Results of the IAEA Coordinated Research Project Enhancing Computer Security for Radiation Detection Systems

Rodney Busquim e Silva[a*], Michael T. Rowland[b], Ricardo Paulino Marques[c], Isabelle Coelho Franco[c], Jianghai Li[d], Tamas Holzer[e], Khalil El-Khatib[f], Nelson Agbemava[g], I Puta Susila[h], Jacek Gajewski[i], David Allison[j], Imbaby Mahmoud [K]

[a]International Atomic Energy Agency, Vienna, Austria
[b]Sandia National Laboratories, Albuquerque, United States of America
[c]University of Sao Paulo, Sao Paulo, Brazil
[d]Tsinghua University, Beijing, China
[e]Budapest University of Technology and Economics, Budapest, Hungary
[f]Ontario Tech University, Oshawa, Canada
[g]Nuclear Regulatory Authority, Accra, Ghana
[h]National Research and Innovation Agency, Jakarta, Indonesia
[i]National Centre for Nuclear Research, Otwock, Poland
[j]AIT Austrian Institute of Technology GmbH, Austria
[K]Egyptian Atomic Energy Authority

Abstract: This work presents the results of the International Atomic Energy Agency's (IAEA) Coordinated Research Project (CRP) on Enhancing Computer Security for Radiation Detection Systems. These systems include a wide range of fixed and mobile radiation detectors used in safety and security applications such as environmental monitoring, border control, nuclear power generation, nuclear research reactor operations, medical applications, and nuclear fuel cycle activities, among others. The signals and data generated by radiation detection systems are transmitted to local or remote monitoring centers through various communication channels, enhancing the effectiveness of threats detection enabling a timely response to alarm conditions. However, during the generation, processing, transmission and display of this information, data can be compromised. This highlights the need for robust computer security measures to protect the confidentiality, integrity, and availability of the information processed, transmitted, stored and displayed. This IAEA CRP aims to develop innovative methodologies and techniques to enhance the computer security of radiation detection equipment, physical protection systems, associated computer-based systems, data communication protocols and the supporting network infrastructure. The project also covers physical protection systems that secure other radioactive materials from theft or sabotage. This CRP brought together 11 organizations from 10 Member States to explore various topics, including threat modeling, cloud computing, malware propagation in large radiation detection networks, defensive computer security architecture, wireless communication security, and simulation of integrated physical protection and radiation detection systems. The participating institutes developed a reference model for synthetic radiation data and anomaly detection techniques, conducted vulnerability assessments of radiation detection systems, and built prototypes of virtual and hardware-in-the loop testbeds. The CRP research also resulted in the development of simulators, including a physical protection-radiation detector simulator featuring a 3D model of a hospital. The collective efforts of the research institutes involved in this CRP are expected to significantly enhance the computer security of radiation detection systems, reinforcing the confidentiality, integrity, and availability of the radiation detection information generated, transmitted, processed, stored and displayed.

Keywords: Cybersecurity, Radiation Detection Systems, Simulation, Capacity Building

1. INTRODUCTION

Operations of nuclear and other radioactive material facilities, along with systems and measures for detecting and responding to nuclear and other radioactive material out of regulatory control, rely on the timely detection of radiation hazards. The signals generated by Radiation Detection Systems (RDS) provide information that is transmitted and monitored in alarm monitoring centers, such as central alarm stations and national analysis centers. These alarms are transmitted through various communication channels, both local and remote (e.g., over the Internet). Since the generation and transmission of both radiation data and alarm data to monitoring

centers are vulnerable to compromise and manipulation, it is essential to implement robust computer security measures to ensure the confidentiality, integrity, and availability of the transmitted, assessed, and stored data.

The objective of the IAEA CRP J02017 *Enhancing Computer Security for Radiation Detection Systems*, is to improve the computer security of RDS. The project's research focuses on ensuring the secure operation of RDS in nuclear security and safety applications, including during Major Public Events (MPE) [1] and in the detection and response to nuclear materials and other radioactive materials outside of regulatory control [2]. The project is developing innovative methodologies and techniques to enhance the computer security of RDS, associated computer-based systems, communication protocols, and network infrastructure.

The researchers involved in this project possess diverse expertise across multiple disciplines and collaborate to enhance computer security for RDS used in nuclear power plants (NPPs), nuclear fuel cycle operations, research reactors, as well as other facilities dealing with radioactive materials (such as medical applications), nuclear material transportation, environmental monitoring, border security, and MPEs. This multidisciplinary team, drawn from various research institutes in ten IAEA Member States, is working in a coordinated manner on several key aspects:

- Defining strategies for connecting radiation detectors sensors.
- Exploring cyber-security of wireless detector networks.
- Developing models for propagation of malwares in distributed radiation detector networks.
- Identifying anomalies during radiation detection system's operation.
- Developing virtual testbeds simulating the radiation detection architecture.
- Exploring the application of data encryption in radiation detection networks.
- Studying the cybersecurity resilience in radiation detection data transmitted or stored in the cloud.

