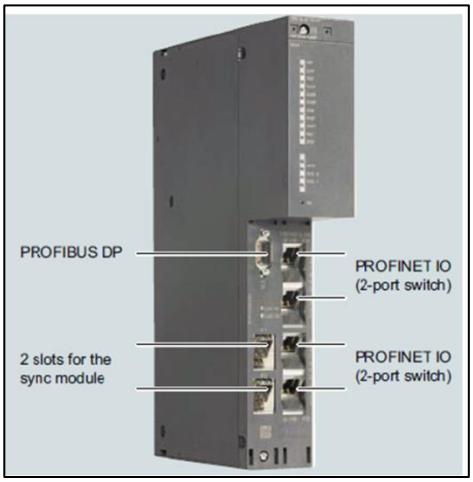

Figure 14. Siemens PCS7 – 400 [32]

PCS7 is not deployed for the highest Safety Category (Cat. A according to IEC 61226) or highest Security Degree (S1, according to IEC 62645).

SPPA –T2000

SPPA-T2000, is an industrial automation platform of SIEMENS for operational I&C applications. The initial name of this platform was TELEPERM XP, with X indicating “eXtensible”, similarly to the X in “XS” from TELEPERM XS, and “P” indicating “Production”, as opposed to “S” in “XS” which indicates Safety. After rebranding the brand ownership was transferred from Siemens AG to Siemens Energy AG and continues to be further maintanined and developed for new operation I&C projects in the nuclear domain. SPPA-T2000 is a universal control system used in power plants since 1994. This platform monitors and controls process parameters like flows, levels, temperatures, pressures, reactor coolant pumps status etc. SPPA platform, based on SIMATIC S5/S7, is composed of automation system, operation and monitoring system, engineering system, diagnostics system, and plant bus.

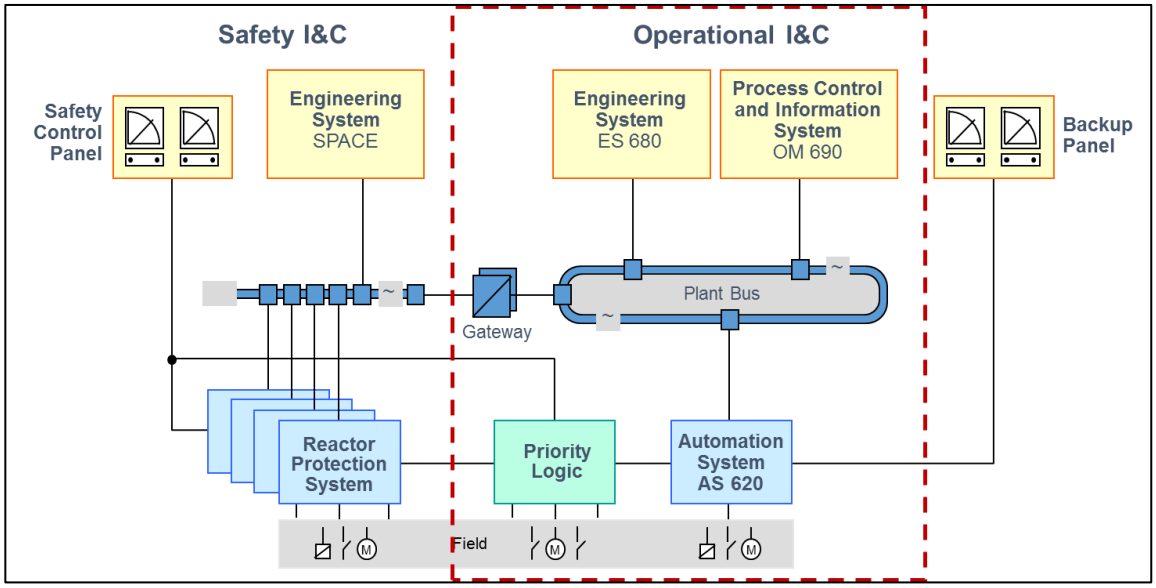

Figure 15. Simplified Example of Operational I&C for Nuclear [31]

As can be seen along the left and bottom dotted lines, there always specific hardware and software based solutions for interfacing from the Safety I&C to the Operational I&C. The interface along the vertical line, i.e. for the exchange of analog and binary signals was specifically addressed in WP AP4.2 with regard to hardware based solutions (data diodes).

Note: The “Priority Logic” hardware modules were not addressed in the SMARTEST2 R&D as this topic was not included in the SMARTEST or SMARTEST2 R&D scope.

Siemens S7-1500

The Siemens SIMATIC S7-1500 PLC is used for controlling critical processes, such as those found in water supply systems, power plants, gas and oil refineries, and other critical industries. As with other I&C systems, PLCs are built to achieve high performance requirements, at the risk of security [33]. This further compounds its already vulnerable position, as by virtue of its role, it is already a prime target for attacks.

As a part of the initial design phase and also due to post-production attacks, the S7-1500 PLC has been outfitted with various security controls. According to Siemens, the S7-1500 PLCs offer “*an improved security concept of protection levels and block protection all the way to communication integrity*” [33]. These controls include:

- SIMATIC Logon
- Deactivation of services
- Deactivation of hardware interfaces
- Robust communication
- Password protection
- Know-how protection against unauthorized access
- Copy protection

Like several other I&C systems, the Siemens SIMATIC S7-1500 uses PROFINET to communicate with systems on its network. The following is a list of the protocols in the PROFINET suite:

- PROFINET/CBA - Component Based Automation
- PROFINET/DCP - Discovery and basic Configuration Protocol
- PROFINET/MRP - Media Redundancy Protocol
- PROFINET/MRRT - Media Redundancy for PROFINET/RT
- PROFINET/PTCP - Precision Time Control Protocol
- PROFINET/RT - Real-Time
- PROFINET/IRT - Isochronous Real-Time
- TCP/IP - Transmission Control Protocol/Internet Protocol

Siemens further uses the S7Comm protocol, which is a proprietary protocol that runs between PLCs of the Siemens S7 family. The S7Comm suite consists of the following protocols [33]:

- COTP - Connection-Oriented Transport Protocol
- TPKT - Transport Packet
- TCP – Transmission Control Protocol

The main features of the S7Comm are:

- Configuration of the PLC
- Starting and stopping the PLC
- Reading and writing process variables
- Program transfer (upload/download)
- Debugging
- Providing debugging information
- Alerting

Both PROFINET and S7Comm are used in conducting administrative level tasks on the S7-1500 PLC, however, S7Comm facilitates tasks at a higher level of criticality and control. As such, the S7Comm is outfitted with integrated security controls to detect and prevent misuse. Similar protection is not observed with PROFINET. Nevertheless, the SMARTEST project considers both communication protocols in its security-testing. The results are discussed in later sections.

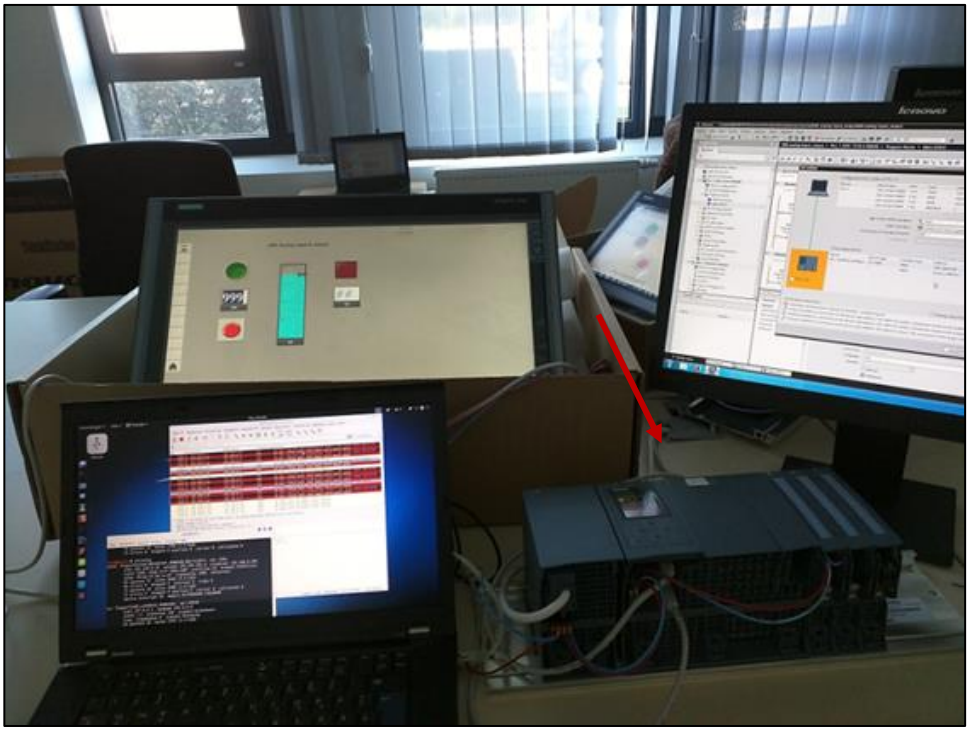

Figure 16. Example of S7-1500 Hardware in the Framatome Test Lab

Note: Representative S7-1500 hardware, as indicated in the bottom left of the above figure, was purchased as part of the SMARTEST R&D budget towards the middle of the SMARTEST R&D project execution. This hardware is still up-to-date for industrial applications, including for use of the newest Siemens Totally Integrated Automation (TIA) portal software.

FRA Safety I&C – 3rd Generation

TELEPERM® XS is Framatome's I&C system platform for safety I&C in the nuclear power plant. It comprises all the necessary hardware and software components, including the software tools required for engineering, testing and commissioning, operation and troubleshooting.

TELEPERM® XS is suitable for new plants as well as for the upgrading and modernization of existing nuclear power plants of virtually all types and from all main suppliers.

TELEPERM® XS is used for implementing various types of I&C systems in the nuclear power plant.

The main applications are:

- Reactor protection system/ESFAS
- Reactor control and reactor limitation systems
- Neutron flux measurement

- Core monitoring
- Rod position monitoring
- Emergency diesel generator control

Qualified Display System

The Qualified Display System (QDS) is a Human System Interface suitable for safety I&C systems in a nuclear power plant [34].

QDS (Figure 17) is a qualified display unit connected to one or several (up to 4) TELEPERM XS (TXS) units. It has been designed as a safety classified screen-based interface for the main control room operators, for use in back fitting projects as well as in new plant application.

The main operational features of the QDS are [34]:

- To provide to the operator a user friendly interface for real-time display of values of TXS signals or for manual controls
- Engineering tools allow the customer to design and create its own HMI and maintenance tools provide means for monitoring the QDS.

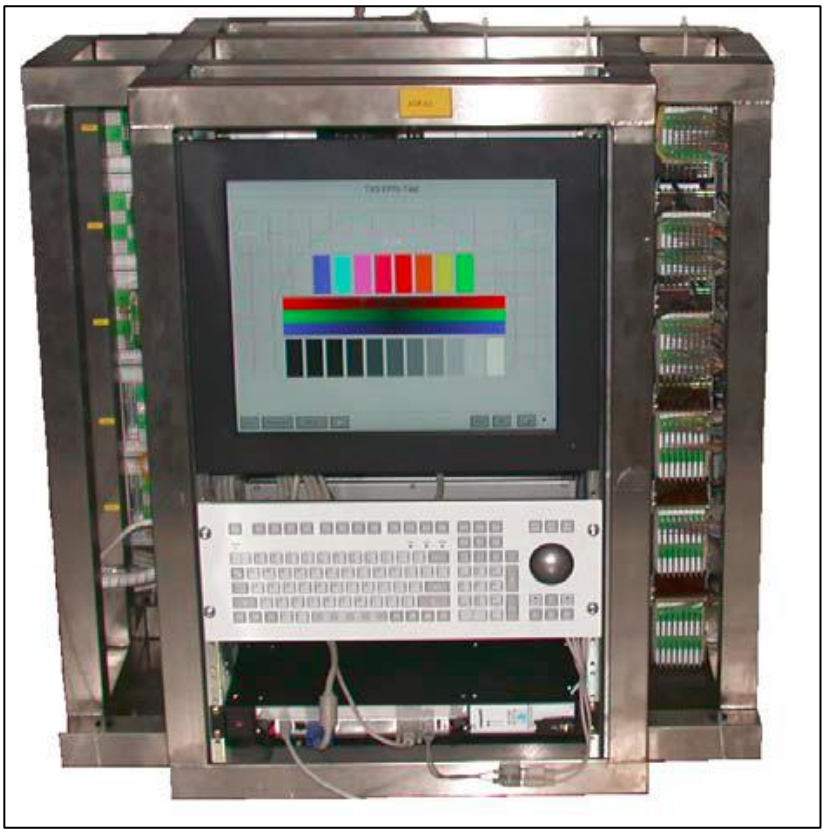

Figure 17. Example of 1st Generation Qualified Display System (QDS) [34]

Possible fuzzing methods include [21]:

- Random (simplest and least effective) - usually ineffective because the test cases are nothing like valid input, and mostly fail to penetrate the target code, as the target system quickly rejects these invalid inputs.
- Template (also known as block or mutational fuzzing) - provides slight alterations, iterating a predetermined number of errors has been uncovered. Although the use of slight iterations has the potential to discover, this process is typically slow and its narrow focus can also result in some vulnerabilities being missed altogether.
- Generational (model-based fuzzing) - simulates randomness, but is designed to adhere to standard definitions that govern the target element (protocol, file format, etc.). In that the malformed inputs are generated based on the original parameters of the protocol or API and so forth. This method reduces wasted efforts whilst ensuring a controlled scope that is wide enough to have far-reach effect in uncovering vulnerabilities.

TXS Compact

TELEPERM XS Compact is an automation system based on FPGA technology that can be used with different modules from the TELEPERM XS portfolio for e.g. signal conditioning, TXS cabinet and installation infrastructure, power supply, etc. to implement safety I&C systems able to fulfill highest requirements of safety-related I&C systems in nuclear power plants. TELEPERM XS Compact offers a wide range of function block types that can be easily combined to implement typical NPP I&C functional requirements and safety functions. Safety I&C solutions on TELEPERM XS Compact contain no CPU and no software, but are entirely operated on configurable hardware logics in the FPGA and memory cells.

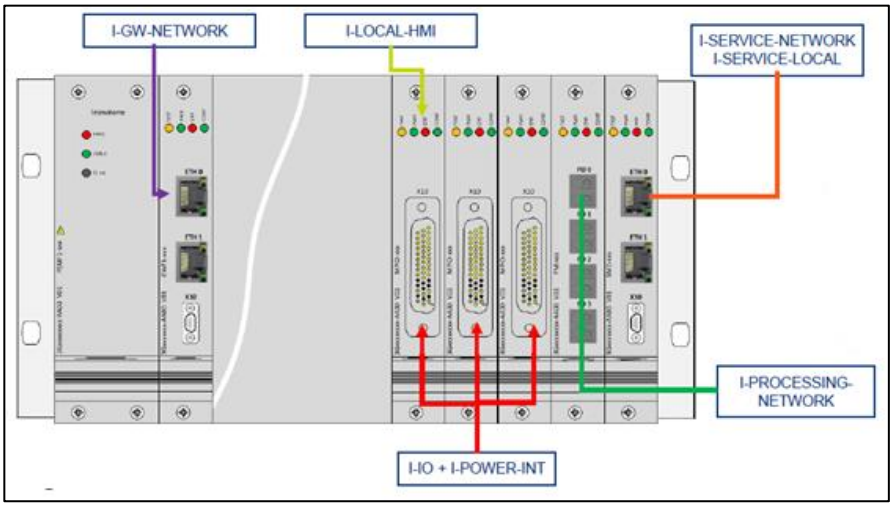

Figure 18. TXS Compact Sub-rack

TELEPERM XS Compact acts as a diverse automation platform, compared to TELEPERM XS Main Line CPU-based devices (such as SVE2/SVE3 application function processor).

TELEPERM XS Compact enables the development of class 1 safety I&C systems according to IEC standards (IEC 61513, IEC 62566, IEC 60987; etc.) and to the system needs and functional requirements. Further details about the Platform are provided in the user manual [35].

10. Execution of the security testing research / procedure of the experiments or analyzes

10.1. Analytical

Identifying cybersecurity vulnerabilities before SCADA systems are implemented is more practical than only conducting a cybersecurity analysis after the product has been deployed. In so doing, this has the potential to reduce cost and to provide high resistance against subsequent security events. As is the typical case, developers are more concerned about functions, giving comparatively less attention to security concerns, in designing SCADA systems. However, the importance of security issues and their influence were reverberated by targeted, advanced and increasingly frequent cyberattacks in recent times, where significant attacks include Stuxnet [3], Dragonfly, Trisis [37], CRASHOVERRIDE [38], etc.

Thus, it is urgent and necessary to have a systematical and reliable approach towards the analysis of potential cybersecurity issues, from the system design stage. In this effort, a novel formal cybersecurity analysis approach is developed, which involves reverse engineering and requirement engineering technology. Fault tree analysis is also considered to partly support the analysis.

Before developing attack models and doing security tests, it is necessary to analysis the places that where potential attacks may happen. This helps researchers to develop more efficient attack models and test schemes. In this part, we give a brief introduction of a formal cybersecurity analysis approach, to assist following attack model and security test research.

The analysis approach includes several steps:

1. **Know the research object**. We believe that know our system (research object) is a foundation to research its vulnerabilities. Formal specification is a logical way to achieve this goal [39], thus, the formal specification should be the achievement in this step.
2. **Ensure the formal specification is correct and is relatively complement for further analysis**. In this part, we develop a novel way to prove it is correct and relatively complementary. This approach combines the Artificial Intelligence (AI) planning technique, use PDDL (Planning Domain Definition Language) [40] as input language, for detail information, see reference [41].
3. **The real analysis work will start after previous two steps**. Literatures, typical attacks will be considered as references. The FTA (Fault Tree Analysis) approach is partly considered. Attack traces are provided as achievements.
4. Finally, the attack traces are proved by a scientific way.

We develop this cybersecurity analysis approach based on an existing SCADA system (popularly used in NPPs). Namely, this is the S7 1500 PLC (see Figure 19). Potential vulnerabilities within the PLC and its networked systems are investigated.

Figure 19. Siemens S7 1500 controllers [33]

As we are not the designer of the controller, reverse engineering technology is considered to retrieve and analyze the system functions that are implemented based on the S7 controller. Part of the work and achievements in this reverse engineering part can be seen in [41] [42]. Artificial Intelligence (AI) planning method and tool are used to help the reverse engineering aspect to prove that the correct and complete system function description is retrieved.

The cybersecurity analysis part is formally carried out similarly with FTA. In the result of this analysis approach, not only the security weaknesses of system, is provided with formal analysis. Also provides is the feasibility, so that it can be referenced by future designers. This process is currently on-going.

10.2. Prototypes

Following the modelling work described in Section 3, a prototype is being developed for verifying the overall proposed methodologies and developed tool sets within selected attack scenarios. The prototype serves as the environment for threat modelling and system modelling. Based on that, test cases can be generated semi-automatically. With interfaces connecting to simulation environment or real I&C systems, the correspondent security model will be updated accordingly and used for testing identified attack patterns as proof of concepts (PoCs) as well as for simulating the result and impact of deployed security controls. The prototype is being developed as a web-like service using Angular JS. As mentioned before, the system architecture model will be implemented using AutomationML while involving additional standard data formats for storing different types of data. For example, PLCopen will be involved for describing control blocks while COLLADA will be used for describing physical security environment.

In the System Architecture Model part, the centric part is the identified assets with id. Their types will be also identified and referenced from an asset type library which we took several typical vendor-specific assets and modelled their security relevant features. The asset type library is expected to be extended in the future to cover most of applied assets. In addition, different aspects of the model will be implemented for describing the protected system while later enable the automatic generation of test cases and the simulation of attacks and controls. In the prototype, the network perspective will be implemented with the JavaScript library gojs, which enables the dynamic connection between assets while displaying the motion of data flows between them. The functional perspective will be implemented using formal specification in a table-like view with editing tool sets. The formal specification enables the simulation of

control impacts. For example, after deployed a Firewall with specific configurations, with in the prototype it can be simulated whether normal functions are affected. It is also expected that the simulation will be extended with the demonstration of physical (damage) results. For example, the affected space area of a robot arm, which loses the control, will be displayed and checked against safety requirements.

In the Security Model part, attack paths will be implemented based on the network perspective. A sequence of the whole attack will be demonstrated step by step over the network perspective implementation. The sequence of the attack will be also modelled using UML activity diagram so later it can be applied for behavior fuzzing (with/without content fuzzing together). In addition, for further abstracting similar attacking units, the tree-like data structure is introduced for storing, viewing and composing attack paths and controls. Based the attack tree, it is meaningful to think how to put basic attacks, like spoofing and eavesdropping. The tree view will be enhanced with triggering conditions for better demonstrate APT in the system. It can interactively to show how an attack happens.

In the Threat Model part, links to public security databases and descriptions are collected for general attacks. In addition, key assets / key words need to be highlighted for later filtering. Based on the general attacks, specific attacks will be developed against the target system. The links between specific attacks and its inspiration: general attacks will assist security expert to determine the likelihood as well as impacts of identified attacks. Furthermore, general attacks may be already associated with suggested security controls (mitigations). It is reasonable to develop specific security controls based on the best practice suggestions.