After 2 years of the project, the researchers from participating institutes have made significant progress through their collaborative efforts across several initiatives.

2. PARTICIPATING INSTITUTES

This project brings together 11 participating institutes from 10 IAEA Member States, all of which are actively contributing to this initiative. These CRP participating institutes are:

- Austrian Institute of Technology GmbH (AIT, Austria), with the project "Threat Analysis and Anomaly Detection for Next Generation Radiation Monitoring System Computer Security".
- Budapest University of Technology and Economics (BME, Hungary), with the project "Virtualized Networks and Automatic Scenario Generation for Enhancing Computer Security of RDSs".
- Egyptian Atomic Energy Authority (EAEA, Egypt), with the project "Interference Management and Advanced Encryption Techniques Application in Radiation Detection Systems".
- Georgia Tech (GTU, USA), with the project "Development of Cyber-Attack Detection Systems for Radiation Detection Systems".
- National Centre for Nuclear Research (NCBJ, Poland), with the project "Testing the Cybersecurity of Wireless Communication Between Remote Radiation Detection Systems and Dosimetry Centre".
- National Research and Innovation Agency (INS, Indonesia), with the project: "Security Consideration in the Design and Implementation of LoRaWAN-based Radiation Monitoring System".
- Nuclear Regulatory Authority (NRA, Ghana), with the project "Improving Computer Security of Radiation Detection System".
- Ontario Tech University (OTU, Canada) with the project "Building Resiliency in Sensor Cloud for Radiation Detection System (RDS)".
- Tsinghua University (THU, China), with the project "Cyber-Physical Approach to Enhance Computer Security of Radiation Detection Systems"
- Sandia National Laboratories (SNL, USA), in cooperation with Livermore Lawrence Livermore National Laboratory (LLNL – USA)
- with the project "Analysis of Defensive Cyber Security Architecture (DCSA) Effectiveness Analysis for the Physical Protection of Radiological Material".

- University of São Paulo (USP, Brazil), with the project “Cyber Security Assessment of Radiation Detection, Associated Systems and Networks”.

3. CURRENT STATUS

After the first year of the project, a Research Coordinated Meeting (RCM) was conducted at LLNL in November 2023 to discuss and assess the relevance of research plans to the overall objectives of the CRP. An IAEA CRP research activity involves agreeing upon and implementing common research elements by one or more participant institutes. To serve as basis for collaborative work, a general reference architecture for RDS, presented in Figure 1, was developed during the first RCM and it subsequently refined throughout the project. This reference model facilitates the integration of all techniques and methodologies under development.

A consultancy meeting was held at the University of São Paulo in Brazil in June 2024, followed by another meeting at the Nuclear Security Training and Demonstration Centre (NSTDC) [3] in October 2024. The second RCM was conducted in November 2024. In addition, the CRP research team held several online meetings to advance the and updated the ongoing work. The following summary outlines the status of the current research areas and results by the participating institutes, and provides a concise overview of the key contributions of each institute. Although almost all the projects involved multiple institutes, only the leading institute for each work is listed.