10.3. Extension of existing MSI fuzz testing framework

The *so-called* Monitoring and Service Interface (MSI) Barrier Test is a comprehensive fuzz testing suit, initially developed for ongoing Safety I&C platform tests.

In the context of the TELEPERM XS Safety I&C platform, the term MSI Barrier refers to the recommendation to connect any external (non-safety I&C) equipment via a Monitoring and Service Interface computer. This assures that an (additional) network message check and network protocol conversion is needed on for messages coming from an external device into the so called “inner zone” (see Figure 20) [43]. This check and protocol conversion is performed in addition to the protocol conversion done by the industry “Gateway” indicated in the Figure. It is assumed that the MSI has a higher safety certification as the gateway. In principle, the MSI performs a very thorough check at the application layer and forwards only messages that are in line with the static configuration generated by the platform code generators.

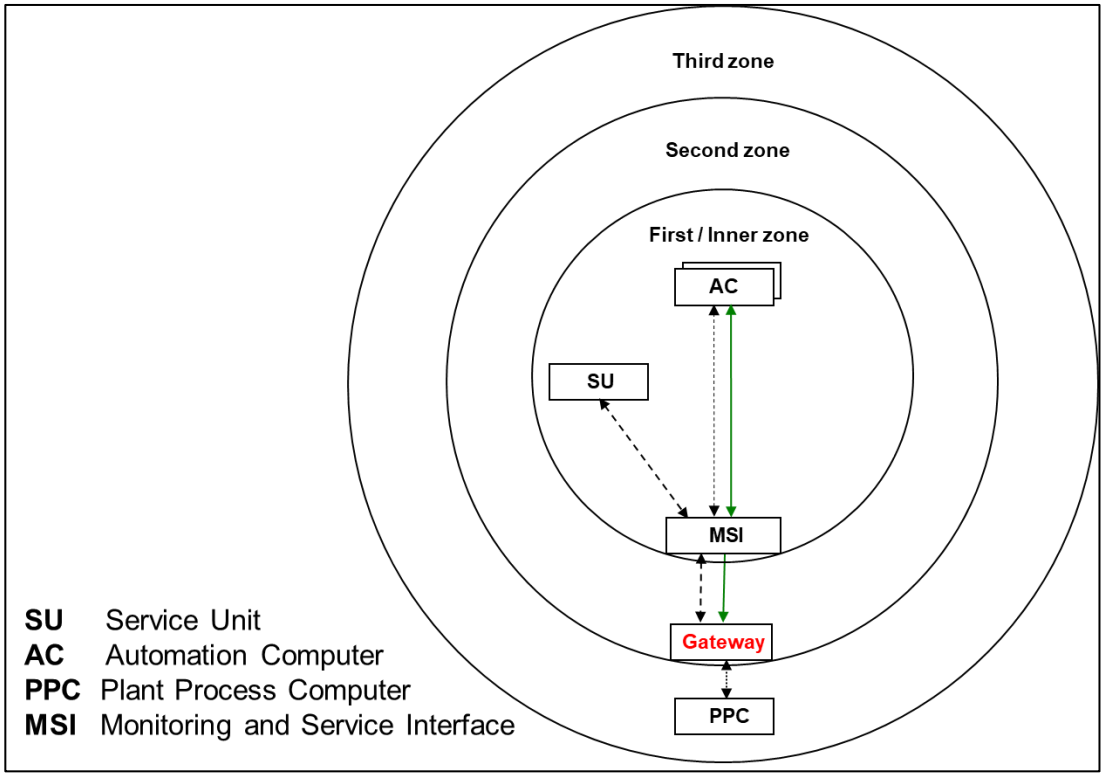

Figure 20. Monitoring and Service Interface Barrier architecture assumptions

The MSI Barrier test is supposed to be performed after major Safety I&C platform tests. This goes in line with the security testing recommendations of ISO/IEC 29119-1 [12] §5.2, see Figure 21.

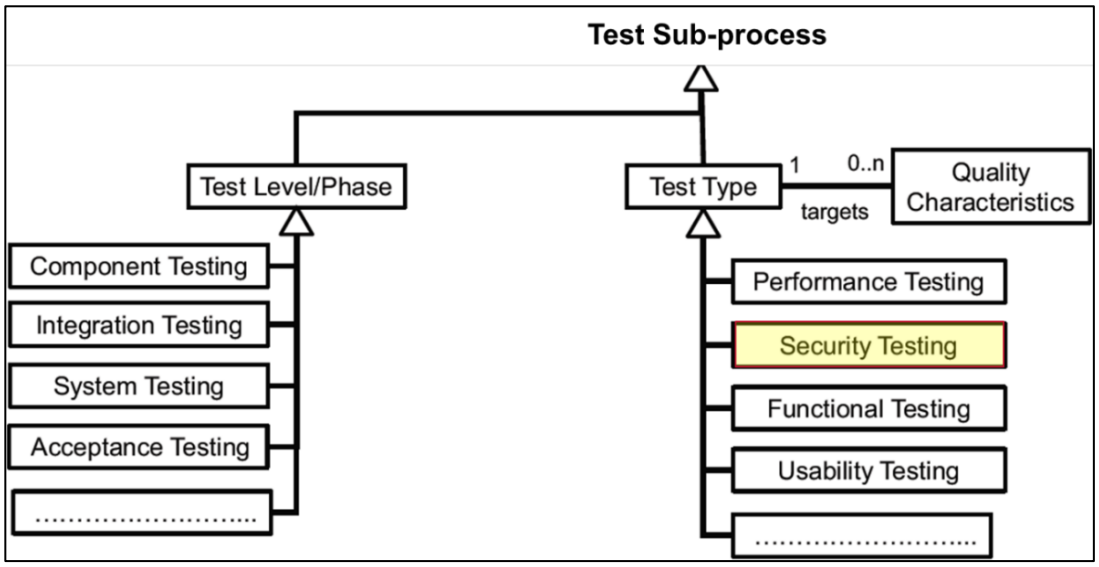

Figure 21. Integrated security testing according to ISO/IEC 29119-1:2013 §5.2

While the MSI Barrier test is targeting one specific configuration, with an Automation Computer (AC), a Gateway and a Service Unit (SU) connected to an MSI computer, the test is quite comprehensive. The test considers many parts of an I&C platform,

including the embedded operating system kernels on the AC and MSI, the networking software on each device, the application software generated by the code generators of the tested platform version, the runtime environments (part of the system software) on each device and implicitly further software components like the cyclic self-test and exception handler, that will trigger in case the cyclic processing of the application software would be successfully manipulated (with a real impact) by a forged message.

This test includes fixed parameterizations for the fuzzing. Within the SMARTEST-FRA project, it is intended to provide extensions to this proprietary test suite, so that different fuzzing approaches can be specified. This should not be limited to changes of a few configuration settings, but by including new fuzzing algorithms, both from the Framatome PhD candidates and the university partners, as e.g., genetic and evolutionary algorithms which are deployed in other research projects of SMARTEST-FAU project partner.

Figure 22 indicates an overview of the MSI fuzzing framework implemented in Python. The framework makes use of libraries, like libpcap, and assumes that one device in the representative configuration is replaced by the device of an attacker. As indicated in the figure, the primary attack vector is supposed to be via the Gateway (GW). However, the test suite is also able to implement an attack vector going via the SU.

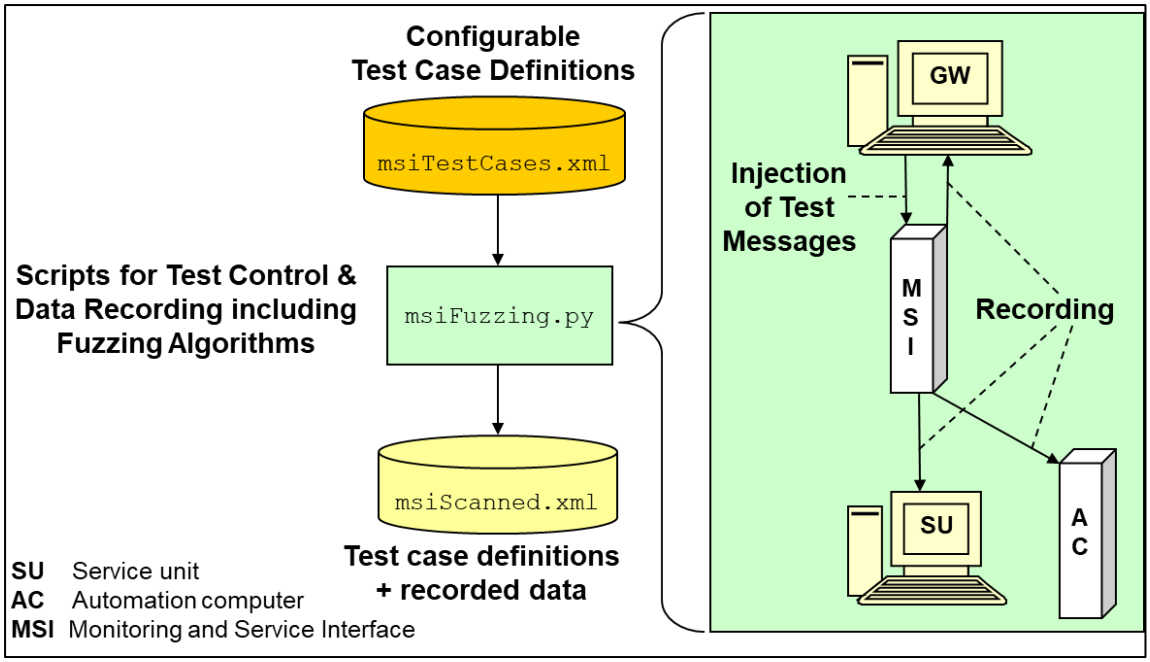

Figure 22. MSI Barrier fuzzing framework structure

Note: The fuzzing tests cannot be installed and run directly on GW or on a Service Unit (SU), even if the GW or SU would run a Linux distribution that supports the Python version and the versions of the software libraries used by the fuzzing test suite. The reason is that these computers come as security hardened versions, which, for example, would not permit to put a network interface device to operate in promiscuous mode (e.g., to replace the sender MAC address in outgoing messages by any manipulated value, instead of the real network interface card (NIC) hardware addresses). Accordingly, as a simplification, for the MSI Barrier fuzzing tests, it is always assumed that the attacker is replacing a computer, e.g., the GW, by its own

readily configured attack notebook, so no credit is taken of any security hardening at that level.

As part of the MSI Barrier fuzzing test the messages must be manipulated at different ISO/OSI layers, as indicated in Figure 23 e.g., for ISO/OSI layer 2, the Logical Link Control (LLC) according to IEEE 802.2. This must be expressed in a semi-formal way, so the fuzzing scripts are able to interpret and execute the intended manipulations.

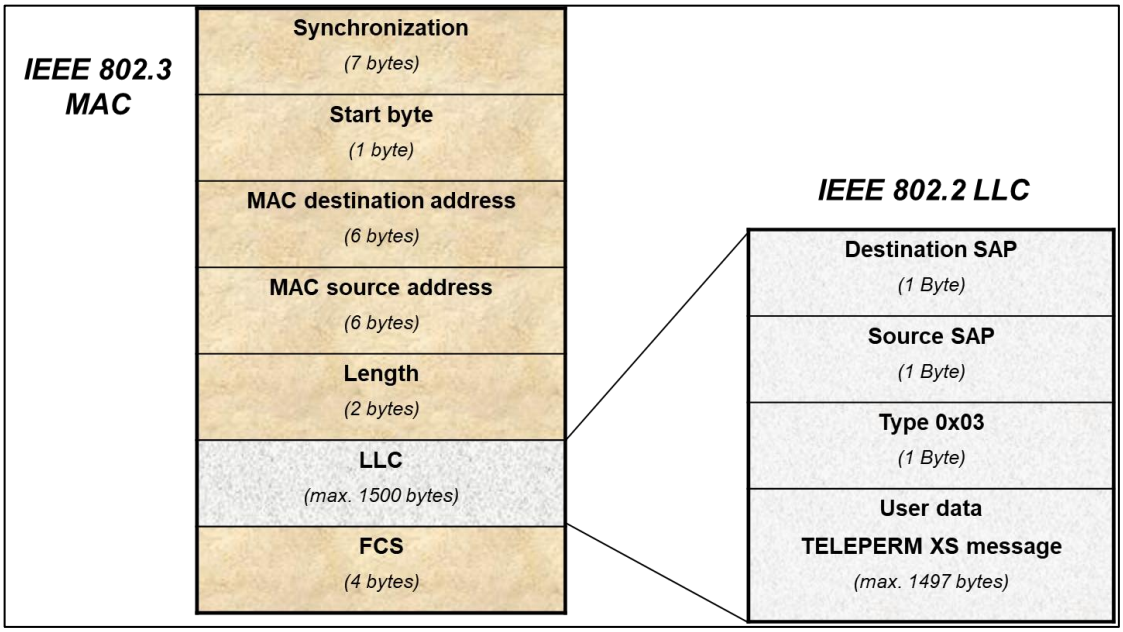

Figure 23. Message Structure: Ethernet Layer Logical Link Control (LLC)

As an example, some possible fuzzing changes are indicated below, followed by an overall description of the representation of the fuzzing tests in the XML notation of the framework.

Manipulation / Fuzzing of MAC Header

MAC = Media Access Control (Hardware address in network)
Manipulation / fuzzing of MAC destination address
- Broadcast address (FF:FF:FF:FF:FF:FF)
- IP Multicast addresses (01:00:5E:00:00:01 and 33:33:06:01:A0:00)
- Addresses of service unit and automation computer
- Random addresses

Manipulation / fuzzing of MAC source address
- Address of service unit and automation computer
- Random addresses

Manipulation / fuzzing of message length
- Maximal length of Ethernet frames
- Type marker for IP Internet Protocol
- Random length

Manipulation / Fuzzing of LLC Header

LLC = Logical Link Control
Manipulation of the Target Service Access Points
Flag of HDLC Header (High-Level Data Link Control)
HDLC escape characters: Interrupt of transmission
SAPs of common protocols (NetBIOS, SNAP)
Eventually: all 256 possible values
Manipulation of Source Service Access Points
SAPs of LAN Management, Sub-Network Access Protocol, etc.
Eventually: all 256 possible values
Manipulation of Message Type
Minimum value and maximum value
Invalid random numbers (all 255 values)

General Manipulations

Messages with statically modified complete content
Filling of messages with 0xFF, escape characters, etc.
Modification of each 2nd or 4th byte in the headers
Increased CP load
Sending of valid and invalid messages within shortened cycles
(e.g., 5 ms and 2 ms)
Suppression of messages
Sending of correct messages with extended cycles (150 ms)
Intention to produce a buffer overflow
Manipulation of Length fields, Transmission of prolonged messages
Sending of command messages
e.g., intention to initiate a CPU reset, deletion of FEPROM

Definition of configurable Test Cases in an XML File

The MSI Barrier Test Framework is based on XML tags that must be structured according to a predefined tree structure.

This allows for a definition of all test cases configured for one fuzzing session to be defined in a comprehensive XML file, e.g., msiTestCases.xml, with a tag <MsiTestSuite> tag as the root. However, inside this tag multiple <TestRun> tags can be included and each <TestRun> can include multiple test groups, test sub-groups and test cases <Tc>.

The following tags (elements) of the XML file indicate an extract of the structure of one test suite instance.

```
<MsiTestSuite>
  <TestRun>
    <Group>
      <Subgroup>
        <Tc>
          <Inject>
          <Expect>
```

Table 1 shows an overview of a selection of XML tags together with their brief description.

Table 1. Example XML tags from a configurable fuzzing test suite instance

Tag	Description
id	ID of a test run, unique within an MSI test suite, ID of a test group, unique within a test run ID of a test subgroup, unique within a test group ID of a test case, unique within a test subgroup
inject	Python function with a predefined function prototype for injecting code at specified relative/absolute positions or pattern based. Random values can be injected according to different random number generation algorithms.
expect	Python function with a predefined function prototype for extracting data from specified relative/absolute positions or pattern based searching
executed	True, after test run was executed
evaluated	Indication whether the results of the test run have been evaluated
begin	Start time of test run, test group, test subgroup, test case
end	Stop time of test run, test group, test subgroup, test case

Each test suite is in fact a test suite instance. As indicated in Figure 16, the input to the framework of Python scripts is a comprehensive XML file, structured with pre-defined XML tags, some of which, like “inject”, may contain powerful functionality. Based on the “expect” tags and some predefined execution logic for the representative network configuration, the input messages can be matched to output messages of a given test case. This is something specific to the MSI barrier test, as it allows consideration of not only the one network interface that is used to directly manipulate a digital device, but also two further networks (i.e., an automation network towards one Automation Computer (AC) and the maintenance network towards the Service Unit (SU)).

Extension of the Fuzzing Framework

Different extensions of the MSI Barrier fuzzing framework were discussed in the SMARTEST R&D project. Some of these will be prototypically implemented until the end of the SMARTEST project (end of 2018). Others will be outlined and can hopefully be addressed in a follow-up R&D project.

The current hardware configuration for the execution of the MSI barrier tests is available in the dedicated test lab for SMARTEST-FRA, see figures describing the test facilities. The test suite can be extended to support other hardware configurations, which is not planned as part of the SMARTEST project.

While the initial MSI Barrier test supports the injection of messages that are composed of a sequence of datagrams (at the LLC layer), the focus of the test cases is more on manipulation of single messages and not on the sequences of messages. The implementation of some more complex scenarios with message sequences, are planned for the SMARTEST.

The initial MSI Barrier test supports the execution of long-term fuzz testing - an explicit requirement of the regulatory body involved in the certification of the initial MSI Barrier functionality and testing. While this allows the fuzz testing to run for 24 hours or even multiple days (e.g., during a weekend), each time starting with different seed values,

this could be configured to be smarter (not just an initial seed value, but changing fuzzing behavior during long-term runs). Due to equipment availability and overall resource limitations this will probably not be addressed as part of SMARTEST.

The initial MSI Barrier test performs some “sanity checks” before and after a test case execution. This includes sending two non-manipulated messages and recording the results at all 3 involved interfaces. This could be extended by further automated checks via pre- and post-conditions.

The initial MSI Barrier test can be extended by including alternative, potentially smarter fuzzing algorithms. This was discussed several times with the project partners, and initial alternative algorithms will be evaluated. However, this will need more in-depth evaluation, beyond the resources allocated to the SMARTEST project.

The fuzzing framework of Python scripts can be extended to address other hardware platforms, which are also available in the dedicated SMARTEST-FRA test lab. This will be addressed to a limited extent within the SMARTEST project, as it will require a refactoring of some of the Python scripts in order to provide additional extension APIs.

Some Defensics® based fuzzing results will be compared to the MSI Barrier framework results, based on a limited set of messages. This could be further extended in a follow-up project.

11. Achieved research results

11.1 WP 4.1: Security Testing of Industrial Network Protocols for Nuclear

A first part of the WP “Tool-Based Testing” forms “security testing of communication protocols” for NPPs (WP4.1).

In general, the "Smartest2" research project focuses on the IT security of software-based control systems. One of the main objectives is to identify suitable cybersecurity measures for process control systems. This initially involves in SMARTEST project examining the various communication protocols (MODBUS, PROFIBUS, and PROFINET) used in current control systems.

These communication protocols offer automation components various functionalities necessary for regulation and control in nuclear power plants. However, current control systems in the automation environment often come with minimal security measures, as they were primarily designed to meet performance requirements, with security measures being implemented outside the systems (e.g., through physical protection) or because the systems' availability and real-time performance could have been compromised. With increasing network connectivity, this is no longer acceptable.

Preliminary work (PhD thesis at Framatome) have addressed the challenge of ensuring compatibility between communicating devices, which is often inadequately handled by conformance and penetration tests due to incomplete specifications. Such inadequacies can lead to delays, congestion, and loss of synchronization, sometimes requiring manual intervention by operators. To mitigate these issues, a compatibility test system that uses a man-in-the-middle approach was designed and implemented to inject errors and monitor the behavior of communicating entities, with a focus on safety-relevant processes. The related research on SMARTEST 2 specifically considers safety-relevant application protocols such as OPC UA, IEC 61850, and MQTT.

Following, the security of three common industrial M2M communication protocols were investigated in this work package:

- OPC UA: Client-server model with extensive features for industrial communication.
- MQTT: Publish/subscribe model, facilitating decoupled communication.
- CoAP: Request/response model, similar to HTTP but optimized for constrained devices.

11.1.1. Industrial Automation and Control protocol OPC UA

OPC UA is a commonly used machine-to-machine communication protocol. As it is used in industrial critical infrastructure, its security is crucial.

A security checks performed by the German Federal Office for Information Security (German BSI) concluded that OPC UA was designed with a focus on security and does not contain latent security vulnerabilities. Thus, the focus of OPC UA security tests should be on protocol implementation. Security testers should especially address the Application Programming Interfaces that are provided by implementers. While the OPC Foundation provides reference implementations for a selection of programming languages, further implementations are available, including libraries that provide their own API on top of the OPC UA protocol for both the OPC UA server and OPC UA client side.

11.1.1.1. Security, Interoperability and Scalability of Open Source OPC UA Implementations

Preliminary studies in the scope of a neighboring DECENT project on decentralized energy storage solutions) delved deeper into the security of communication protocols, with correlation on network protocols examined in the SMARTEST 2 project specifically open-source OPC UA implementations. It involved a dynamic exchange of knowledge with two PhD students from Framatome GmbH, affiliated with the University of Erlangen-Nürnberg (FAU) and the Technical University of Munich (TUM). Two significant research related projects were completed, both of which have been published.

The first study analyzed four popular open-source implementations and found that they generally offer strong security standards, making them viable alternatives to commercial options with scalability varying notably depending on the programming languages used. However, some shortcomings remain, such as missing upper timeout limits in python-opcua and less stringent packet type checks in node-opcua. Notably, no significant security flaws were identified in open62541 and UA-.NETStandard. Considering both security and scalability, open62541 and UA-.NETStandard achieved the best results. This research was published in ETFA 2020 [44].

The second study demonstrated that these implementations have a comprehensive coverage of features and functionalities with minimal interoperability issues. This work was published in GI Jahrestagung 2020 [45].

These studies among several studies have highlighted critical security issues in open source OPC UA implementations, identifying significant security gaps. These include default settings that lack adequate security measures, leaving systems vulnerable, and function manuals that often fail to provide secure configuration guidelines. Additionally, in some cases, essential security features are not implemented at all, further compromising system security.

In the course of experimental security testing, PhD students at Framatome investigated how to secure OPC UA Server configuration for smart charging station where a cyber-secure configuration for respective hardware is crucial. Two tasks were performed:

- Tests with S7-1500, with two function manuals Si18 and Si 21: The first examines the manufacturer recommendations for security settings of OPCUA servers including on the manufacturer PLC Siemens SIMATIC S7-1500. In the manuals, safety-critical settings were often disabled or at least no note was given that would have led to a configuration as safe as possible, revealing security problems even at commercial solutions. From these points of view, the manual of the Siemens PLC was also criticized.
- Penetration test of the OPC UA Server hosted by the S7-1518 with Metasploit OPC UA-extension: The 2nd release is a metasploit extension for testing with OPC UA servers. Metasploit is a penetration testing framework. Based on the publications, we conducted penetration tests with the Metasploit framework and the OPC UA server of a Siemens PLC. We first followed the PLC function manual but then a special communication manual also from Siemens. In the second configuration, no critical information could be obtained from the PLC with penetration testing.

Table 2- Penetration test results- OPC UA Server hosted by the S7-1518 with Metasploit OPC UA-extension

Phase	Default Configuration	Configuration According to security manual[Si21]
Discovery	Found server	Found server
Authentication	Login with empty credentials was possible	No login possible (no fitting credentials found and not possible with self-signed certificate)
Configuration	Revealed unencrypted communication (MessageSecurityMode: MessageSecurityMode.None_) Revealed all nodes, even writeable ones and those reserved for privileged users!	Login was not possible, hence no configuration could be derived

Results highlight the importance of sensitizing employees to safe configurations. Additionally, we preconize that manufacturers should enhance the transparency and communication of safety-relevant information to users. The related papers were published at the 6th GI/ACM Standardization Workshop on Industrial Automation and Control Systems (IACS). Within the framework of the 51st Gesellschaft für Informatik (GI) event in September 2021, workshops were also presented.

General countermeasures on how to address the cybersecurity concerns of OPC UA were formulated and presented in 2023 IAEA International Conference on Computer Security in the Nuclear World: security for Safety. A contribution was also prepared for IAEA cybercon 2023 in Vienna, that presented the latest results[1] at the conference (conference contribution and poster presentation).

[1] For both proprietary and open-source implementations of OPC UA, it requires a combination of technical measures, such as encryption and firewalls, as well as non-technical measures, such as regular software

PhD students at Framatome closely follow the latest developments from the OPC UA Foundation, which is increasingly relevant to the SMARTEST2 R&D project. This relevance of this part of the SMARTEST2 R&D is further heightened by the consideration of industrial protocols, such as OPC UA, by the nuclear IEC SC45 WG3 and WG9.

11.1.1.2. Use and Validation of OPC UA libraries in JavaScript open software stacks

In the Framatome Cybersecurity Laboratory, further doctoral students were introduced to the topic, in particular with regard to the use and evaluation of the continuously improving OPC UA libraries. In this context, the latest versions of the OPC UA standards were also evaluated.

Applicability of existing node-OPC UA implementation using new runtime "Deno"

OPC UA has several proprietary and open source implementations in different programming languages due to its interoperability. Among them, a JavaScript implementation node-OPC UA has advantages such as usability, code maturity, etc. JavaScript is a just-in-time compiled programming language that is runtime system is running.

Within this context, the conducted research presents and evaluates measures to overcome errors when running the JavaScript implementation of OPC-UA protocol on Deno. Deno is a potential and unofficial successor as it was developed by the original author of Node.js. Node.js is the most common runtime for running JavaScript programs. A promised improvement of Deno is the focus on higher security, such as a default restricted file system and Network access.

PhD candidates at Framatome examined measures to eliminate errors when running node-opcua on Deno and evaluated them considering the current lack of a dedicated OPC UA implementation and the limited research literature on this topic. The code examples, to explore approaches to remove obstacles to Node.js code execution using Deno, are adapted from a basic server implementation using the node-opcua library. Workarounds and debugging schemes were provided to run Node.js-designed programs on Deno particularly ensuring the secure execution of OPC UA deployments in JavaScript environments, acknowledging the compatibility drawbacks2. Despite these challenges, Deno's requirement to manage uncaught promises is a strong security advantage.

updates and employee training. Organizations can ensure their OPC UA systems' secure and reliable operation by implementing these measures.

[2] Firstly, eliminating package managers is not viable. Secondly, using the unstable option is required. Thirdly, handling or commenting out assertions is necessary, with handling consuming significant resources during debugging and commenting reducing Deno's benefits

As part of a bachelor's or master's thesis, representative use cases (test suites) have to be designed and implemented so that these scenarios can be repeated for newer versions of Deno until Deno has reached a sufficient maturity level. Furthermore, it will also be very interesting to investigate how (quickly) Deno catches up, especially with regard to the OPC UA implementation and whether this brings fundamental advantages [46] [47].

11.1.1.3. Real-Time Performance of OPC UA

plays an important role in ensuring specific safety policies, especially in real-time applications. With TSN, communication remains within the limits of jitter, loop times and packet loss rates. For this reason, OPC-UA, the most widely used machine-to-machine (machine-to-machine Machine, M2M) communication protocol expands its application horizon with TSN. Open62541 is the only open source implementation that has been integrated into the TSN functions of Linux distributions.

As part of the experiments, the partner FRA investigated performance of OPC UA over TSN (**OPC UA PubSub over TSN**). The current study builds on existing research by evaluating all these qdiscs in point-to-point and bridged topologies using open-source software on commercial off-the-shelf hardware. This provide a foundation for future research and practical use specially in WP4.7. Early findings show different queuing disciplines are more suitable for different requirements and traffic patterns. Further results demonstrated that the connection of OPC UA applications with different queuing disciplines (qdisc) ensures compliance with real time limits and certain performance limits can be achieved using open-source software and standard hardware.

The research demonstrated that when developing models representing the internal structure of software, communication networks and network protocols of I&C system:

- COTS hardware and open-source software can effectively meet the real-time requirements of OPC UA applications, though qdisc performance varies significantly with different configurations.
- System architects and engineers should carefully evaluate the characteristics of the qdiscs and configure them to align with the application-specific requirements to optimize OPC UA deployment.

The related paper was published [48]. Additionally, at vgbe Conference on IT Security" in Hamburg Altona in 2022 [49], R&D results were presented and later a corresponding publication in the International technical journal for power and heat generation was submitted in the first half of 2022 Parts of these results were presented at the 7th GI/IACS workshop on 30 September 2022 in Hamburg.

In addition to OPC-UA (), most widely used machine-to-machine (M2M) communication protocol, there are other interesting, lightweight protocols, such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), which have different strengths than OPC UA. These protocols are also investigated in SMARTEST2 as part of the AP 4.1 security test of NPP-specific protocols.

11.1.2. Lightweight Messaging and Telemetry

MQTT is a widely used communication protocol in IoT networks. Compared to OPC UA, it promises a lighter design, which scores especially with limited processors, such as in IoT devices. Since MQTT is a TCP protocol, its security is handled by TLS. There are several parameters and configurations for deploying TLS.

As part of WP4.1 security testing of "NPP-specific protocols", MQTT is being investigated as an emerging and potentially interesting protocol for the nuclear sector.

Two significant studies have been conducted to evaluate the performance and security of open-source MQTT implementations, each yielding important insights. The partner FRA identified a trade-off between resource consumption and network latency among different implementations. The related paper was published in CCNC 2021 [50]. Additionally, a study on TLS Cipher Suite Performance on MQTT, demonstrated that resource consumption can be optimized by carefully selecting the cipher suite and adjusting the length and rate of MQTT messages. The results were published at NOMS 2022 conference [51]. These studies emphasize the importance of selecting appropriate MQTT implementations and configurations to balance performance and resource usage, as well as optimizing security settings to enhance overall efficiency of MQTT protocol. Parts of these results were also presented at the 7th GI/IACS workshop on 30 September 2022.

The partner FRA also conducted a study of slow denial of service (DoS) attacks on MQTT built on the existing literature. The research focused on expanding the capabilities of such attacks, successfully removing the concurrent client limit, and reaching more than 25,000 active connections. This resulted in a noticeable increase in resource consumption and highlights the potential vulnerabilities in MQTT-based IoT systems.

In addition, PhD students implemented a distributed DoS (DDoS) variant of the attack for the first time by randomizing source IP addresses and simulating packets from multiple sources. This approach complicates the detection and defense efforts of Intrusion Detection Systems (IDS) and reveals additional vulnerabilities in IoT security. The results underline the importance of developing robust security mechanisms and strategies to protect against slow DoS and DDoS attacks in resource constrained IoT environments. This study contributes to advancing research in the field of IoT security, especially regarding the MQTT protocol. By addressing these security challenges, the aim is to drive the continued growth and success of IoT deployments in various areas. The results were successfully submitted and presented at the BlackSeaCom conference [52].

Furthermore, MQTT continued to be considered as an open network protocol for machine-to-machine communication regarding security aspects in Q1/2024, especially as part of a doctoral thesis that is expected to be completed in the first half of 2024. MQTT examples were discussed in particular during a technical exchange with Idaho Nation Laboratory - Nuclear Energy in September 2023 in Idaho/USA. Potential

applications include potential future nuclear projects in Europe as well as potential contributions to the first Small Modual Reactor (SMR) pilot projects.

11.1.3. MQTT Lightweight IoT Communication CoAP

The Constrained Application Protocol (CoAP) is a protocol specifically designed for the Internet of Things and further developed for embedded devices, which takes over the basics of REpresentational State Transfer (REST).

CoAP is a protocol specifically designed for the Internet of Things and further developed for embedded devices, which takes over the basics of REpresentational State Transfer (REST). Conducted research includes two key assessments related to CoAP.

The first is an assessment of security mechanisms for CoAP has early findings indicating that OSCORE offers advantages over DTLS in terms of security.

The second assessment focuses on transport protocols for CoAP comparing how different transport layer protocols, UDP and TCP, affect performance. The partner FRA identified 4 different load profiles based on the combination of short-lived connections and periodic and intermittent traffic and determined which transport layer protocol performs best in each load profile. Early findings highlight trade-offs between using UDP and TCP, considering factors such as performance and reliability.

Parts of these results were presented at the 7th GI/IACS workshop on 30 September 2022 [53] [54].

11.2. WP 4.2: New Hardware-based Security Solutions and Validation

Cryptographic systems have become an integral part of our daily life through the need of security activities such as communication, electronic money systems, disc encryptions. Cryptography provides the necessary protection from the threats by ensuring the confidentiality and integrity data in transit, authentication of senders and recipients to one another and protecting against repudiation,

Random bit generators are a key component for strengthening and securing the confidentiality of electronic communications and used in many cryptographic applications like key generation, encryption, masking protocols, internet gambling. Unpredictable random numbers are essential for the security of cryptographic algorithms for generating the underlying secret keys. Field programmable gate arrays (FPGAs) form an ideal platform for hardware implementations of many of these security algorithms.

A random bit generator is a device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased. Methods for generating random has been used from ancient times, including dice, coin flipping, the shuffling of playing cards, the use of yarrow stalks, and many other techniques. There are

number of random number generation schemes and Random Number Generators actively used in IT security products.

Cryptographic quality is achieved by random bit generators that satisfy a number of requirements as specified in the international standard:

- Unpredictable: Unpredictability is a required property of an RBG. It should not be possible to predict the output of a properly implemented and working RBG. Forward secrecy refers to the inability to predict future output of the RBG based on the knowledge of previous output values and/or internal states. The inability to deter-mine prior output of an RBG, given knowledge of the current or any future output of the RBG, is known as backward secrecy.
- Unbiased: Each potential outcome has the same chance of occurring
- Independent: The generated outcome is said to be memoryless and should not be influenced by previous outcomes.

Figure 24 depicts the conceptual functional model of Random bit generators as defined in the International Standard:

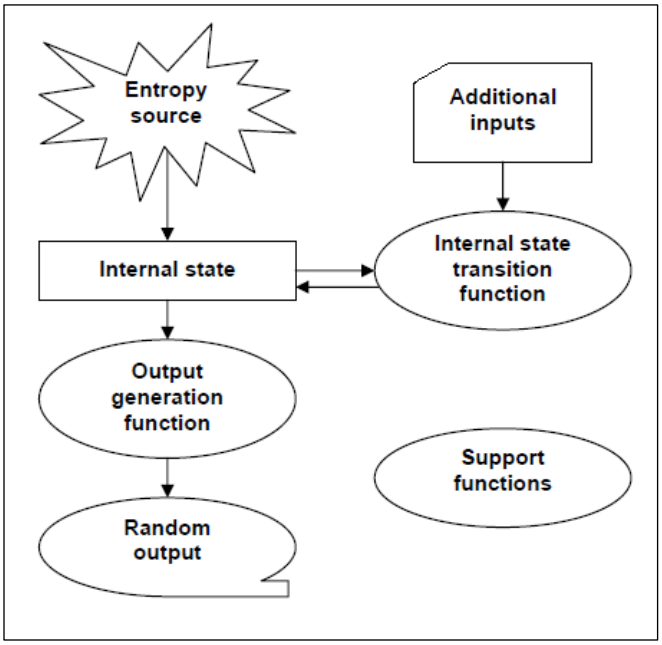

Figure 24- RGB functional model

The entropy source is a key component in RBG reference model, it quantifies the amount of unpredictability or uncertainty relative to an observer. Every RBG shall have a primary entropy source. RBGs are classified into two basic types depending on the nature of their primary entropy source. The primary entropy source will either be a non-deterministic entropy source or a deterministic entropy source. If an entropy source is a system from which any amount of entropy can be extracted by sampling, provided that this system runs for a sufficiently long period of time, then it is deemed to be a non-deterministic entropy source. In particular, no deterministic

algorithm should be able to predict the output of a non-deterministic entropy source. If an entropy source is a seed value, it is called a deterministic entropy source. This seed value may be supplied to the RBG from an external system or internally from the RBG. If the seed value is supplied externally to the RBG, it is assumed by the RBG to have sufficient entropy and to have been drawn from a specified set. On the other hand, if the seed value is supplied internally from within the RBG, it is assessed to have sufficient entropy and to have been drawn from a specified set. Care shall be taken to ensure that an adversary cannot gain sufficient control over the seed value to degrade the entropy of the output of the RBG. An RBG is said to be an NRBG if its primary entropy source is non-deterministic. An RBG is said to be a DRBG if its primary entropy source is deterministic. An RBG may also utilize additional entropy sources that can be either deterministic or non-deterministic.

ISO/IEC 18031 distinguishes non-deterministic and deterministic random bit generators (also called pseudo random bit generators), while recognizing the use of hybrid random bit generators. Typically, non-deterministic and hybrid random bit generators are based on a conceptual model with an entropy source (or multiple entropy sources integrated by a suit-able signal noise generating design), a stochastic model and a cryptographic post-processing.

A Random Bit Generator (RBG) may be implemented in different hardware technologies, including in FPGA technology. The security test should first verify the conceptual model with regard to potential systematic faults, e.g. non-biased entropy source, design of the noise source, derived from a well-documented publicly available design, suitable pseudo random algorithm etc. Then the security test should address implementation by using adequate test instrumentation and a validation of the stochastic model. Finally, the crypto-graphic post-processing should be validated.

The 4th part of the multipart ISO/IEC 27033 standards series explain how we should use security gateways in order to secure communications between networks. Precisely, it shows the importance of firewall, intrusion protection system and the requirements for security gateways based on threats analysis, and also the different implementation of them. However, nuclear power plants need the highest level of security due to the importance of these structures. It is why firewalls are simply not enough to ensure the complete networks protection. The concept of diode communications applies well in this case. This allows only unidirectional data transfers, in connotation with the electronic component between different networks.

To ensure a better security of nuclear power plants security networks, data diode gateway could also be deployed. It uses a unidirectional communication from a low classified network to a high classified network. In this case, no acknowledgment is sent during or after the transfer. That could pose a problem for the integrity of the data.

As part of WP4.2, the partner FRA Security performed the development and implementation of a secure data diode protocol.

Communication is established by optic fiber between the two different networks transceiver. In our case, AT-MC102XL transceiver are used. Because of the optic fiber includes a return channel for transfers, two other transceivers that send Fast Light Pulse were connected to simulate an acknowledgment and avoid any possibility of recovering data of the high classified level network by a hacker. On the other hand, data could be encrypted for a better level of security.

The protocol for data transfer chose is User Data Protocol (UDP), that enables faster, unidirectional and high file transfer. It doesn't send acknowledgement, allowing higher transfer speed, but in order to save the integrity of the data, we have to send every data several times. The limitation of UDP could be the loss of data packets, but in the case of these installation there are none or very few, and this consideration has been verified experimentally during a simulation. On the other hand, if the data is higher than 64KB, it is split in right size packets for different transfers. At the reception, a right size buffer combines data in the right order using identifiers in data headers. The programming language used is Python because of its reliability, portability and extensive support libraries.

In order to visualize the different transfers, a Typescript browser interface has been developed.

The simulation showed that an UDP communication over a data diode can provide both high throughput and high reliability. The results of the analysis presented in this work demonstrated that the usage of unidirectional gateways can reduce common security risk factors in power plants and critical infrastructures. However, it is also important to place other security equipment like filter and firewall to reduce the risk of loss of integrity and availability for the receiving network, as it is recommended in the ISO 27033-4 standard.

11.3. WP 4.3: Security Testing at the Source Code and Binary Code Level

As part of the WP4.3, work has been realized to evaluate different security fuzzing approaches. The findings of this research [55] emphasize how important it is to use tailored fuzzing techniques to detect vulnerabilities. The authors show that various fuzzing tools, such as AFL ((American Fuzzy Lop), Radamsa, and CGE, expose buffer overflows to different degrees through experimental assessments. According to their investigation, the specialized method CGE (Constraint-Guided Evolution) performs better than general fuzzers like AFL and Radamsa, especially in situations when complicated buffer logic is involved. This result emphasizes how important it is to use specialized testing techniques and domain-specific expertise to increase the effectiveness of security testing initiatives. The study also emphasizes that different fuzzing approaches must be used in order to address a variety of problems, including those presented by network systems.

Additional research regarding guided search patterns for exploitable vulnerability classes has been carried out which focuses on a structured guided search approach for identifying particular software vulnerabilities, including race conditions and buffer overflows. In order to find required and sufficient circumstances for the vulnerabilities, it employs a three-step procedure that begins with restricting the search space to concentrate on relevant code paths. Next, it analyzes and determines search target restrictions using symbolic execution and SMT-solving. Finding situations that meet these restrictions is the last stage, in which heuristic-based methods like genetic algorithms are used as needed. The SMARTEST-SWE framework is used to implement this approach. It improves on traditional static and dynamic analysis by combining heuristic and systematic methodologies. This guarantees a comprehensive investigation of possible vulnerabilities, even in circumstances that are complicated and undecidable. Results of this research [56] show that buffer overflows and race scenarios may be found using the guided search methodology, especially the SMARTEST-SWE method. The guided search approach performs better in detecting buffer overflows than conventional fuzzing tools such as AFL, Radamsa, and QSYM, particularly in cases where bounded loops are present. Additionally, by examining various interleavings of concurrent thread executions and demonstrating how these interleavings may result in inconsistent outputs, it correctly detects race situations. The method's blend of heuristic approaches like evolutionary algorithms and systematic techniques like symbolic execution and SMT-solving guarantees thorough vulnerability discovery, even in cases that are challenging or difficult to determine. The integration allows a thorough examination and efficient reduction of any software vulnerabilities.