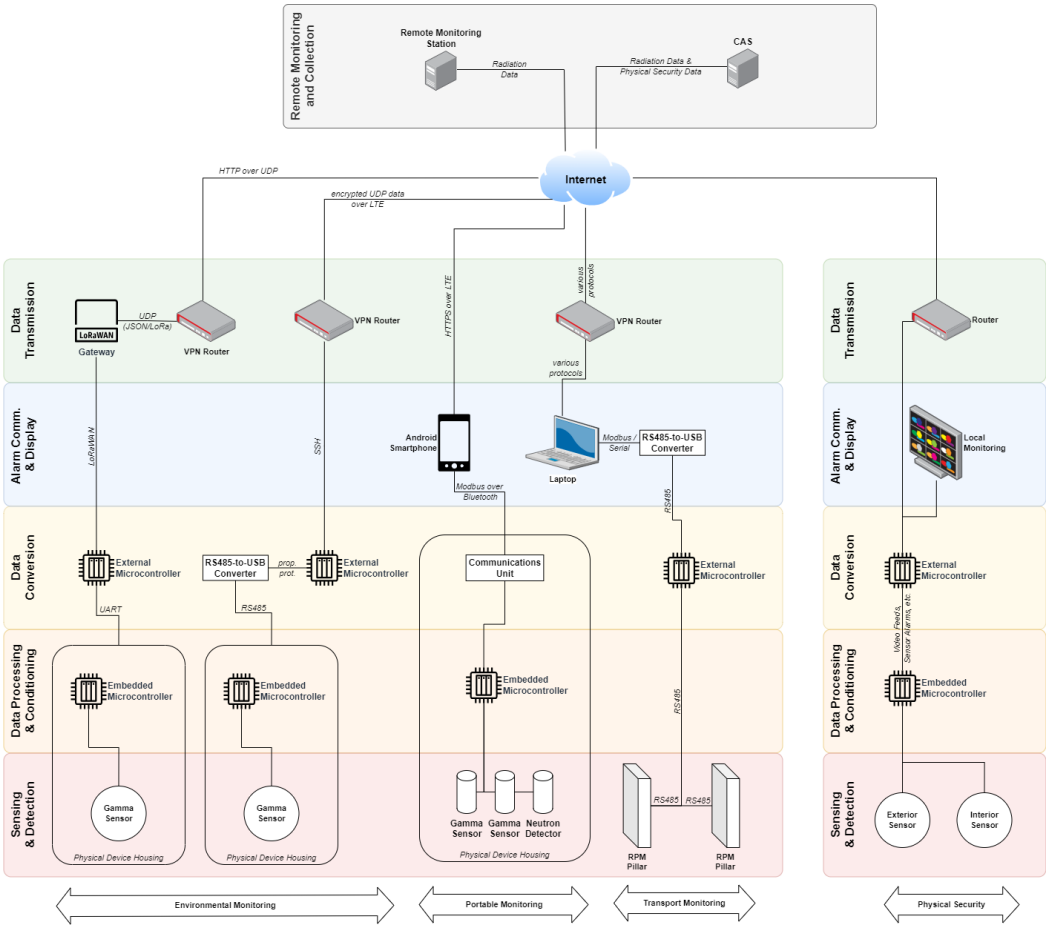

Figure 1. CRP General Reference Architecture

3.1 Austrian Institute of Technology (AIT)

AIT research activities leveraged automated threat analysis using *ThreatGet* [4] to conduct a comprehensive analysis of both real-world and reference RDS architectures. The analysis was used leveraged to develop use-cases and adversary scenarios against RDS. AIT is also conducting an analysis of the attack surface and vulnerabilities of RDSs from open-source information, as well as identifying common concepts and technological components often found in RDSs.

Preliminary analysis of several real-world RDS architectures, including environmental radiation monitoring systems used by NCBJ (Poland) and BRIN (Indonesia), handheld and backpack-based radiation detection devices, and static radiation portal monitors has been carried out. In addition, more detailed modelling of NCBJ's environmental radiation monitoring system has been carried out in *ThreatGet*, with automated threat analysis results generated. Input from all project partners, led by AIT, has seen the creation of a reference architecture that can be used to contextualize results from the project, as well as allow practitioners to better understand the organization of their digital RDS. Analysis of this reference architecture will be used to provide risk probabilities for USP's (Brazil) virus propagation model, based on a MPE use case, details of which are provided by NRA (Ghana) as can be seen in Figure 2.

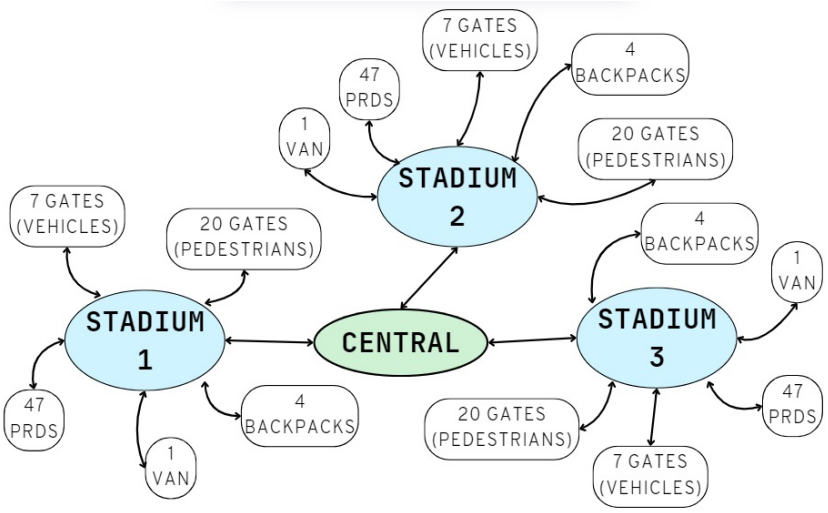

Figure 2. Major Public Event Use Case

3.2 Budapest University of Technology and Economics (BME)

BME has selected a national early warning system for their test scenario, featuring two distinct RDSs. BME analyzed the systems and implemented a virtual topology using the infrastructure as a code approach, for rapid, reproducible, and easy deployment. Additionally, BME developed synthetic data generation methods for RDSs research, using a system based on generative neural networks, to be used in the simulated early warning system. A comprehensive model was developed to handle various devices, services, operations, and connections, serving as the foundation for the test scenario. The proposed method was published in a conference paper [5].