In the year 2022, a guided research was carried out for races based on data flow patterns [57]. The authors' primary objective is to provide efficient methods for methodically locating software vulnerabilities. They are especially concerned with race conditions brought on by concurrent threads' instructions that are not properly spaced out. Their goal is to address the difficulties that are created by the growing complexity of software and the constraints of traditional testing methods such as fuzzing. The authors primarily target pre-operational exploitation of races produced by unpredictably interleaved instructions. Researchers want to create intelligent algorithms based on static analysis to extract logical constraints and systematically solve them to discover vulnerabilities. The efficacy of the suggested technique in discovering race conditions in software is the key learning and high-level outcomes of the article. The authors present a systematic approach that operates random search strategies in terms of both detection capabilities and efficiency. They achieve this by identifying three patterns of data flow that are prone to race and developing a methodology for race detection based on patterns. The study emphasizes the advantages of the suggested strategy, especially its capacity to limit the search to certain patterns and minimize dependence on actual code executions.

11.4. WP 4.4: Security Testing of User Interaction Relevant Parts

The detailed analysis of the cybersecurity aspects of user interactions with control systems (WP 4.4) is intended to investigate the secure interaction using digital systems. Ideally, a comparable level of safe interaction should be demonstrated, as in the operation of conventional mechanical controls in a conventional control room.

Within the framework of a doctoral thesis, the secure user interaction is considered together with formal approaches to investigate cybersecurity-relevant aspects for functional safety and cybersecurity. Since there is still little literature in this area of the interface of the three knowledge areas (1) Human Factors Engineering (HFE) / Human Machine Interface (HMI), (2) functional security and (3) cybersecurity, a corresponding notation based on the work of 2022 has been further developed to be able to present further user interactions as well as pre- and post-conditions.

The same principles that are generally applied to SCADA systems regarding vulnerabilities in cyber breaches can also be found in Human Machine Interfaces (HMIs). Nevertheless, user interfaces can be considered as one of the most critical attack vectors in SCADA systems that can be used. Some past cybersecurity incidents, such as Stuxnet, are just proof of this. Several factors related to the usability, access and operating principles of these assets are considered for this specific weakness. The quality of the graphics, alarms, trends, and news when not adequately provided to operators is another reason for discrimination against HMIs' cybersecurity. Especially with the increasing demand for the integration of commands regarding functions in higher security categories (Cat B, Cat A [IEC 61226]), such a platform can be the weakest link in a security chain. For these reasons, considering cybersecurity for such systems is crucial from the early development stage.

The project SMARTEST2 uses a semi-formal representation method to describe the functional specification of a SCADA architecture. In this case, user interfaces are used as an example for SCADA architectures to test and implement this methodology. A functional specification is a guideline and a continuous reference point for the following phases of system development. This "reverse engineering" of the functional specification of the UI platform has the main objective of gaining a deeper understanding of the relevant technology, which are the safety-related HMIs. The development of a new and formal functional specification of the platform at a sufficiently high level would facilitate the future steps to assess the weak points of the system at both architectural and operational level. This semi-formal representation method is adapted to take cybersecurity attributes and features of the system into account. In addition, it would be more effective to develop and deploy the various security measures and procedures in later stages.

This topic (WP 4.4) will continue to be worked on as part of the completion of a doctoral thesis (expected in the second half of 2024).

As part of the new HALDEN research programs, in which Framatome GmbH is represented historically with the focus on Human Factors Engineering (HFE), cybersecurity priorities were planned in 2022 and integrated in 2023, which are particularly interesting for secure user interface aspects in SMARTEST2. In 2023, the first HALDEN cybersecurity meetings took place and more with a cybersecurity/HFE focus are planned. As part of a CEN/CENELEC CLC TC/45X, contacts were also established with a professor who worked on this topic in France.

11.5. WP 4.5: Forensic Readiness Testing

Security measures to detect tampering are particularly important for critical infrastructures. Since perpetrators are also considered who operate within a system and have insider knowledge, physical security measures (preventive security controls) often do not apply. Therefore, Forensic Readiness Tests will be used to investigate measures for a secure detection of manipulations.

The conducted research expands upon a crucial facet of this previous one, by exploring of advanced logging strategies in the context of Node.js, offering insights into the evolving landscape of secure runtime environments for OPC UA deployment in order to enhance system reliability, debugging efficiency, security, and understanding of system performance.

We explored the value and benefits of implementing advanced logging techniques in OPC UA deployments in Node.js. OPC UA is a leading protocol for interoperable and secure data exchange in industrial automation and IoT. By applying sophisticated logging strategies, deployments can be optimized to Node.js.

Using a case study, we demonstrated the real impact of integrating robust logging solutions into OPC UA applications. It highlights how such practices improve system reliability, increase debugging efficiency, increase security, and make system performance understandable. These valuable insights help developers and system administrators manage and maintain complex OPC UA applications and strengthen the important role of a well-implemented logging strategy. Based on the analysis of a specific instance of an OPC UA Server-Client pair implemented in Node.js, a discussion about optimization strategies that could further strengthen the robustness and security of OPC UA systems takes place. The discussion aims to open ways for more research and promote a continuous pursuit of more efficient and secure industrial automation and data communication systems.

In a Node.js environment, basic logging starts with the built-in console module, but this approach falls short for complex systems like OPC UA. Effective logging in production requires advanced features such as log levels, structured JSON logging, timestamps, and the ability to log to multiple destinations. Logging frameworks such as Winston, Pino, Bunyan, and Roarr provide the necessary

structure and detail. Winston, the most popular and comprehensive logging framework for Node.js, is used as the primary reference for implementing an advanced logging strategy in a case study.

The approach involves replacing regular console logs with more detailed and structured messages, resulting in enhanced debugging and a deeper understanding of system behavior, leading to more efficient OPC UA deployments. A discussion about optimization strategies that could further strengthen the robustness and security of OPC UA systems takes place. The discussion aims to open ways for more research and promote a continuous pursuit of more efficient and secure industrial automation and data communication systems.

The results of the research were presented to GI workshop in September 2023 [58].

11.6. WP 4.6: I&C / Electrical Power Systems

In the context of the rise of cyber-attacks, sensitive infrastructures are not immune to it, as the IACS are the backbone of controlling the operation of the process industry, such as nuclear plants, a novel research led by the partner FRA aims to enhance the cyber-security of power plant components by extending and using an updated plant simulator. This work was made in a scope of a master thesis, where the partner FRA assumes that attack scenarios would have an immediate impact such as attacker having direct access to an industrial communication network or supporting assets that controls at least one critical primary asset.

In order to carry on the research. it is assumed that a sophisticated attacker, as part of an Advanced Persistent Threat (APT), breach the cyber protection of the facility and aims to damage primary assets (e.g. main cooling water pumps, feed water pumps, safety valves, circuit breakers).

The adversary performs gradual manipulations at the application level. One of the task is to detect and predict any a potential anomaly is designed and implemented based on machine learning of expected behavior.

The attack that is used here is a kind of direct manipulation of control systems, and an expected result from APT. These type of attacks are chosen as example as its results can be damaging and have serious consequences short and long term on the hardware, as power grid stability could be impacted. The figure below shows the assumed used attack to study and defend against, it helps the adversary gain undetected access to the maintenance network of the NPP. This access allows the manipulation of different ICS, which must be detected to prevent further damage.

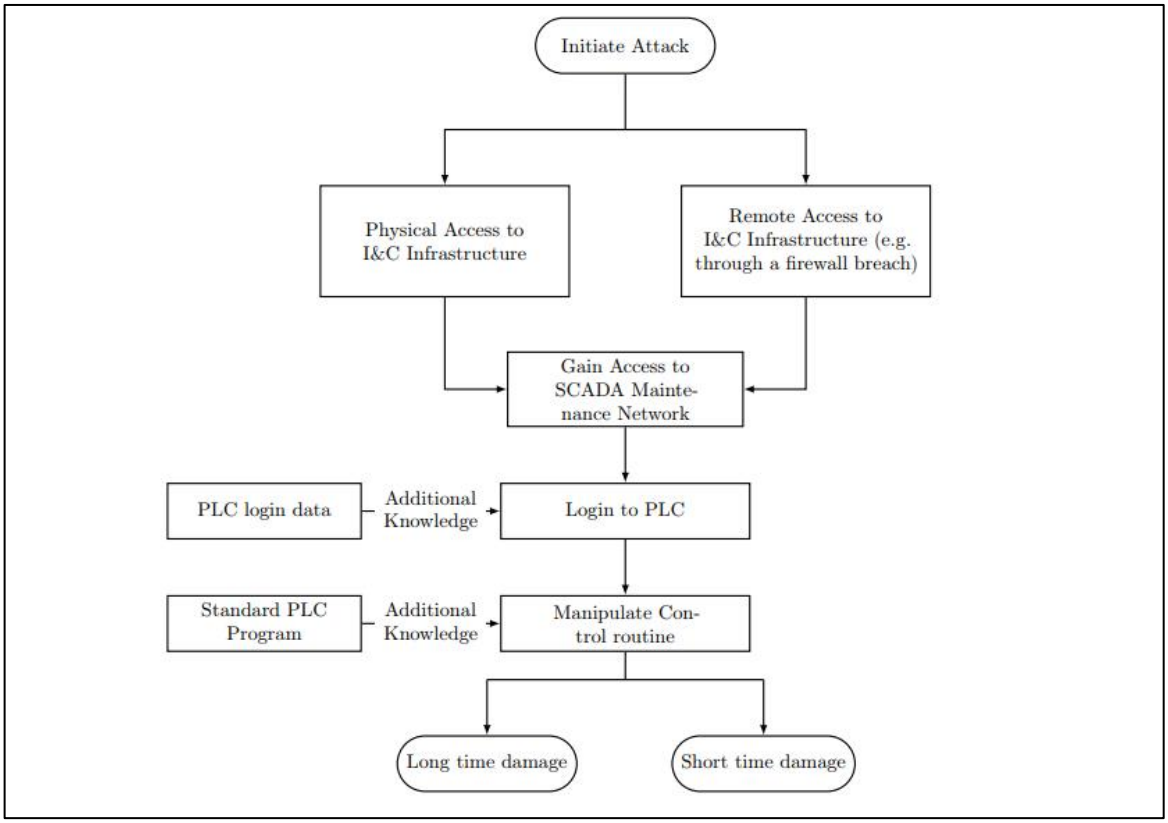

Figure 25- General attack flow

The MLP based prediction approach was adopted as it has high flexibility, allowing for changing the PLC configuration without much effort as the MLP model can just be retrained with the newly recorded data. Also the use of digital twin is recommended for physical system, as these systems will operate over a long time horizon, with subsystems being replaced several times in the expected lifetime. A digital twin will enable the adjustment for the subsystem accordingly without a full retraining, which might be necessary with a MLP based predictor.

The setup environment consists of a virtual environment using the manipulation in MATLAB because the Data broker only works on Linux-based Workstations. Furthermore, the PLCs included are only prepared to establish attacks previously covered in other related works (a Ph.D. thesis [1] D. Gupta, “Nuclear Safety related Cybersecurity Impact Analysis and Security Posture Monitoring,” Ph.D. dissertation, 2021), as the model is already trained, so a Hardware in the Loop (HiL) Setup can also be used. The requirement is that all data communication is handled over OPC UA and all variables are available to the detection algorithm. Upon the implementation of the algorithms and training of the model, along with use of attack scenarios, the test results show that all attacks could be detected even if the initial manipulation happened within the detection tolerance, as in the steam generator spoof to 14.85 m.

These results correspond to the result from the paper mentioned previously. The evaluation of the detection time of this algorithm is difficult due to several related and open questions. Indeed, the algorithm designed to prevent hardware damage in case of a successful attack. The results show that larger manipulations are detected within seconds, when the manipulation is larger than the detection tolerance. More data regarding the manipulation impact on the components' lifetime are necessary to evaluate the sufficiency of the tolerance area.

Another task aimed at finding a solution, to detect the manipulation of attackers that surpassed the protective security controls of the ICS of NPPs. Conversely, the target IACS typically is a stable system that can follow the currently needed power output. This fact is used to simulate multiple power loads and use them for the generation of the training data. The system produces more than adequate results given the mentioned constraints and false positives can be eliminated by choosing the corresponding tolerance values. However, to achieve this elimination it is necessary to choose the tolerance starting with shortly over 10% up to nearly 60% within the scaled data. These tolerance levels should be lowered drastically in the future. An option to handle this problem would be to include the reconfiguration of the models search space, by increasing the number of possible neurons in each layer substantially.

From the context of impact and reaction time, the topic needs to be researched, as there is no available data on the impact of small changes to the control of hardware components. Detailed testing is necessary to understand how different margins could impact the system, especially when some oscillations are inserted, increasing the component's load while still staying within the broad operation range. Therefore, two main questions need to be answered for further definition of the detection accuracy. First which example manipulations introduce a force necessary to decrease the expected runtime of the component? Second how much reaction time does the operator have to prevent damage to the system?

This research also raises question for data accuracy as it is a critical point within the deployment of such a system is data reliability. If the used sensor data is identical to the set of sensor data used within the control algorithms (which are manipulated), it would also be possible to record the network traffic for a given time period and replay the record. In this case, the algorithm cannot detect the executed manipulations as only correct data is presented and used for the prediction. Therefore, the question needs to be answered, how trust in the data received can be established as the algorithm can only use the available data for prediction and detection.

11.7. WP 4.7: Modelling of Security Tests Relevant Artefacts

This WP includes the modeling of all safety and security-relevant artefacts at the network protocol level together with the partner HS-MD. The modeling is intended to simulate and evaluate the effects of safety-relevant events on functional safety and nuclear safety. The risks are then prioritized to formulate suitable test approaches for attack scenarios. Lightweight MAC security solutions are to be studied, implemented, and tested for use in critical infrastructures. The tool support is important as a basis for possible later extensions for use in the nuclear industry and for critical infrastructures.

Thus modelling all safety- and security-relevant artifacts at the network protocol level allows to examine the relevant vulnerabilities i.e. the impact of security-related events on functional safety and nuclear safety to be assessed and simulated. Risks can then be assigned and prioritized to conduct an effective and appropriate approach. In this approach, attack scenarios are formulated and tested with the communication protocols. Assuming that maintaining integrity plays a crucial role in restricting and even preventing the manipulation of communications, possible solutions are reviewed to determine their usefulness. Recent advancements in cryptographic protection measures for critical infrastructure have led to the development of lightweight MAC security solutions. These solutions support time-critical communication with significantly reduced resource requirements. Within the framework of the SMARTEST2 research project, these solutions have been thoroughly investigated, prototypically implemented, and tested for small example critical infrastructure scenarios. A future expected project outcome is the development of a secure switch that supports MAC-based security measures and offers secure key exchange functionality. The overall goal is to maintain the integrity of network communication to eliminate misuse or manipulation and increase the trustworthiness of communication over the network. The protocols currently used in nuclear power plants, the protocols applied in new automation systems, and the lightweight approaches will undergo thorough security testing.

The main objective of WP4.7 within the Project was to develop and refine models for security tests that are relevant to the artefacts used in Digital Instrumentation & Control (I&C) systems in Nuclear Power Plants. This involved creating a comprehensive framework that can simulate and analyze potential security vulnerabilities in various components of I&C systems. This framework is also used to carry penetration testing on the I&C systems.

The primary objectives of WP4.7 were:

- To develop models representing the internal structure of software, communication networks and network protocols of I&C systems.
- To simulate intelligent attack scenarios to identify potential security vulnerabilities.
- To integrate these models with existing testing frameworks and evaluate their effectiveness.

A TXS Rack and two notebooks were used in the testing environment. The focus was on the Monitoring and Service Interface (MSI) barrier, which acts as an interface between Automation Computers (AC) in zone 1 (Highest security level) and other computers in zones 2 and 3.

A Gateway computer in zone 3 is assumed to be compromised and infiltrated with malicious code. It serves as launch point for various attacks. Penetration testing scripts, fuzz attacks, and Denial of Service (DoS) attacks were executed from this gateway computer to evaluate if an attacker could breach the MSI Barrier and access the AC in zone 1. The partner FRA defined several test methodologies to conduct the testing activities:

- **Penetration Testing:** Python scripts were used to simulate attempts across the MSI Barrier. The tests aimed to determine if unauthorized access could be achieved, thus compromising the AC in zone 1.
- **Fuzz Testing** involved sending a large volume of random data to the MSI Barrier to identify potential vulnerabilities. The objective was to observe how the system handled unexpected or malformed data inputs and to identify any weaknesses that could be exploited.
- **Denial-of-Service (DoS) Attacks**: DoS attacks were simulated by overwhelming the MSI Barrier with a flood of requests from the compromised Gateway computer. The goal was to assess the system's resilience to such attacks and its ability to maintain operational integrity under stress.

The penetration testing scripts revealed that the MSI Barrier effectively prevented unauthorized access to the AC in zone 1. No successful breaches were recorded, indicating a robust defense against direct penetration attempts. Fuzzy testing identified several instances where the MSI Barrier's performance degraded under abnormal data conditions. While no critical vulnerabilities were found, the tests highlighted areas for improvement in input validation and error handling. The DoS attacks caused temporary slowdowns in the MSI Barrier's response times but did not lead to a complete system failure. The AC in zone 1 remained protected, although the MSI Barrier's capacity to handle prolonged attack scenarios requires further enhancement.

The activities under WP4.7 successfully demonstrated the effectiveness of the MSI Barrier in preventing unauthorized access to critical I&C systems in NPPs. The penetration and fuzz testing provided valuable insights into the system’s security posture, while the DoS attacks underscored the need for further resilience improvements. The developed models and testing methodologies will serve as a foundation for ongoing and future security assessments of automation systems in nuclear and other critical infrastructures.

11.8. WP 4.8: Security Testing of Formal Specifications

Formal methods enhance system understanding by identifying inconsistencies, ambiguities, and incompleteness, thus aiding in risk awareness. However, they are less popular in the industrial domain compared to semi-formal methods due to their lack of practicality. The goal of SMARTEST2 WP 4.8 is to apply a formal method to analyze system vulnerabilities and provide a practical approach to bridge the gap between formal methods and practicality. To achieve this goal, the PhD student worked on developing a model that could be expressed in formal language using an easy-to-use, reliable and effective approach.

The objective of the study carried out develop an integrated safety with cybersecurity analysis approach, which is applicable for Industrial Control Systems (ICS). While developing this approach, care was taken not only to examine the entire system, but also to provide effective details. In the study, the Refueling Machine (RM) system was discussed. The studies on the system are listed below;

1. Reverse engineering RM functional separation in a formal language
2. Identification of the system hazards
3. Analysis of the possible attacks that can cause a specific hazard
4. Representing the analysis results in Casual Fault Graph (CFG) and Node List

The main function of RM is to unload and reload the fuel assembly. Although it has many functions besides what is stated, it has been approached in terms of fuel assembly for the study.

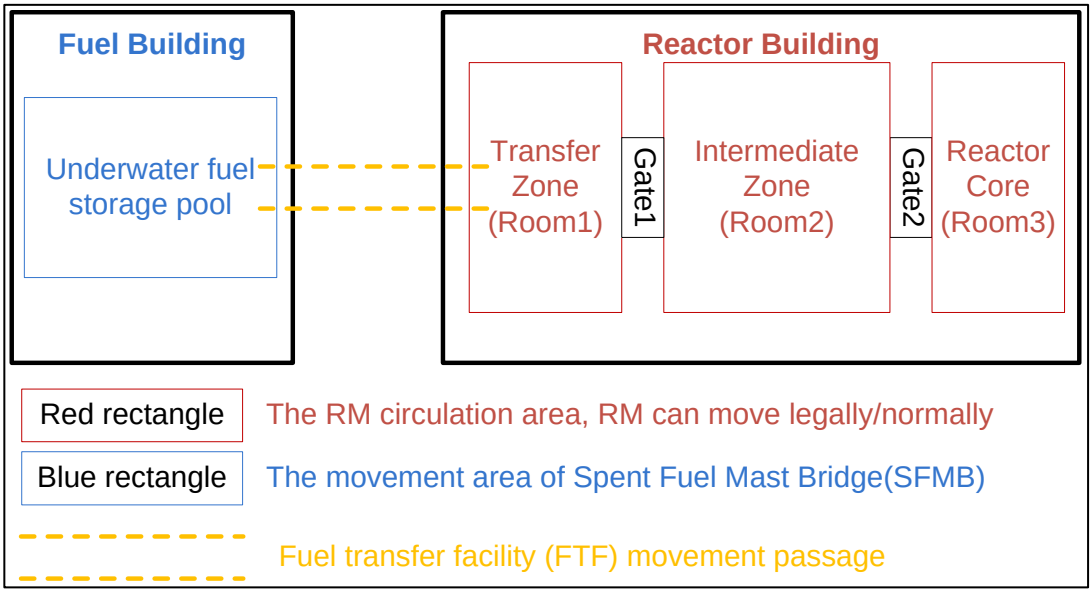

Figure 26- Example layout of a refueling site

As shown simply in the Figure 26, Fuel Building locates beside the reactor core and used to store the fuel assembles (FA). Before the refueling starts, Fuel Transfer

Facility (FTF) transfers the FA to the Transfer Zone (Room 1). Then RM carries it from Room 1 to Reactor Core (Room 3) and then lower it to the target cell.

Other functions of RM are shown in Figure 27. Classification of these functions have been made by their implementation mechanism (e.g. OPLC, SPLC, camera presence)

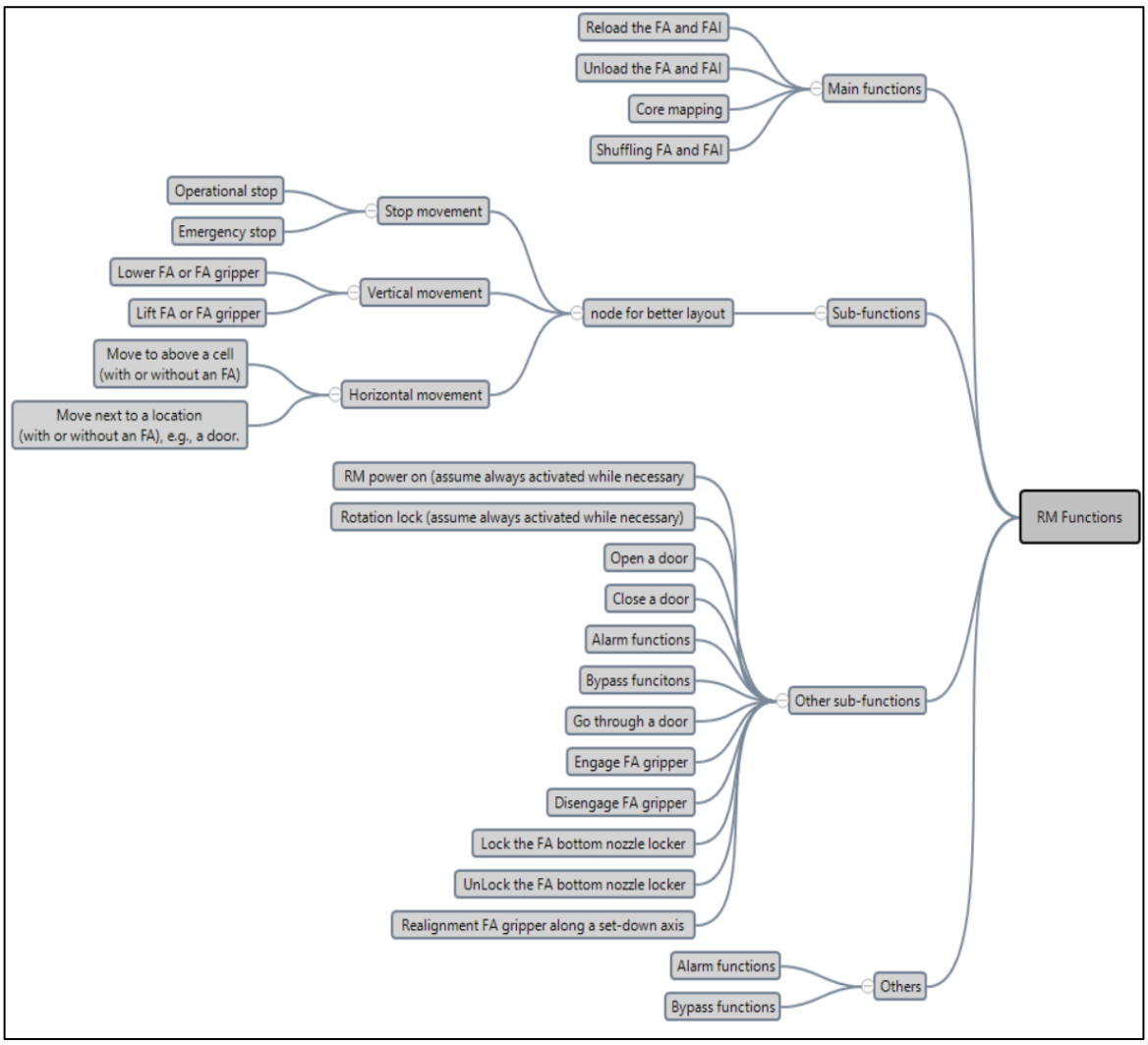

Figure 27-Functions of Refueling Machine

This is only the initial impression of the RM system. To be sufficient for a thorough safety and cybersecurity analysis, a deep understanding should be obtained. To get that deep understanding PhD student applied Reverse Engineering on RM functional specification and expressed it in Hoare Triple to reach formal language goal. Reasons for using the Hoare Triple method in this study;

- Format is compatible with the functional specification
- It is a powerful tool to ensure that the software is functioning correctly

- Each module can be verified independently, which facilitates the analysis of large and complex systems

To create formally expressed Hoare Triple the requirements are identifying the function and verifying preconditions and post conditions. In order to complete expression, OPRA principle (Table 3) has used (only OPR used for this research).

Table 3- OPRA principle

OPRA	Description
Object	Objects relevant to the function execution, both virtual and physical
Property	Properties of an object
Relation	Relations between among objects
Assertion	As assertion in formal logic, but it is not involved in the FS

In Figure 28 it is shown that one example for Hoare Triple.

$$
\begin{aligned}
&Precondition(Lower\_FA\_TargetCell)\\
&\Longleftrightarrow\\
&RMAbove(TargetCell) \wedge InRoom(RM, CoreArea)\\
&\wedge GripperAbove(FAGripper, TargetCell)\\
&\wedge \mathbf{FAAbove(FA,TargetCell)}\\
&\wedge PlacedHoistAlong(FAHoist, TargetCell\_Axis)\\
&\wedge RMnextto(TargetCellNexttoTo)\\
&\wedge Vertical(TargetCell) \wedge \mathbf{Empty(TargetCell)}\\
&\wedge (OnloadRM) \wedge Engaged(FAGripper) \wedge \mathbf{FAHighLevel(FA)}\\
&\wedge \mathbf{GripperHighLevel(FAGripper)}\\
&\wedge GripperInside(FAGripperFingers, FA\_TopNozzle)\\
&\wedge RMStopped(H) \wedge RMStopped(Z)\\
&\wedge RotationLocked(FAGripper) \wedge (NoAlarm)
\end{aligned}
$$

$$
\begin{aligned}
&Postcondition(Lower\_FA\_TargetCell)\\
&\Longleftrightarrow\\
&\mathbf{FAInside(FA,TargetCell)} \wedge InRoom(RM, CoreArea)\\
&\wedge PlacedHoistAlong(FAHoist, TargetCell\_Axis)\\
&\wedge RMnextto(TargetCellNexttoTo) \wedge Vertial(TargetCell)\\
&\wedge \mathbf{Full(TargetCell)} \wedge (OnloadRM) \wedge Engaged(FAGripper)\\
&\wedge \mathbf{FALowLevel(FA)} \wedge \mathbf{GripperLowLevel(FAGripper)}\\
&\wedge GripperInside(FAGripperFingers, FA\_TopNozzle)\\
&\wedge RMAbove(TargetCell) \wedge RMStopped(H) \wedge RMStopped(Z)\\
&\wedge RotationLocked(FAGripper) \wedge (NoAlarm)
\end{aligned}
$$

Figure 28- Example of expressed preconditions and post conditions

Then Partner FRA PhD student check and update functional specification. For checking correctness and completeness of the functional system AI planning has used. In the end, sufficient knowledge of the system reached with the reverse engineering. Identification of the system hazards is based on the examined functional separation. In other words, the results of reverse engineering are the key

source of the analysis approach of the study. The first step of the analysis is to make the correct definition of "hazard" for the system being studied. According to IEC 61508, a hazard is defined as a source of harm[3]. Therefore, to prevent severe consequences, it is essential to identify the factors that could lead to these outcomes (Figure 29). To reach system hazards;

1. System has described formally
2. Deviations generated based on the examined FS
3. Potential consequence of the derivations evaluated
4. Hazards sorted out according to their severity level and our selected acceptance level

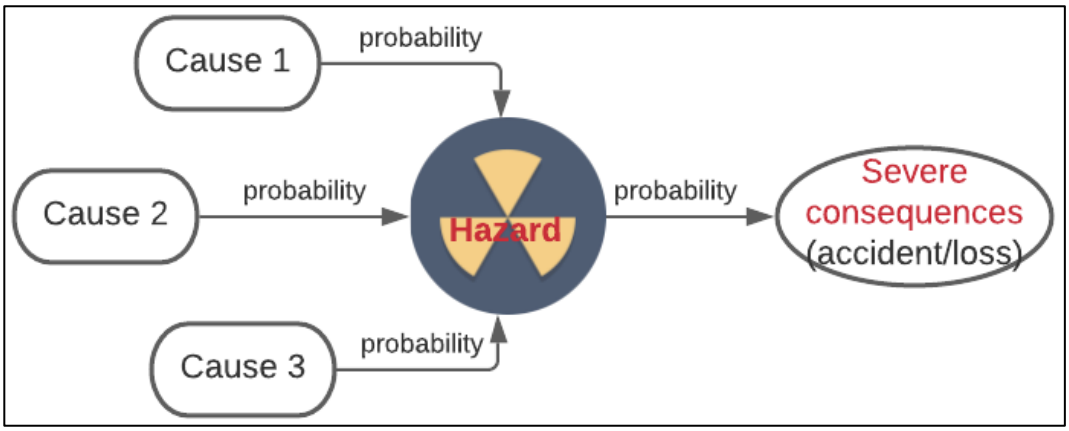

Figure 29- Relationship between causes, consequences and hazards

Cyber security analysis were carried out on the logic of “which attacks because which hazard scenarios”. First, the relationship between hazard and compromised function[4] was examined. Since a hazard can contain more than one compromised function, the combination of causes of each compromised function involved was considered when examining the causes of hazards. Thus, the hazard analysis was converted to the compromised functions analysis.

In the following there are two options of continue to the analysis (Figure 30), first is building attack models and analyze feasibilities and second one is using analysis frameworks to perform the analysis.

[3] Dean S. IEC 61508 — Understanding Functional Safety Assessment. Measurement and Control. 1999;32(7):201-204. doi:10.1177/002029409903200703

[4] Compromised function: functions are not executed as expected

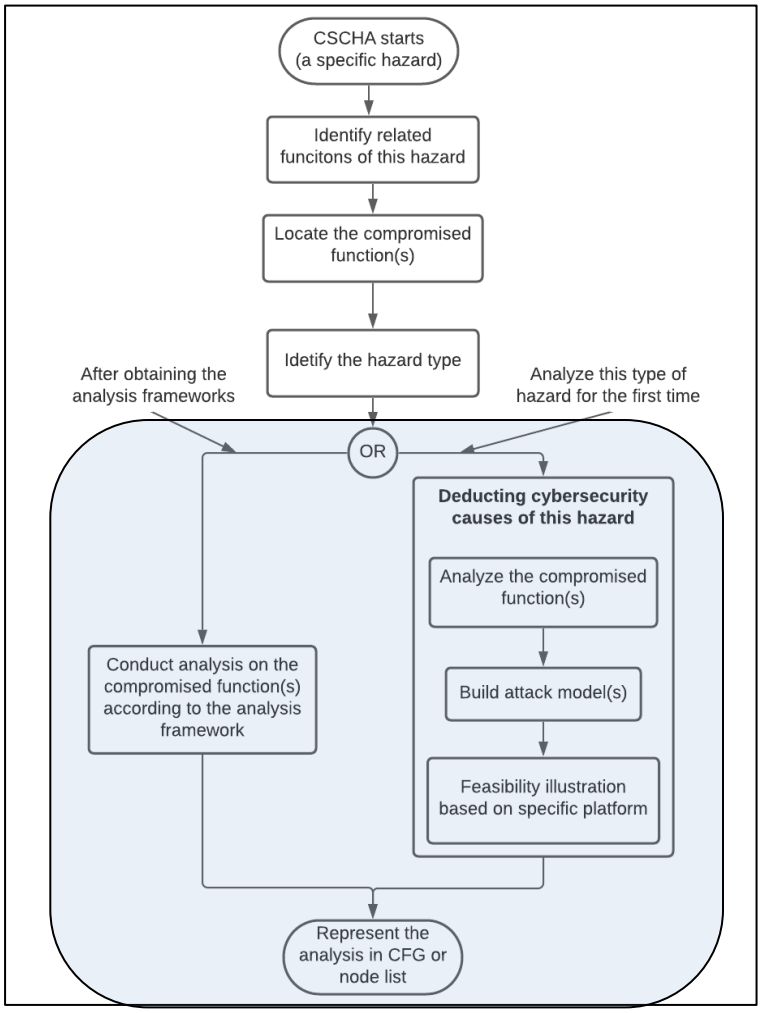

Figure 30- Workflow of hazard analysis (blue part shows the two options)

In this case, PhD students used the second option by generating frameworks. An example hazard scenario case is given to better understanding. The case is “The door is closed but the RM is still moving towards to door”. According to the Figure 5, first step is the identification of the compromised functions by examining involved objects and functional specification. Those functional specifications are “Go Through the Door” and “Horizontal Movement Stop” functions (Figure 31).

$$Precondition(\text{HMS1}) \Leftrightarrow Movement(RM, X) \wedge NextTo(RM, Door) \wedge Closed(Door) \wedge \ldots$$

$$Postcondition(\text{HMS1}) \Leftrightarrow Movement(RM, X) \wedge \neg Activated(RM\_X\_Motor) \wedge \neg Released(RM\_X\_Brake) \wedge \ldots$$

$$Precondition(\text{Go\_Through\_Door}) \Leftrightarrow Open(Door) \wedge Open(FA\_Hoist\_Gripper) \wedge \ldots$$

Figure 31- Functional specifications of example hazard scenario

For the Horizontal Movement Stop Function, preconditions are satisfied but the function is not executed. In the other hand for the Go Through the Door Function,

preconditions are not satisfied but the function is executed. So, these two functions are compromised.

According to the Figure 31, the possible ways of compromising these two functions should be analyzed. As a result of the analysis, it can be concluded that the CPU was tricked by the attacker with the multiplexing method. The output of the analyses performed on the CPU can be found in Figure 32.

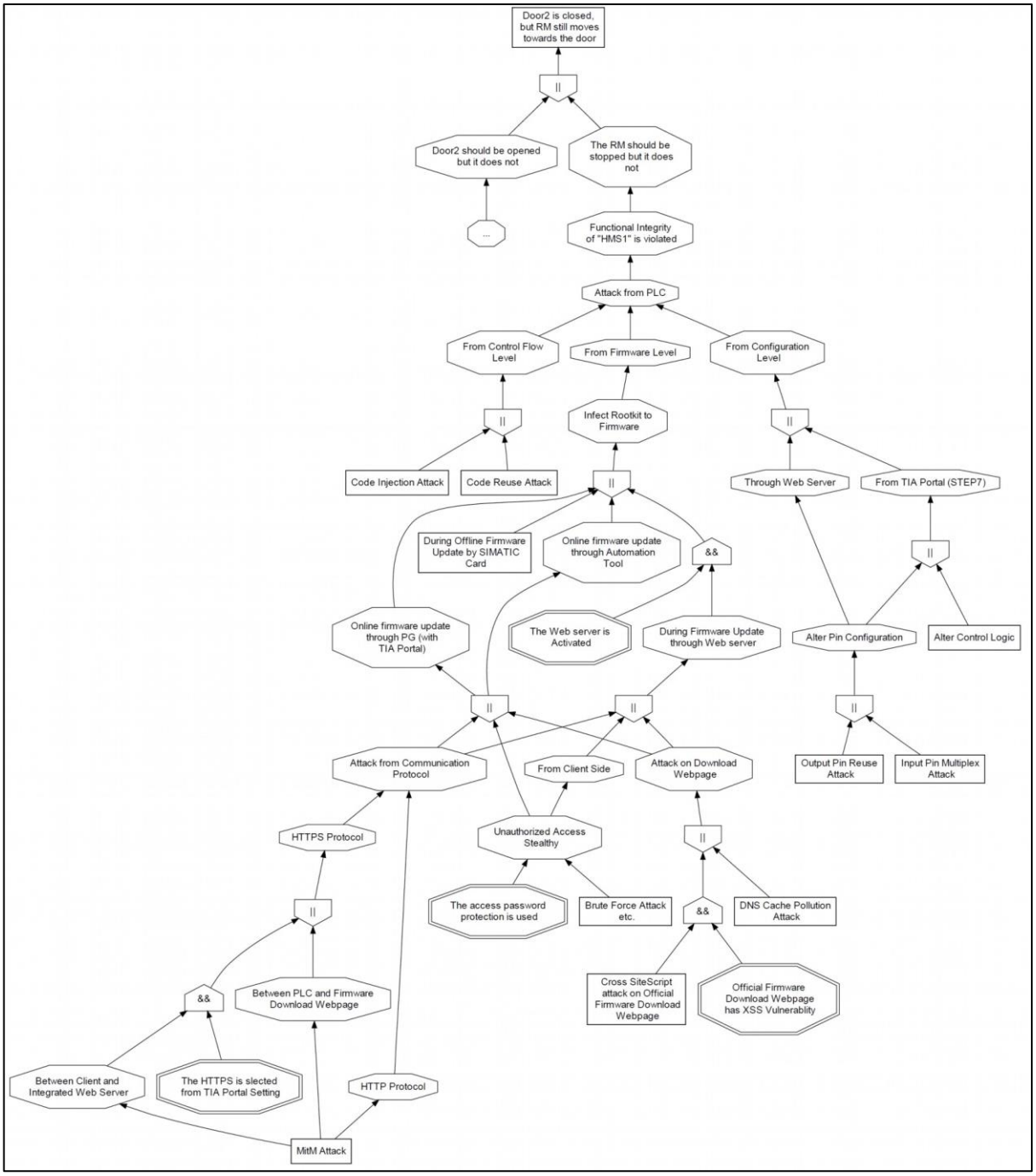

Figure 32- Basic output of the analysis based on CPU part

When the major components in ICS are examined, not only CPU-based, the PhD student used a "node list"[5] because it would be difficult to represent the outputs graphically (Figure 33).

```
------------------------------------------------------------
5. SPLC+OPLC+Camera--LowerFA+brakes+alarm--type II hazard
SPLC+OPLC+Camera(the Refueling Schdule Table (RST) and the camera are involved in the hazard)
    NC_SPLC_ControlledAction     //this node is defined in the "Only SPLC" framework
    NC_OPLC+SPLC+Camera+RST_ControlledAction   //the OPLC controlled part
        NC_CPU_CorrectInfo
            NC_CPU_CorrectCommand
            NC_CPU_ModifiedCommand
        NC_CPU_FakeInfo    //the OCPU receives fake information is fake
            NC_CPU_RecIncorrectCommand_Operator   //this node is defined in the "OPLC+Camera"
                                          //&& indicates the conjunction of NC_CPU_RecIncorrectCommand_Operator
                                             //and NC_CPU_RecFakeRSTInfo
                NC_CPU_RecIncorrectCommand_Operator
            &&
                NC_CPU_RecFakeRSTInfo   //the OCPU receives fake RST (Refueling Schdule Table)
                                       //(it indicates which cell the FA should be lowered in)
                    NC_OCPU_RecIncorrectRST_Sensor  //the OCPU receives fake info from the sensor
                        NC_MitM_TransChannel
                        NC_PII
                            NC_TagPin
                        NC_InputModule
                            NC_InfectRootkit
                &&                      //&& indicates "NC_OCPU_RecIncorrectRST_Sensor&&NC_OCPU_RecIncorrectRST_SCPU"
                    NC_OCPU_RecIncorrectRST_SCPU     //the OCPU receives fake RST from the SCPU
                        NC_SCPU_Send_IncorrectRST
                            NC_SCPU_Rec_RightInfo_Sensor
                                NC_SCPU_IncorrectCommand //the SCPU sends incorrect RST information to the OCPU
                                    NC_CodeModification
                                    NC_CotrolFlow
                                    NC_PIQ
                            NC_SCPU_Rec_Incorrect_Sensor

                        NC_SCPU_Send_CorrectRST
                            NC_MITM_TransChannel
                                NC_MITM_Sensor_InputModule
                                NC_InputModule
                                    NC_MITM_PROFINET
------------------------------------------------------------
```

Figure 33- Node list representation of the analyze made upon every major component

To summarize how to perform the cybersecurity causes analysis on system hazards, the involved compromised functions are analyzed first, as a hazard is composed of various compromised functions. Each type of compromised function is then analyzed from different levels by building attack models, and their feasibilities are examined. The analysis of hazards is obtained by simply combining the analysis of each compromised function. To improve analysis efficiency, the general parts of each type of analysis are extracted into nodes, allowing them to be reused, updated, and transplanted easily. Two methods are used to represent the analysis results: one in a graphical form and the other in a textual form. The former is more vivid, while the latter is more compact, and also provides a foundation for later automating the analysis.

As a result, the partner FRA developed an approach to achieve the goals of WP 4.8. In this approach, the system is first studied by formally reverse engineering functional specification (FS). Then, the system hazards are identified, and the cybersecurity causes are analyzed. An approach is proposed to check whether the reverse-engineered results are correct and complete (at a specific level). A limitation of this checking approach is that when there is a conflict among the

[5] Node List: Pick up each main component or general part that exists in many compromised function analyses as a node, omit the very detail representation under each node.

specified goal states, the planner does not provide any reminder, which might bring a little inconvenience. At the hazard identification stage, a reliable way to generate deviations, which contributes to identifying system hazards relatively completely, is proposed. The limitation of this hazard identification approach is the amount of work, but if this process can be made more automated later on, then it will be more efficient. When the cybersecurity causes of system hazards are analyzed, possible attacks at each level, component, and the whole system structure are identified, and contributions are made to improving analysis efficiency by generating analysis frameworks. In the analysis, the safety PLC is treated mostly the same as the standard PLC except for the fail-safe input/output part, but more detailed differences need to be considered in practice.

In the future, if the overall analysis can be performed automatically, for example, the hazard identification and the cybersecurity causes analysis parts, it would be more efficient.

11.9. WP 4.9: Testing of Semi-Formal Representation of Security Controls

Work Package 4.9 focused on the testing of semi-formal representations of security controls for Digital Instrumentation & Control (I&C) systems used in Nuclear Power Plants (NPPs). The partner FRA aims to develop, implement, and evaluate semi-formal methods to represent security controls, enhancing the systematic approach to detecting and mitigating security vulnerabilities in these critical systems.

Thus, the primary objectives of WP 4.9 include:

To develop semi-formal representations of security controls for I&C systems

To integrate these representations into existing testing frameworks

To evaluate the effectiveness of these representations in improving the detection of security vulnerabilities and enhancing the overall security posture.

A semi-formal approach combines the rigor of formal methods with the flexibility of informal methods. Various security controls were identified and documented using semi-formal representations such as state diagrams, flowcharts, and structured natural language descriptions. The semi-formal representations were integrated into the existing security testing frameworks developed in other work packages. Tools and platforms supporting semi-formal methods were utilized to facilitate the integration and application of these representation. The semi-formal representations were tested in a controlled environment using the I&C system’s testbed. Various attack scenarios were simulated to assess the effectiveness of the security controls represented semi-formally. Metrics of evaluation included detection rates and overall impact on system security.

Security controls, such as access controls, data integrity checks, and communication security protocols, were documented using semi-formal methods. Tools like UML (Unified Modeling Language) were used to create state diagrams and flowcharts representing these controls. The semi-formal representations were mapped to the corresponding components and processes within the existing security testing frameworks. Python scripts and other automated testing tools were modified to incorporate these semi-formal descriptions, ensuring they were adequately tested.

Simulated attack scenarios included penetration tests, fuzz testing, and denial-of-service attacks. Each scenario was executed multiple times to gather sufficient data for analysis. The performance of the semi-formal representations in detecting and mitigating these attacks was meticulously recorded and analyzed.

Overall, the semi-formal representations significantly improved the detection rate of potential security vulnerabilities compared to purely informal methods, due to the clearer and more precise definitions of security controls. The structured nature of semi-formal methods facilitated better identification and documentation of security controls, leading to more effective testing. The integration of semi-formal representations enhanced the overall security posture of the I&C systems by providing a more systematic and rigorous approach to security testing. The approach proved beneficial in identifying complex vulnerabilities that might have been overlooked using purely informal methods.

12. National and international related progress between 2018 and 2024

Section 6 contains an overview of the state-of-the art in 2014/2015 from different perspectives, including standardization, publications and commercial products. Section 8 contains a snapshot of the corresponding state-of-the art as of end 2018 and beginning of 2019.

This section provides a brief summary of major cybersecurity and especially cybersecurity testing related developments between 2018 and 2024.

During execution of our project, the following became known to SMARTEST-FRA R&D project and partially influenced the research decisions and progress.

- Standardization Council Industry 4.0 (SCI 4.0): R&D project members and PhD candidates contributed to the SCI 4.0 since December 2015, initially for the Functional Safety and the Cybersecurity technical working groups. This support is ongoing, especially with regard to input for past and new white papers. These included a Sino-German whitepaper on Functional Safety, a whitepaper on cybersecurity testing and an ongoing whitepaper on cybersecurity grading.

- CEN/CENELEC CLC/TC45AX: Technical Committee TC45AX of CEN/CENELEC decides on all Nuclear IEC standards on I&C, including Cybersecurity, on whether selected nuclear IEC standards shall become mandatory EU standards, e.g. indicated by the prefix EN (European Norm), e.g. EN IEC 62645. National translation of these EN standards will also indicate the concerned national standards institute, e.g. DIN EN IEC 62645. Members and PhD candidates of the SMARTEST and SMARTEST2 R&D teams supported especially the work on IEC 63096 on cybersecurity controls for the nuclear domain. This including the translation or translation review to the German language.
  Note: Additionally, the translation to the Chinese language was supported. This will facilitate EU companies to achieve faster acceptance for Nuclear Safety I&C and Cybersecurity products and services offered for the Chinese nuclear industry, by avoiding the needed for additional certifications according to national only cybersecurity standards.

- Manufactured in China 2025: This is the corresponding program to the Standardization Council Industry 4.0 and was supported in the context of the completed and ongoing Sino-German activities, currently related to a whitepaper on security grading.

- IEC 62645 [14]: The top-level nuclear IEC cybersecurity standard received an amendment in 2019 and was translated to German language. No new release was published during the SMARTEST R&D project execution.

- IEC 62859 [15]: This standard is to some extend similar to the broader IEC TR 63069 for the industry domain. However, as it is targeting only nuclear facilities it is more precise an in line with the safety and security grading defined by the nuclear IEC standards. During the SMARTEST2 R&D project no new version was published.

- IEC TR 63069: This IEC Technical Report (TR) within IEC TC65 provides a general guidance on topics to be addressed as part of the functional safety and

cybersecurity considerations. Members of the SMARTEST and SMARTEST2 R&D project are involved in the corresponding mirror committee “DKE/TBINK AK IT”, including two professors mentoring some of the SMARTEST2 R&D a candidates. Work on a new version of IEC TR 63096 is currently (June 2024) ongoing. Consensus is difficult, as consistency over multiple industry domains has to be achieved for a significant part of both, functional safety and cybersecurity.

- IEC 63096: This is the main nuclear IEC cybersecurity standard on security controls for the nuclear domain. The last international intermediate meeting of IEC TC45/SC45A WG9 which addresses the nuclear IEC cybersecurity topics was hosted in February 2019 by Framatome GmbH and a subsequent corresponding intermediate meeting was hosted in 2023 by Siemens Energy in Erlangen, both with participation of members and PhD candidates of the SMARTEST and/or SMARTEST2 R&D. The latest international intermediate meeting of IEC TC45/SC45A WG9 was held in Budapest in May 2024. By the end of the SMARTEST2 R&D final report preparation (June 2024) now amendment or new version of IEC 63096 was published as compared to IEC 63096:2020 and DIN EN 63096:2021.

- IAEA NSS No. 33-T: The 2018 version of the “Computer Security of Instrumentation and Control Systems at Nuclear Facilities – Technical Guidance” will be updated during a first consultancy meeting on a revision of IAEA NSS No. 33-T in the week from 2nd to 6th September 2024. Accordingly, no new version was published during the SMARTEST2 R&D project execution. Information technology – Security technology – Methodology for IT security evaluation, GB/T 30270-2013. This standard provides a methodology for the evaluation of IT security. It also proposes to support the application of standard ISO/IEC 15408. The methodology for IT security evaluation mentioned in this standard is limited to EAL1~EAL4 evaluation which are defined in ISO/IEC 15408, but it does not provide EAL5~EAL7 and other evaluation guidelines.

- Information security technology – Guide of implementation for information security risk assessment, GB/T 31509-2015. This standard specifies the process and method for the implementation of information security risk evaluation. It can be applied to the management of information security risk evaluation projects of non-confidential information systems by various security evaluation agencies or evaluated organizations, and guides the organization, implementation, and acceptance of risk evaluation projects.

- Information security technology – Technical requirements and testing and evaluation approaches for network – based intrusion detection system, GB/T 20275-2013. This standard specifies the technical requirements and test evaluation methods of the network intrusion detection system. The requirements include security function requirements, self-security function requirements, security assurance requirements and test evaluation methods, and the classification requirements of the network intrusion detection system are proposed. It can be applied during design, development, testing and evaluation of network intrusion detection systems.

- Information security technology – Technical requirements, testing and evaluation approaches for information system security audit product, GB/T 20945-2013. This standard specifies the technical requirements and test evaluation methods for

information system security audit products. The technical requirements include security function requirements, their own security function requirements and security assurance requirements. Also the classification requirements for information system security audit products are proposed. It can be applied during the design, development, testing and evaluation of information system security audit products.

- Information security technology – Testing and evaluation approaches for network vulnerability scanners-GB20280. This standard specifies the testing and evaluation method, to network vulnerability scanners. The testing and evaluation approaches are limited to the products that are used for IT systems scanning (manually or automatically). Products that are specifically for database system scanning are not covered by this standard.

- Information security technology – Security technical requirements and testing and evaluation approaches for firewall-GB20281. This technical report specifies the technique requirements and the testing and evaluation method for firewall products where the TCP/IP is used as transportation protocol. In this standard, the firewalls are characterized into 4 categories. Also proposed three (3) security levels for these firewall products security performances.

13. List of own publications

The following list of publications is included as well in the references section. Starting with [64] until [132].

- Asmaa Tellabi, Ines Ben Zid, Edita Bajramovic, Karl Waedt, Safety, “Cybersecurity and Interoperability of Modern Nuclear Power Plants”, Athens PESARO, 2018
- Felix Freiling, Edita Bajramovic, “Principles of Secure Logging for Safekeeping Digital Evidence”, Hamburg IMF, 2018
- Yuan Gao, Xinxin Lou, Venesa Watson, Deeksha Gupta, “Industry 4.0 Standardization on Cybersecurity & Interoperability from the Nuclear Integrator’s Perspective”, Warrington NuclearIndCtrlSec, 2018
- Juergen Bochtler, Karl Waedt, Edita Bajramovic, Venesa Watson, “Development of a new IEC Standard on Cybersecurity Controls for I&C in Nuclear Power Plants - IEC 63096”, Vienna IAEA, 2018
- Xinxin Lou, Karl Waedt, Yuan Gao, Ines Ben Zid, Venesa Watson, “Combining Artificial Intelligence planning advantages to assist preliminary formal analysis on Industrial Control System cybersecurity vulnerabilities”, Iasi, ROMÂNIA, 2018
- Deeksha Gupta, Edita Bajramovic, Mithil Parekh, Karl Waedt, “Cyber Threat Scenarios for Electrical Systems of Nuclear Power Plants”, London ICONE, 2018
- Venesa Watson, Edita Bajramovic, Xinxin Lou, Karl Waedt, “Example of graded and lifecycle phase-specific security controls for nuclear i&c and ePs use cases”, London ICONE, 2018
- Asmaa Tellabi, Ludger Peters, Christoph Ruland, Karl Waedt, “Security Aspects of Hardware Virtualization Technologies for Industrial Automation and Control Systems”, Berlin GI, 2018
- Mithil Parekh, Yuan Gao, Asmaa Tellabi and Karl Waedt, “Secure Interoperability of I&C and IT systems”, Berlin GI, 2018
- Venesa Watson, Xinxin Lou, Yuan Gao and Karl Waedt, “Addressing Security gaps in Industries seeking to adopt I4.0”, Berlin GI, 2018
- Venesa Watsons and Jochen Sassmannshausen, “Time Sensitive Ethernet Technology for Next Generation CPS/Industry 4.0”, Berlin GI, 2018
- Asmaa Tellabi, Karl Christoph Ruland, Ines Ben Zid, Karl Waedt, “Virtualization on Secure Platforms for Industrial Applications”, Shanghai, ICRMS, 2018
- Jochen Link, Karl Waedt, Ines Ben Zid, Xinxin Lou, “Current Challenges of the Joint Consideration of Functional Safety & Cyber Security, their Interoperability and Impact on Organizations”, Shanghai, ICRMS, 2018
- Venesa Watson, Edita Bajramovic, Mahlet Bejiga, Karl Waedt, “Designing Trustworthy Monitoring Systems”, Shanghai, ICRMS, 2018
- Venesa Watson, Jochen Saßmannshausen, “An Evaluation of Time-Sensitive Ethernet Technology for Next Generation CPS”, St Petersburg, ICPS, 2018
- Venesa Watson, Jochen Saßmannshausen, “Comparion of AFDX, AVTP, PROFINET and TTE”, St Petersburg, ICPS, 2018
- Edita Bajramovic, Venesa Watson, “Insider Threat Modelling and Analysis for Power Plants”, Rome, ISNCC, 2018

- Venesa Watson and Jochen Sassmannshausen, “Time-Sensitive Ethernet Technology for Next Generation CPS/Industry 4.0”, Barcelona, CyberICPS
- Venesa Watson and Mahlet Bejiga, “Dependability Analysis of the AFDX Frame Management Design”, Sweden, SAFECOMP, 2018
- Xinxin Lou, “Cybersecurity analysis of Industrial Control System towards system function view”, Erfurt VDE, FunkionaleSicherheit, 2019
- Asmaa Tellabi, Edita Bajramovic, Sebastien Champigny, Mathias Lange, Karl Waedt, Yongjian Ding, “International Standards as Precondition for Prevention of Cyber Attacks on Nuclear Power Plant”, Berlin, KTG, 2019
- J. Schindler, V. Watson, K. Waedt: Interoperability of fast charging station with battery booster, IACS, GI2019, Kassel, 2019
- Ines Ben Zid, Deeksha Gupta, Xinxin Lou, Dr. Karl Waedt, “A Functional Specification Based Approach For Analyzing The Cyber Security Of End User Interfaces Within NPP”, Tsukuba ICONE, 2019
- Asmaa Tellabi, “Security aspects of FPGA and virtualization case studies”, Kassel, GI, 2019
- Edita Bajramovic, Deeksha Gupta, Yun Guo, Karl Waedt, Anis Bajramovic “Security Challenges and Best Practices for IIoT”, Kassel, GI, 2019
- Ines Ben Zid, Xinxin Lou, Mithil Parekh, Karl Waedt, “The application of Artificial Intelligence for Cyber Security in Industry 4.0”, Kassel, GI, 2019
- Josef, Xinxin Lou, Venesa Watson, Karl Waedt, “Interoperability of lithium ion battery packsfor fast charging station booster”, Kassel, GI, 2019
- Venesa Watson, Jochen Sassmannshausen and Karl Waedt, “Secure Granular Interoperability with OPC UA”, Kassel, GI, 2019
- Xinxin Lou, Yun Guo, Yuan Gao, Karl Waedt, Mithil Parekh, “An idea of using Digital Twin to perform the functional safety and cybersecurity analysis”, Kassel, GI, 2019
- Deeksha Gupta, D. Govindaraj, Robert Altschaffel, Karl Waedt, “Blue Team Support For Electrical Power System (EPS) Related Cybersecurity Readiness”, Vienna IAEA ICONS, 2020
- Xinxin Lou, Peter Ladkin, Karl Waedt, Ines Ben Zid: Applying reverse engineering to perform integrated safety and cybersecurity analyses of system functionality, Proceedings of the 28th Safety-Critical Systems Symposium, York, UK, 2020
- Tellabi; Xinxin Lou, Karl Waedt: A Prototype of a new Virtualized Secure Embedded Product for Operational and Safety Related I&C Functions, International Conference on Nuclear Security (ICONS 2020), Vienna, 2020
- Yan Gao, Xinxin Lou; Operational Security Analysis and Challenge for IoT Solutions, INFORMATIK2020 GI/IACS Industrie 4.0, Karlsruhe, Germany, 2020
- Mithil Parekh, Karl Waedt, Asmaa Tellabi: Aligning with cybersecurity framework by modelling OT security, INFORMATIK2020 GI/IACS Industrie 4.0, Karlsruhe, Germany, 2020
- Venesa Watson, Christoph Ruland, Karl Waedt; MAC-layer Security for Time-Sensitive Switched Ethernet Networks, INFORMATIK 2020 GI/IACS Industrie 4.0, Karlsruhe, Germany, 2020

- Ines Ben Zid, Xinxin Lou, Karl Waedt “Consideration of Artificial Intelligence for Cybersecurity Aspects Of I&C Systems”, Vienna IAEA ICONS, 2020
- Yun Guo, Xinxin Lou, Edita Bajramovic, Karl Waedt, “Cyber Security Risk Analysis And Technical Defense Architecture Research Of ICS In Nuclear Power Plant Construction Stage”, Vienna IAEA ICONS, 2020
- Schindler, Asmaa Tellabi, Karl Waedt; Gossip protocol approach for a decentralized energy market with OPC UA client-server communication, INFORMATIK2020 GI/IACS Industrie 4.0, Karlsruhe, Germany, 2020-09
- Deeksha Gupta, Christine Bürger, Ines Ben Zid, Karl Waedt, “BSI Grundschutz - neue Anforderungen für mobile Servicegeräte für Rückbau und Normalbetrieb”, Berlin Kerntechnik, 2020
- Deeksha Gupta, Yongjian Ding, D. Govindaraj, Mathias Lange, Martin Szemkus, Karl Waedt; Simulation Model for Threat and Impact Analysis on Modern Electrical Power Systems, INFORMATIK2020 GI/IACS Industrie 4.0, Karlsruhe, Germany, 2020-09
- Asmaa Tellabi, Timothée Guiraud, Karl Waedt, “ABAC and RBAC for IACS for Industrie 4.0 Access Control Management”, GI IACS, 2021
- Larissa Moussi, Timothée Guiraud, Edita Bajramovic, Karl Waedt, “Secure Unidirectional Security Gateways for Industrie 4.0”, GI IACS, 2021
- Martin Szemkus, Josef Schindler, Ivo Hempel, Robert Altschaffel, Karl Waedt, “Primary and Supporting Assets for IACS Risk Management”, GI IACS, 2021
- Robert Altschaffel, Martin Szemkus, Karl Waedt, Ivo Hempel, Josef Schindler, Jana Dittmann, “Supporting Security in Industrial Automation and Control Systems by the use of domain-specific modelling”, GI IACS, 2021
- Karl Waedt, Ines Ben Zid, Josef Schindler, “Selected Industry 4.0 Cybersecurity Concepts For Small Modular Reactors And Microreactors”, IAEA IC and CS for SMR, 2022
- Karl Waedt, Ines Ben Zid, Josef Schindler, Egor Dronov, “Cybersecurity Konzepte aus Industrie 4.0 für bestehende Anlagen”, Bremen, KELI, 2022
- Waedt, I. Ben Zid, J. Schindler, E. Kirdan, Cybersecurity Education Programmes & Laboratories Brainstorming, NATO Science for Peace and Secuiry Series D: Information and Communication Security – Vol. 62, p. 100-107, 2022
- Waedt, I. Ben Zid, J. Schindler, “Cybersecurity Risk Management During all NPP Lifecycle Phases”, Leipyig, KTG, 2022
- Edin Kreho, Roger Djeukoua, Timothée Guiraud, Karl Waedt, “Scalable backend representation of security posture of IIoT systems”, Hamburg, GI-IACS, 2022
- Josef Schindler, Siwar Belaidi, Erkin Kirdan, Dr. Karl Waedt, “Securing javascript runtime of OPC UA deployments”, Hamburg, GI-IACS, 2022
- Z. Zhao, K. Waedt, et.al, Sino-German White Paper on Security Tests for Industrie 4.0 and Intelligent Manufacturing, Sino-German Intelligent Manufacturing / Industrie 4.0 Standardisation Sub-Working Group, Deutsche Gesellschaft für Internationale Zusammenarbeit (GZI) on behalf of German Federal Ministry for Economic Affairs and Climate Action (BMWK), Beijing/Berlin, 2022

- Ludger Peters, Mahmould Khalaf, Karl Waedt, Josef Schindler, Siwar Belaidi, “Model based integrity monitoring of Industrial Automation and Control Systems”, Hamburg, GI-IACS, 2022
- Mahmoud Khalaf, Ludger Peters, Karl Waedt, “Modeling Security Controls and System Assets as Autonomous Planning Tasks”, Hamburg, GI-IACS, 2022
- Louis Roger Tchuegoue Djeukoua, Edin Kreho, Siwar Belaidi, Karl Waedt, “Interactive graphical modeling of security artefacts for abstracted Industry 4.0 automation systems”, Hamburg, GI-IACS, 2022
- Karl Waedt, Egor Dronov, Josef Schindler, Fabian Cermak, “IT-Sicherheit in allen Lebenszyklen von Energieanlagen”, Moers IT-Sicherheit für Energieanlagen, 2022
- Erkin Kirdan, Josef Schindler, Karl Waedt, “Securing Machine-to-Machine Communication in the Nuclear Domain with OPC UA”, Vienna IAEA CyberCon23, 2023
- Ludger Peters, Karl Waedt, Siwar Belaidi, “Machine Learning based predictive control to ensure integrity of industrial automation and control systems”, Vienna IAEA CyberCon23, 2023
- Mahmoud Khalaf, Karl Waedt, “Formal Logic Modeling of I&C Systems”, Vienna IAEA CyberCon23, 2023
- Baptiste ODO, Emma BRIEU, Karl WAEDT, “Constraints for Assets and Application Security Controls”, Berlin, GI-IACS, 2023
- Emma BRIEU, Baptiste ODO, Karl WAEDT, “Semi-formal representation of cybersecurity grading for IIoT”, Berlin, GI-IACS, 2023
- Erkin Kirdan, Josef Schindler, Karl Waedt, “Optimizing OPC UA Deployments on Node.js through Advanced Logging Techniques”, Berlin, GI-IACS, 2023
- Romarick Yagatha, Josef Schindler, Siwar Balaidi, Karl Waedt, “Best practices and strategies in securing IIoT networks: Security enhancement of industrial automation and control systems by automated models Case study of smart factories”, Berlin, GI-IACS, 2023
- Natasha Edeh, Robert Altschaffel, Karl Waedt, “Generation of Plausible Synthetic Data for Stego-Malware Detection for Inter-zone IACS Protocols”, Berlin, GI-IACS, 2023
- Ndeye G. Ndiaye, Venesa Watson, Karl Waedt, “Cybersecurity Testing for Industry 4.0”, Berlin, GI-IACS, 2023
- Romarick Yatagha, Karl Waedt, Josef Schindler, Erkin Kirdan, “Security challenges and best practices for resilient IIoT Networks: Network Segmentation”, Berlin, GI-IACS, 2023
- Josef Schindler, Karl Waedt, Erkin Kirdan, “Developments in cybersecurity for critical and renewable energy infrastructure”, Paris, REN, 2023
- Karl Waedt, Josef Schindler, Erkin Kirdan, “Cybersecurity challenges along the OT/IT Supply Chain for Energy Facilities and Critical Infrastructure”, Hamburg, vgbeItSec, 2023
- Erkin Kirdan, Karl Waedt, “Covert Timing Channel Attack on OPC UA-based Industrial Control Systems”, Nürnberg, WIFS, 2023

- Karl WAEDT, Ines BEN ZID, Josef SCHINDLER, Erkin KIRDAN, “Skalierbare detektive Sicherheitsmaßnahmen für physikalische Assets”, Köln, BMUV-GRS, 2023

14. Summary

Note: For an English language version summary, see subsection 14.2.

14.1. Zusammenfassung

Das Forschungsvorhaben „SMARTEST2“ bezieht sich auf Untersuchungen zur Verbesserung der IT-Sicherheit von vernetzten software-basierten leittechnischen Systemen. Über die letzten Jahre zeigt sich der Trend zum Einsatz einer zunehmenden Anzahl von teilweise heterogenen Hardware- und Software-Komponenten sowie einer immer stärker zunehmenden Komplexität der individuell eingesetzten Komponenten und der daraus resultierenden vernetzten Leittechnik-Umgebungen. Eine weitere herausfordernde Entwicklung stellt der generelle Wandel von isolierten IT-Systemen hin zu immer komplexeren Kommunikationsstrukturen und stärker vernetzten IT-Umgebungen dar. Durch die Vernetzung komplexer, heterogener Systeme und Umgebungen vergrößert sich die Angriffsfläche und es ergeben sich neue Möglichkeiten für potentielle Angreifer. Die Untersuchung von Testverfahren zur Erkennung von Schwachstellen in vernetzten software-basierten leittechnischen Systemen stellt daher ein aktuelles und wichtiges Forschungsfeld dar.

Im Vorgänger-Projekt „SMARTEST“ konnten durch eine erfolgreiche Zusammenführung der Kompetenzen von Hochschulen / Universitäten und Industrie bereits wichtige Grundlagen auf dem Gebiet erarbeitet werden. Der Austausch und Informationstransfer zwischen den einzelnen Partnern ermöglichte auf der einen Seite den Aufbau einer Expertise hinsichtlich Automatisierungssysteme und Leittechnik-Umgebungen sowie den Aufbau einer Expertise hinsichtlich IT-Sicherheit für Einzelsysteme und vernetzte Umgebungen auf der anderen Seite. Im Rahmen von „SMARTEST“ und „SMARTEST2“ konnten durch die Partner HS-MD, FRAM und OvGU-AMSL drei unabhängige Testumgebungen umgesetzt werden. Diese Laboraufbauten bzw. Security-Demonstratoren realisieren repräsentative Steuerungsprozesse und ermöglichen durch ihre Vielfältigkeit und Konfigurierbarkeit die Betrachtung angepasster und erweiterter Angriffsrealisierungen, die Umsetzung von praktischem Security Testing und eine unabhängige experimentelle Validierung. Die exemplarische Anwendung der erarbeiteten Verfahren unter Laborbedingungen deutet darauf hin, dass die angestrebte Kombination von Basisangriffen und Knowledge-Levels, ein hierarchisches Attack Testing über verschiedene Layer und damit ein smartes Testen, das effektiv und gezielt durchgeführt werden kann, ermöglicht. Zudem realisierte man erforderliche Tools, z. B. zum Lesen sowie zur Manipulation von Netzwerkpaketen der industriellen Kommunikation in den Laboraufbauten.

Im Forschungsvorhaben „SMARTEST“ wurden zudem neue Forschungsfragen sowie Forschungsbedarf identifiziert. So konnte z. B. der Ansatz des hierarchischen Testens als kombinierte Anwendung von Basis-Angriffen, Knowledge-Levels und Komponentenstruktur bisher nur demonstrativ und exemplarisch umgesetzt werden. Die Realisierung einer automatischen Generierung von vielfältigen Angriffssequenzen konnte bisher nicht erreicht werden. Die Ursache liegt u. a. daran, dass proprietäre

Bestandteile der Software und Protokolle bisher nur unzureichend nachvollzogen werden konnten. Für die angestrebte akkurate Erfassung der Kommunikation und des Systemverhaltens ergab sich daher weiterer Forschungsbedarf u.a. aufgrund von unvollständigen bzw. fehlenden Modellteilen, der Vielzahl unterschiedlicher Hardware-/Softwarekomponenten und Protokolle sowie deren Interaktion in Steuer- und Kontrollprozessen. Dadurch zeigt sich, dass eine quantitative Einschätzung und Beurteilung von möglichen Strukturwirkungen, aufgrund der Vielzahl unterschiedlicher Einflussfaktoren deutlich umfangreicher ist, als ursprünglich angenommen wurde. Dies gilt aus gleichen Gründen auch für Fragen hinsichtlich der Bestimmung und Bewertung des Abdeckungsgrades und möglicher Restrisiken, die bisher nicht zufriedenstellend beantwortet werden konnten.

„SMARTEST2“ umfasste die weitere Erforschung von Ansätzen zur Automatisierung und Generalisierung von Testverfahren zur systematischen Unterstützung bei der Erkennung von IT-Sicherheitsschwachstellen in komplexen, vernetzten leittechnischen Systemen, unter Fortführung, Ausbau sowie Intensivierung der begonnenen Zusammenführung der Kompetenzen von Hochschule, Universitäten und Industrie. Aufbauend auf den 3 verfügbaren unabhängigen Testumgebungen, Laborumgebungen bzw. Security-Demonstratoren erfolgte eine praktische Umsetzung inkl. Bewertung der Testansätze unter Berücksichtigung der Konfigurationsvielfalt.

Mit der Anwendung in den unterschiedlichen Testumgebungen wurde die Wiederverwendbarkeit und Validierbarkeit der erarbeiteten Verfahren sichergestellt. Unter Anwendung der in „SMARTEST“ und „SMARTEST2“ erarbeiteten Ansätze wurde eine einheitliche Modellierung und Generalisierung von Infrastrukturen und Einzelsystemen erreicht. Des Weiteren wurden geeignete Cybersicherheits-Schutzmaßnahmen für Prozessleittechniksysteme identifiziert, unter Einbeziehung verschiedener Kommunikationsprotokolle aktueller Leittechniksysteme.

Folgende wissenschaftliche und technische Arbeitsziele wurden verfolgt:

- Die Aufarbeitung von Security-Schwachstellen unter Berücksichtigung vorliegender Safety Levels. Dies umfasst die Anforderungsdefinition eines einheitlichen, anlagenunabhängigen Modellierungsansatzes, die Modellierung dynamischer Aspekte diverser Kommunikationsstrukturen inklusive des steuerungsprozessabhängigen Verhaltens sowie die Erforschung eines Modellierungsansatzes, der sowohl IT-Security als auch Safety-Aspekte erfasst, um eine Aussage über das mögliche Gefährdungspotenzial treffen zu können.

- Die Evaluation, Bewertung und Erweiterung des Modellierungsansatzes an den drei unterschiedlichen Testumgebungen/Security-Demonstratoren der Partner sowie die Generierung eines einheitlichen Angreifer-/Angriffsmodels und Angriffsszenarien aus den erarbeiten Testdaten. (hauptverantwortlich: HS-MD)

- Hierarchisches intelligentes Testen mittels Basisangriffen durch (hauptverantwortlich: OVGU-AMSL):
  - Anpassung und Verfeinerung exemplarischer Angriffsszenarien und Definition exemplarischer Angriffssequenzen als kombinierte Basis-Angriffe über alle Analysebereiche und Knowledge Levels;
  - demonstrative Umsetzung der Angriffssequenzen auf die verschiedenen Testumgebungen;

- Verfeinerung, Anpassung und Erweiterung der Angriffsszenarien unter Berücksichtigung der erarbeiteten Ergebnisse und Erkenntnisse zur Umsetzung einer automatischen Generierung von Testfällen und Automatisierung von Testsequenzen sowie die Validierung automatisch generierter Angriffssequenzen.

- Entwicklung systematischer, angriffsspezifischer Testverfahren mittels: sukzessiver Identifikation relevanter Schwachstellenklassen (hauptverantwortlich: FAU-SWE):
  - Entwicklung und Einsatz statischer Analyseverfahren zur Eingrenzung des Suchraums und zur Ermittlung der zu verfolgenden Testziele;
  - Entwicklung und Einsatz dynamischer Testverfahren auf der Basis heuristischer Optimierung in Bezug auf die zuvor statisch identifizierten Testziele; - Herleitung eines Leitfadens mittels Zuordnung der untersuchten Schwachstellenklassen und der sich ergebenden Testmuster
  - Tool-basiertes Testing in verschiedenen Bereichen bzw. Ebenen; dies beinhaltet (hauptverantwortlich: FRAM):
    - Security-Tests von KKW-spezifischen Protokollen,
    - Security-Maßnahmen auf Hardware-Basis,
    - Security-Tests auf Quelltext- und Binärebene,
    - Security-Tests von Benutzerschnittstellen,
    - Forensic Readiness Tests,
    - Security-Tests der digitalen Komponenten der elektrischen Systeme,
    - Modellieren sicherheitsrelevanter Artefakte,
    - Security-Tests mittels formaler Spezifikationen,
    - Testen semi-formaler Repräsentationen von Sicherheitsmaßnahmen

- Dokumentation und Publikation der Erkenntnisse sowie Austausch mit Fachexperten (alle Partner)

Die durchgeführten Arbeiten legen die Grundlage für den Kompetenzerhalt auf diesem Gebiet. Das Vorhaben zielt auf die Entwicklung und Weiterentwicklung intelligenter Testverfahren zum Aufzeigen von Schwachstellen in nuklearen Leittechniksystemen.

Ziel ist es, anhand der erzielten Ergebnisse möglichst viele Schwachstellen in nuklearen Leittechniksystemen mittels intelligenter Testverfahren aufzuzeigen. Durch ihre anschließende Behebung kann das Spektrum an IT-basierten, vorsätzlichen Angriffen und der damit verbundene Wirkungsradius reduziert werden. Primär soll dadurch das Risiko kritischer Störfälle, die durch zunehmende aktuelle Bedrohungen durch spezialisierte IT-Angriffe ausgelöst werden können, verringert werden. Damit ordnet sich das Vorhaben auch in die förderpolitischen Ziele des Förderbereichs „Transienten und Unfallabläufe“ des Projektträgers PT-GRS Reaktorsicherheitsforschung ein. Konkrete, anlagenspezifische Informationen bzw. Kenntnisse, die im Rahmen dieses Projekts bekannt werden und zur Gefährdung nuklearer sowie nichtnuklearer Leittechniksysteme missbraucht werden könnten, werden vertraulich behandelt. Für einen Austausch unter Fachexperten werden sensible Informationen ggf. anonymisiert bzw. nach dem Grundprinzip des „Responsible Disclosure“ behandelt.

14.2. Summing-up

Note: For a German language version, see subsection 14.1.

The SMARTEST2 R&D was a great R&D opportunity for technical advancement of cybersecurity for the nuclear domain in Germany and for German companies providing EU and international products and services for nuclear power plants. The R&D scope was an extension of the initial SMARTEST R&D, from 2015 to 2019 with some of the work packages maintained, as requested in the external R&D grant conditions. This includes technically especially the WP4.1 on industrial communication protocols and the work-packages related to semi-formal approaches. New work-packages, e.g. on Electrical Power Systems (EPS) and forensic-readiness were explicitly included into the SMARTEST2 scope.

All project partners tried to increase the Technology Readiness Level (TRL) in line with the intention to cover TRL3 to TRL5. Several publications demonstrated the tool-based approach, a key part for the SMARTEST2-FRA scope. Especially with the OvGU partner, which was also involved in a joint IAEA CRP, hardware in-the-loop approaches could be further extended based on an R&D context that was not yet available for previous R&D projects.

As with the SMARTEST staffing, where a total of 8 PhD candidates was gradually included into the R&D, the SMARTEST2 staffing had to be incremental, partially due to COVID19 related restrictions. At the end of the SMARTEST2 R&D 5 new PhD candidates were involved together with 3 former PhD candidates that have been hired in parallel to the project execution in 2020, 2022 and 2023. The number of involved students increased due to 2 new dual-study sudents and several interns, additionally to the Bachelor and Master thesis students.

The SMARTEST2 R&D together with other, smaller cybersecurity R&D projects with participation of the Framatome GmbH cybersecurity team, especially IAEA CRP 2008, ABAC and DECENT provided a solid context for the application for new R&D projects including their partial funding at German level (project SYNTHESIS) and the EU level (projects SYNAPSE and PANDORA). However, these EU R&D projects are part of other major topics, e.g. cybersecurity and renewable energy or artificial intelligence and thus only partially, technically applicable to the nuclear domain.

Accordingly, a follow-up project, even if not called SMARTEST3, would greatly benefit the further progress along higher TRL levels for cybersecurity in the nuclear domain, including for spent fuel storage facilities and preparation for requirements to be met internationally by German companies. The future R&D may, e.g. address emerging Safety I&C platforms for the nuclear domain, like TXS Compact, new critical infrastructure specific requirements, e.g. on software/firmware updates, communications monitoring and patch management, as these may also impact nuclear facilities. As with SMARTEST2, major results will be published at IAEA conferences, German KTG symposiums, international nuclear conferences, like ICONS, GI workshops, IEEE events and other scientific peer reviewed conferences or journals, jointly with future university, institute and/or industry partners.

15. References

[1] International Electrotechnical Commission, *IEC 61226:2005: Nuclear Power Plants — I&C Systems Important to Safety — Classification of Instrumentation and Control Functions*, 2005.

[2] International Electrotechnical Commission, *IEC 61513:2011, Nuclear Power Plants — I&C Systems Important to Safety — General Requirements for Systems*, 2011.

[3] R. Langner, Robust Control Systems Network: How to achieve reliable control after Stuxnet. Momentum Press, 2012.

[4] AutomationML, *"<AutomationML/>"*, www.unserebroschuere.de/automationml/WebView, 2018

[5] J., Li, B., Zhao and C. Zhang, "*Fuzzing: A Survey*". Cybersecurity 1(1), 2018.

[6] R. Clausing, Y. Gao, M. Parekh, J. Dittmann, K. Waedt and Y. Ding, "*Proposal for a public reference architecture for vulnerability testing in nuclear power plants*" IAEA International Conference on Nuclear Security: Commitments and Actions, Vienna, 2016.

[7] International Organization for Standardization/ International Electrotechnical Commission, *ISO/IEC 27034-2:2015 — Information technology — Security techniques — Application security — Organization normative framework*, 2015.

[8] International Organization for Standardization/ International Electrotechnical Commission*, ISO/IEC TR 27034-5-1:2018 — Information technology — Security techniques — Application security — Protocols and application security control data structure, XML schemas*, 2018.

[9] International Electrotechnical Commission, *IEC 60880:2006, Nuclear Power Plants — I&C Systems Important to Safety — Software Aspects for Computer-based Systems Performing Category A Functions*, 2006.

[10] International Electrotechnical Commission, *IEC TS 62318:2003 Multimedia systems and equipment - Multimedia home server systems - Home server conceptual model*, 2003.

[11] B. Schneier, "*The Process of Security*", https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html, 2000.

[12] International Organization for Standardization/ International Electrotechnical Commission, *ISO/IEC/IEEE 29119-1:2013 Software and systems engineering — Software testing — Concepts and definitions*, 2013.

[13] International Organization for Standardization/ International Electrotechnical Commission, *ISO/IEC TR 24772:2013, Information technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use*, 2013.

[14] International Electrotechnical Commission, *IEC 62645:2014, Nuclear Power Plants — I&C Systems — Requirements for Security Programmes for Computer-based Systems*, 2014.

[15] International Electrotechnical Commission, *IEC 62859:2015, Nuclear Power Plants — I&C Systems — Requirements for Coordinating Safety and Cybersecurity [Draft]*, 2015.

[16] International Organization for Standardization/ International Electrotechnical Commission, *ISO/IEC TR 27019:2013, Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*, 2013.

[17] L. Freitas, "*The Good, The Bad, and The Ugly of TypeScript. Is TypeScript really worth it?*", https://blog.codeminer42.com/the-good-the-bad-and-the-ugly-of-typescript-58a3ff3e248, 2017.

[18] International Atomic Energy Agency, *IAEA NSS No. 33-T:2018, Computer Security of Instrumentation and Control Systems at Nuclear Facilities*, 2018.

[19] Synopsys®, "*Fuzz Testing (Defensics)*", https://www.synopsys.com/software-integrity/resources/datasheets/defensics-fuzz-tests.html, 2017.

[20] Synopsys®, "*State of Fuzzing 2017 - Where the zero days are*", https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/state-of-fuzzing-2017.pdf, 2017.

[21] Synopsys®, "*Synopsys® Defensics® Suite Development Kit Developer Guide For Defensics*", 2017.

[22] Synopsys Editorial Team, "*Debunking the top 5 Defensics fuzz testing myths*", https://www.synopsys.com/blogs/software-security/debunking-defensics-fuzz-testing-myths/, 2018.

[23] B. Rosborough, "*A review of Beyond Security beSTORM® and Codenomicon Defensics®: Which is the smarter fuzzer?*", https://www.beyondsecurity.com/fuzzer_comparison.html, 2018.

[24] PeachTech, "*Peach is a better alternative to Synopsys® Defensics®*", http://www.peach.tech/news/peach-fuzzer-better-alternative-synopsys-defensics/, 2016.

[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021)

[26] IEC 62443-2-4:2023 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providersTC 65

[27] DIN EN IEC 62443-3-3 (VDE 0802-3-3):2020-01 Industrielle Kommunikationsnetze -IT-Sicherheit für Netze und Systeme - Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level (IEC 62443-3-3:2013 + COR1:2014); Deutsche Fassung EN IEC 62443-3-3:2019 + AC:2019

[28] IEC 62541-14:2020 OPC Unified Architecture - Part 14: PubSub TC 65/SC 65E

[29] Information and Computer Security ;Nuclear Security Guidance Committee (NSGC) NSGC/53rd NUSSC Meeting, 15 June 2022PowerPoint Presentation (iaea.org)

[30] https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

[31] Framatome GmbH, "*Framatome TXS*", http://www.framatome.com/EN/customer-564/teleperm-xs-system-overview.html, 2012.

[32] Siemens, "*SIMATIC S7-400 - Process automation with the SIMATIC PCS 7 CPU 410-5H controller*",

https://support.industry.siemens.com/cs/document/96839331/process-automation-with-the-simatic-pcs-7-cpu-410-5h-controller?dti=0&lc=en-US, 2017.

[33] Siemens, "*SIMATIC S7-1500 – The ultimate plus for productivity and efficiency*", https://www.siemens.com/global/en/home/products/automation/systems/industrial/plc/simatic-s7-1500.html, 2018.

[34] Framatome GmbH, "*Framatome TXS - TELEPERM XS user manuals: Qualified Display System (Hardware)*", 2010.

[35] Framatome GmbH, "User Manual: TXS Compact Service-Unit", D02-ARV-01-230-748

[36] Offensive Security, What is Kali Linux ?https://docs.kali.org/introduction/what-is-kali-linux, 2018.

[37] Dragos Inc, "*TRISIS Malware*", https://dragos.com/wp-content/uploads/TRISIS-01.pdf, 2017.

[38] Dragos Inc, "*CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations*," https://dragos.com/wp-content/uploads/CrashOverride-01.pdf, 2017.

[39] E. M. Clarke, J. M. Wing, et al., "*Formal methods: state of the art and future directions*", ACM Comput. Surv., vol. 28, no. 4, pp. 626–643, 1996

[40] M. Fox and D. Long, "*PDDL2.1: An extension to PDDL for expressing temporal planning domains*", J. Artif. Intell. Res., vol. 20, pp. 61–124, 2003.

[41] X. Lou, K. Waedt, Y. Gao et al., "*Combining Artificial Intelligence planning advantages to assist preliminary formal analysis on Industrial Control System cybersecurity vulnerabilities*," Proc. IEEE conference (ECAI 2018), Vol.10, No.1, 2018.

[42] X. Lou, I. BenZid et al., "*Semi-Formal Representation and Evaluation of Security Properties*". In: Eibl, M. & Gaedke, M. (Hrsg.), INFORMATIK, 2017.

[43] K. Waedt, E. Bajramovic, V. Watson and M. Parekh, "*Cybersecurity Penetration and Fuzz Testing, IAEA TM on Engineering and Design Aspects of Computer Security in I&C Systems for NPPs*", Gloucester, UK, 2017.

[44] Mühlbauer, N., Kirdan, E., Pahl, M. O., & Carle, G. (2020, September). Open-source OPC UA security and scalability. In 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) (Vol. 1, pp. 262-269). IEEE.

[45] Mühlbauer, N., Kirdan, E., Pahl, M. O., & Waedt, K. (2021). Feature-based comparison of open source OPC-UA implementations.

[46] Schindler, J., Belaidi, S., Kirdan, E., & Waedt, K. (2022). Securing javascript runtime of OPC UA deployments.

[47] Kirdan, Erkin; Schindler, Josef; Waedt, Karl (2023): Optimizing OPC UA Deployments on Node.js through Advanced Logging Techniques. INFORMATIK 2023 - Designing Futures: Zukünfte gestalten. DOI: 10.18420/inf2023_199. Bonn: Gesellschaft für Informatik e.V.. PISSN: 1617-5468. ISBN: 978-3-88579-731-9. pp. 1995-2001. Wirtschaft, Management Industrie - 8th Industrial Automation and Control Systems Standardization Workshop (IACS 2023). Berlin. 26.-29. September 2023

[48] Kirdan, E., Rezabek, F., Mülbauer, N., Carle, G., & Pahl, M. O. (2023). Real-Time Performance of OPC UA. arXiv preprint arXiv:2310.17052.)

[49] K. Waedt, J. Schindler, I. Ben Zid, E. Dronov, Cybersecurity Konzepte aus Industrie 4.0 für bestehende Anlagen, vgbe energy journal 11, 2022.

[50] BENDER, Melvin, KIRDAN, Erkin, PAHL, Marc-Oliver, et al. Open-source mqtt evaluation. In : 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2021. p. 1-4.

[51] DIMOV, Valentin, KIRDAN, Erkin, et PAHL, Marc-Oliver. Resource tradeoffs for TLS-secured MQTT-based IoT Management. In : NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2022. p. 1-6.

[52] E. Kirdan, P. Horvath and M. -O. Pahl, "Work-in-Progress: Slow Denial of Service Attack on MQTT-Based IoT," 2023 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Istanbul, Turkiye, 2023, pp. 426-431, doi: 10.1109/BlackSeaCom58138.2023.10299779. (July 2023)

[53] SULEYMANOV, Emil, KIRDAN, Erkin, et PAHL, Marc-Oliver. Securing coap with dtls and oscore. In : 2022 6th Cyber Security in Networking Conference (CSNet). IEEE, 2022. p. 1-7.

[54] POP, David, KIRDAN, Erkin, et PAHL, Marc-Oliver. Performance Comparison of UDP and TCP for Different CoAP Load Profiles. In : NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2023. p. 1-6.

[55] Loui Al Sardy, Andreas Neubaum, Francesca Saglietti, Daniel Rudrich, "Comparative Evaluation of Security Fuzzing Approaches", 2019

[56] Andreas Neubaum, Loui Al Sardy, Marc Spislaender, Francesca Saglietti, Yves Biener, "Testing for IT Security: a Guided Search Pattern for Exploitable Vulnerability Classes", 2021

[57] Andreas Neubaum, Loui Al Sardy, Marc Spislaender, Francesca Saglietti, Sara Kretschmer, "A Guided Search for Races Based on Data Flow Patterns", 2022

[58] Kirdan, Erkin; Schindler, Josef; Waedt, Karl (2023): Optimizing OPC UA Deployments on Node.js through Advanced Logging Techniques. INFORMATIK 2023 - Designing Futures: Zukünfte gestalten. DOI: 10.18420/inf2023_199. Bonn: Gesellschaft für Informatik e.V.. PISSN: 1617-5468. ISBN: 978-3-88579-731-9. pp. 1995-2001. Wirtschaft, Management Industrie - 8th Industrial Automation and Control Systems Standardization Workshop (IACS 2023). Berlin. 26.-29. September 2023

[59] D. Beresford, "*Exploiting Siemens Simatic S7 PLCs*", https://media.blackhat.com/bh-us-11/Beresford/BH_US11_Beresford_S7_PLCs_WP.pdf, 2011

[60] D. Beresford, "*Siemens Simatic S7-1200 - CPU START/STOP Module (Metasploit)*", https://www.exploit-db.com/exploits/19833/, 2011.

[61] E. Bajramovic and A. Lainer, "*Forensic-Related Application Security Controls for RHEL in Critical Infrastructure*", GESELSCHAFT INFORMATIK, 2017.

[62] Framatome GmbH, "*Framatome TXS - TELEPERM XS user manual TXS Core SW Release 3.6.5*", 2012.

[63] Basil, Windows Packet Divert, https://github.com/basil00/Divert, 2018.

[64] Asmaa Tellabi, Ines Ben Zid, Edita Bajramovic, Karl Waedt, Safety, "Cybersecurity and Interoperability of Modern Nuclear Power Plants", Athens PESARO, 2018

[65] Felix Freiling, Edita Bajramovic, “Principles of Secure Logging for Safekeeping Digital Evidence”, Hamburg IMF, 2018
[66] Yuan Gao, Xinxin Lou, Venesa Watson, Deeksha Gupta, “Industry 4.0 Standardization on Cybersecurity & Interoperability from the Nuclear Integrator’s Perspective”, Warrington NuclearIndCtrlSec, 2018
[67] Juergen Bochtler, Karl Waedt, Edita Bajramovic, Venesa Watson, “Development of a new IEC Standard on Cybersecurity Controls for I&C in Nuclear Power Plants - IEC 63096”, Vienna IAEA, 2018
[68] Xinxin Lou, Karl Waedt, Yuan Gao, Ines Ben Zid, Venesa Watson, “Combining Artificial Intelligence planning advantages to assist preliminary formal analysis on Industrial Control System cybersecurity vulnerabilities”, Iasi, ROMÂNIA, 2018
[69] Deeksha Gupta, Edita Bajramovic, Mithil Parekh, Karl Waedt, “Cyber Threat Scenarios for Electrical Systems of Nuclear Power Plants”, London ICONE, 2018
[70] Venesa Watson, Edita Bajramovic, Xinxin Lou, Karl Waedt, “Example of graded and lifecycle phase-specific security controls for nuclear i&c and ePs use cases”, London ICONE, 2018
[71] Asmaa Tellabi, Ludger Peters, Christoph Ruland, Karl Waedt, “Security Aspects of Hardware Virtualization Technologies for Industrial Automation and Control Systems”, Berlin GI, 2018
[72] Mithil Parekh, Yuan Gao, Asmaa Tellabi and Karl Waedt, “Secure Interoperability of I&C and IT systems”, Berlin GI, 2018
[73] Venesa Watson, Xinxin Lou, Yuan Gao and Karl Waedt, “Addressing Security gaps in Industries seeking to adopt I4.0”, Berlin GI, 2018
[74] Venesa Watsons and Jochen Sassmannshausen, “Time Sensitive Ethernet Technology for Next Generation CPS/Industry 4.0”, Berlin GI, 2018
[75] Asmaa Tellabi, Karl Christoph Ruland, Ines Ben Zid, Karl Waedt, “Virtualization on Secure Platforms for Industrial Applications”, Shanghai, ICRMS, 2018
[76] Jochen Link, Karl Waedt, Ines Ben Zid, Xinxin Lou, “Current Challenges of the Joint Consideration of Functional Safety & Cyber Security, their Interoperability and Impact on Organizations”, Shanghai, ICRMS, 2018
[77] Venesa Watson, Edita Bajramovic, Mahlet Bejiga, Karl Waedt, “Designing Trustworthy Monitoring Systems”, Shanghai, ICRMS, 2018
[78] Venesa Watson, Jochen Saßmannshausen, “An Evaluation of Time-Sensitive Ethernet Technology for Next Generation CPS”, St Petersburg, ICPS, 2018
[79] Venesa Watson, Jochen Saßmannshausen, “Comparion of AFDX, AVTP, PROFINET and TTE”, St Petersburg, ICPS, 2018
[80] Edita Bajramovic, Venesa Watson, “Insider Threat Modelling and Analysis for Power Plants”, Rome, ISNCC, 2018
[81] Venesa Watson and Jochen Sassmannshausen, “Time-Sensitive Ethernet Technology for Next Generation CPS/Industry 4.0”, Barcelona, CyberICPS
[82] Venesa Watson and Mahlet Bejiga, “Dependability Analysis of the AFDX Frame Management Design”, Sweden, SAFECOMP, 2018
[83] Xinxin Lou, “Cybersecurity analysis of Industrial Control System towards system function view”, Erfurt VDE, FunkionaleSicherheit, 2019

[84] Asmaa Tellabi, Edita Bajramovic, Sebastien Champigny, Mathias Lange, Karl Waedt, Yongjian Ding, “International Standards as Precondition for Prevention of Cyber Attacks on Nuclear Power Plant”, Berlin, KTG, 2019

[85] J. Schindler, V. Watson, K. Waedt: Interoperability of fast charging station with battery booster, IACS, GI2019, Kassel, 2019

[86] Ines Ben Zid, Deeksha Gupta, Xinxin Lou, Dr. Karl Waedt, “A Functional Specification Based Approach For Analyzing The Cyber Security Of End User Interfaces Within NPP”, Tsukuba ICONE, 2019

[87] Asmaa Tellabi, “Security aspects of FPGA and virtualization case studies”, Kassel, GI, 2019

[88] Edita Bajramovic, Deeksha Gupta, Yun Guo, Karl Waedt, Anis Bajramovic “Security Challenges and Best Practices for IIoT”, Kassel, GI, 2019

[89] Ines Ben Zid, Xinxin Lou, Mithil Parekh, Karl Waedt, “The application of Artificial Intelligence for Cyber Security in Industry 4.0”, Kassel, GI, 2019

[90] Josef, Xinxin Lou, Venesa Watson, Karl Waedt, “Interoperability of lithium ion battery packsfor fast charging station booster”, Kassel, GI, 2019

[91] Venesa Watson, Jochen Sassmannshausen and Karl Waedt, “Secure Granular Interoperability with OPC UA”, Kassel, GI, 2019

[92] Xinxin Lou, Yun Guo, Yuan Gao, Karl Waedt, Mithil Parekh, “An idea of using Digital Twin to perform the functional safety and cybersecurity analysis”, Kassel, GI, 2019

[93] D. Gupta, D. Govindaraj, R. Altschaffel, K. Waedt, “Blue Team Support For Eps Related Cybersecurity Readiness”, Vienna IAEA ICONS, 2020

[94] X. Lou, P. Ladkin, K. Waedt, I. Ben Zid: Applying reverse engineering to perform integrated safety and cybersecurity analyses of system functionality, Proceedings of the 28th Safety-Critical Systems Symposium, York, UK, 2020

[95] A. Tellabi; X. Lou; K. Waedt: A Prototype of a new Virtualized Secure Embedded Product for Operational and Safety Related I&C Functions, International Conference on Nuclear Security (ICONS 2020), Vienna, 2020

[96] Y. Gao, X. Lou; Operational Security Analysis and Challenge for IoT Solutions, INFORMATIK2020 GI/IACS Industrie 4.0, Karlsruhe, Germany, 2020

[97] M. Parekh, K. Waedt, A. Tellabi: Aligning with cybersecurity framework by modelling OT security, INFORMATIK2020 GI/IACS Industrie 4.0, Karlsruhe, Germany, 2020

[98] V. Watson, Ch. Ruland, K. Waedt; MAC-layer Security for Time-Sensitive Switched Ethernet Networks, INFORMATIK2020 GI/IACS Industrie 4.0, Karlsruhe, Germany, 2020

[99] I. Ben Zid, X. Lou, K. Waedt “Consideration of Artificial Intelligence for Cybersecurity Aspects Of I&C Systems”, Vienna IAEA ICONS, 2020

[100] Yun Guo, Xinxin Lou, Edita Bajramovic, Karl Waedt, “Cyber Security Risk Analysis And Technical Defense Architecture Research Of Ics In Nuclear Power Plant Construction Stage”, Vienna IAEA ICONS, 2020

[101] J. Schindler, A. Tellabi, K. Waedt; Gossip protocol approach for a decentralized energy market with OPC UA client-server communication, INFORMATIK2020 GI/IACS Industrie 4.0, Karlsruhe, Germany, 2020-09

[102] D. Gupta, Ch. Bürger, I. Ben Zid, K. Waedt, “BSI Grundschutz - neue Anforderungen für mobile Servicegeräte für Rückbau und Normalbetrieb”, Berlin Kerntechnik, 2020
[103] D. Gupta, Y. Ding, D. Govindaraj, M. Lange, M. Szemkus, K. Waedt; Simulation Model for Threat and Impact Analysis on Modern Electrical Power Systems, INFORMATIK2020 GI/IACS Industrie 4.0, Karlsruhe, Germany, 2020-09
[104] Asmaa Tellabi, Timothée Guiraud, Karl Waedt, “ABAC and RBAC for IACS for Industrie 4.0 Access Control Management”, GI IACS, 2021
[105] Larissa Moussi, Timothée Guiraud, Edita Bajramovic, Karl Waedt, “Secure Unidirectional Security Gateways for Industrie 4.0”, GI IACS, 2021
[106] Martin Szemkus, Josef Schindler, Ivo Hempel, Robert Altschaffel, Karl Waedt, “Primary and Supporting Assets for IACS Risk Management”, GI IACS, 2021
[107] Robert Altschaffel, Martin Szemkus, Karl Waedt, Ivo Hempel, Josef Schindler, Jana Dittmann, “Supporting Security in Industrial Automation and Control Systems by the use of domain-specific modelling”, GI IACS, 2021
[108] Dr. Karl Waedt, Mrs. Ines Ben Zid, Mr. Josef Schindler, “Selected Industry 4.0 Cybersecurity Concepts For Small Modular Reactors And Microreactors”, IAEA IC and CS for SMR, 2022
[109] Dr. Karl Waedt, Mrs. Ines Ben Zid, Mr. Josef Schindler, Egor Dronov, “Cybersecurity Konzepte aus Industrie 4.0 für bestehende Anlagen”, Bremen, KELI, 2022
[110] K. Waedt, I. Ben Zid, J. Schindler, E. Kirdan, Cybersecurity Education Programmes & Laboratories Brainstorming, NATO Science for Peace and Secuiry Series D: Information and Communication Security – Vol. 62, p. 100-107, 2022
[111] K. Waedt, I. Ben Zid, J. Schindler, “Cybersecurity Risk Management During all NPP Lifecycle Phases”, Leipyig, KTG, 2022
[112] Edin Kreho, Roger Djeukoua, Timothée Guiraud, Karl Waedt, “Scalable backend representation of security posture of IIoT systems”, Hamburg, GI-IACS, 2022
[113] Josef Schindler, Siwar Belaidi, Erkin Kirdan, Dr. Karl Waedt, “Securing javascript runtime of OPC UA deployments”, Hamburg, GI-IACS, 2022
[114] Z. Zhao, K. Waedt, et.al, Sino-German White Paper on Security Tests for Industrie 4.0 and Intelligent Manufacturing, Sino-German Intelligent Manufacturing / Industrie 4.0 Standardisation Sub-Working Group, Deutsche Gesellschaft für Internationale Zusammenarbeit (GZI) on behalf of German Federal Ministry for Economic Affairs and Climate Action (BMWK), Beijing/Berlin, 2022
[115] Ludger Peters, Mahmould Khalaf, Karl Waedt, Josef Schindler, Siwar Belaidi, “Model based integrity monitoring of Industrial Automation and Control Systems”, Hamburg, GI-IACS, 2022
[116] Mahmoud Khalaf, Ludger Peters, Karl Waedt, “Modeling Security Controls and System Assets as Autonomous Planning Tasks”, Hamburg, GI-IACS, 2022
[117] Louis Roger Tchuegoue Djeukoua, Edin Kreho, Siwar Belaidi, Karl Waedt, “Interactive graphical modeling of security artefacts for abstracted Industry 4.0 automation systems”, Hamburg, GI-IACS, 2022

[118] Dr. Karl Waedt, Egor Dronov, Josef Schindler, Fabian Cermak, “IT-Sicherheit in allen Lebenszyklen von Energieanlagen”, Moers IT-Sicherheit für Energieanlagen, 2022
[119] Erkin Kirdan, Josef Schindler, Karl Waedt, “Securing Machine-to-Machine Communication in the Nuclear Domain with OPC UA”, Vienna IAEA CyberCon23, 2023
[120] Ludger Peters, Karl Waedt, Siwar Belaidi, “Machine Learning based predictive control to ensure integrity of industrial automation and control systems”, Vienna IAEA CyberCon23, 2023
[121] Mahmoud Khalaf, Karl Waedt, “Formal Logic Modeling of I&C Systems”, Vienna IAEA CyberCon23, 2023
[122] Baptiste ODO, Emma BRIEU, Karl WAEDT, “Constraints for Assets and Application Security Controls”, Berlin, GI-IACS, 2023
[123] Emma BRIEU, Baptiste ODO, Karl WAEDT, “Semi-formal representation of cybersecurity grading for IIoT”, Berlin, GI-IACS, 2023
[124] Erkin Kirdan, Josef Schindler, Karl Waedt, “Optimizing OPC UA Deployments on Node.js through Advanced Logging Techniques”, Berlin, GI-IACS, 2023
[125] Romarick Yagatha, Josef Schindler, Siwar Balaidi, Karl Waedt, “Best practices and strategies in securing IIoT networks: Security enhancement of industrial automation and control systems by automated models Case study of smart factories”, Berlin, GI-IACS, 2023
[126] Natasha Edeh, Robert Altschaffel, Karl Waedt, “Generation of Plausible Synthetic Data for Stego-Malware Detection for Inter-zone IACS Protocols”, Berlin, GI-IACS, 2023
[127] Ndeye G. Ndiaye, Venesa Watson, Karl Waedt, “Cybersecurity Testing for Industry 4.0”, Berlin, GI-IACS, 2023
[128] Romarick Yatagha, Karl Waedt, Josef Schindler, Erkin Kirdan, “Security challenges and best practices for resilient IIoT Networks: Network Segmentation”, Berlin, GI-IACS, 2023
[129] Josef Schindler, Karl Waedt, Erkin Kirdan, “Developments in cybersecurity for critical and renewable energy infrastructure”, Paris, REN, 2023
[130] Dr. Karl Waedt, Josef Schindler, Erkin Kirdan, “Cybersecurity challenges along the OT/IT Supply Chain for Energy Facilities and Critical Infrastructure”, Hamburg, vgbeItSec, 2023
[131] Erkin Kirdan, Dr. Karl Waedt, “Covert Timing Channel Attack on OPC UA-based Industrial Control Systems”, Nürnberg, WIFS, 2023
[132] Dr. Karl WAEDT, Fr. Ines BEN ZID, Hr. Josef SCHINDLER, Hr. Erkin KIRDAN, “Skalierbare detektive Sicherheitsmaßnahmen für physikalische Assets”, Köln, BMUV-GRS, 2023

16. Abbreviations

2D	Two-Dimensional
3D	Three-Dimensional
AC	Automation Computer
ACK	Acknowledge
AI	Artificial Intelligence
ANSI	American National Standards Institute
API	Application Programming Interface
APT	Advanced Persistent Threat
ASC	Application Security Controls
ASME	American Society of Mechanical Engineers
AutomationML	Automation Markup Language
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DIN	German Institute for Standardization
DoS	Denial-of-Service
EPR	Evolutionary Pressurised Reactor
EPS	Electrical Power Systems
ESFAS	engineered safety features actuation system
FA3	Flamanville 3
FSM	Finite State Machine
FPGA	field programmable gate array
GW	Gateway
HMI	Human Maschine Interface
HPC	Hinkley Point C
HTTP	Hypertext Transfer Protocol
HW	Hardware

I&C	Instrumentation and Control
IACS	Industrial Automation and Control Systems
IAEA	International Atomic Energy Agency
ICONE	International Conference on Nuclear Engineering
ICT	Information and Communication Technologies
ICT	Information and Communication Technologies
ID	Identification number
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
JSON	JavaScript Object Notation
LAN	Local Area Network
LLC	Logical Link Control
MSI	Monitoring and Service Interface
NIC	Network Interface Card
NPP	Nuclear Power Plant
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
OPC UA	Open Platform Communications Unified Architecture
PC	Personal Computer
PLC	Programmable Logic Controller
QDS	Qualified Display System
R&D	Research & Development
RHEL	Red Hat Enterprise Linux
RHEL	Red Hat Enterprise Linux
SCADA	Supervisory Control and Data Acquisition

SDK	Software Development Kit
SIEM	Security Information and Event Management
SU	Service Unit
SUT	System Under Test
TCP/IP	Transmission Control Protocol/Internet Protocol
TIA	Totally Integrated Automation
TR	Technical Report
TRL	Technology Readiness Level
UML	Unified Modeling Language
WP	Work Package
XML	Extensible Markup Language