Meanwhile, BME also started to analyze the cybersecurity of different handheld and backpack-based radiation detection devices used at NSTDC. BME has identified potential weaknesses that can be exploited in some special circumstances, compromising the data the operator receives from the RDSs. These weaknesses include configuration problems, unencrypted communication over wireless channels, and the usage of malicious hardware implants, which can be demonstrated in the general reference architecture presented earlier.

3.3 Egyptian Atomic Energy Authority (EAEA)

Wireless Sensor Networks (WSNs) play an important part in distributed RDS. The EAEA developed a method for interference temperature calculation using Channel Availability Metric (CAM) concept. The method uses calculated interference temperature of a channel in a cost function of a routing protocol to account for interference/jamming and use of channel switching to avoid channel with higher interference/jamming. The use of error correcting code to mitigate jamming effect is also investigated.

The EAEA research team has also developed a method for malicious node identification in radiation detection WSNs [6]. This method is based on a two-step identification solution, one step for correlation of sensor readings and the second step performing reputation analysis from network traffic. Enhanced method is proposed to include Particle Filter approach in the first step. The team developed as well as an Authenticated

Encryption Standard (AES) co-processor and implemented its blocks in FPGA. Additionally, the team generated radiation detection data both count per minute (CPM) data for Gamma source intensity values and waveform shape for spectroscopy and pulse shape discrimination based on semi empirical method guided by physics principles.

3.4 Georgia Institute of Technology (GTU)

GTU has developed an RDS testbed with hardware in the loop capabilities. RDS attack pathways and vulnerabilities were analyzed to determine potential successful exploitation of various communication channels. Fault and cyber-attack detection models have also been developed when RDS has been compromised or suspected of compromise due to unexpected behaviors. Moreover, several Artificial Intelligence/Machine Learning (AI/ML) classifiers for the cyber-attacks have also been developed. The team is currently focusing on identifying scenarios of cyber-attacks on RDS. This involves generating spectra using GEANT4, manipulating these spectra, parsing raw spectroscopic data (N42), and reverse engineering spectroscopic data as a proof of concept. To support these activities, the team developed several Python [7] tools for peak fitting and finding regions of interest. These tools facilitate easy implementation of attacks and allow researchers to quickly and visually assess the impact of spoofed data, helping to determine the potential success of an attack.

3.5 Nuclear Regulatory Authority (NRA)

NRA of Ghana worked on the development of threat analysis for cloud service computing and on using simulation for nuclear security measures in MPEs for training. With respect to the threat analysis for cloud computing service: the work focused on developing a threat analysis report to examine the impact of malware infection at different stages of cloud data handling: data acquisition, data processing, and data distribution and storage. For each stage, potential attack vectors and scenarios were explored to understand how malware infection can disrupt cloud-based operations. To mitigate these risks, the threat report recommends organizations implement multi-layered security strategies, including strong authentication, encryption, real-time monitoring and intrusion detection, and strict access controls at each phase of data handling in the cloud.

As for using simulation for nuclear security measures in MPEs, and based on the fact that training and exercise are key components in any threat management, especially when dealing with large crowds at MPE, the NRA team collaborated with OTU to develop a simulation that allows for training network operators at managing RDS used for MPE. The simulation, while in early development stage, should offer more than just a glimpse of this real-world vigilance—it replicates it. By modeling dynamic detection zones and crowd behaviors, it allows operators to foresee what might happen during such a large event. Using this simulation tool, operators can test various responses, fine-tune their strategies, and prepare for the unthinkable, ensuring that, when the real crowds gather, they are ready to mitigate any threat that arises.

3.6 National Centre for Nuclear Research – Poland (NCBJ)

NCBJ is building a prototype of the RDS around its research reactor MARIA. It is designed as a virtual private network (VPN), compatible with the requirements of Polish regulator and the country-wide Radiation Emergency Centre (CEZAR). Current design is a dual system consisting of wired and wireless networks, providing for communications redundancy increasing the system resilience to possible attacks. Two wireless technologies (GSM and Long Range Wide Area Network - LoRaWAN) are currently being implemented, whose performance will be compared in a series of field tests, which will include testing of their cybersecurity. Future tests are designed and will be done in the modified cybersecurity test bed “CyberLAB” created as a part of IAEA CRP Enhancing Computer Security Incident Analysis at Nuclear Facilities. Search will be for possible situations in which either the used devices or the data transmission has been compromised or suspected of compromise. ML classifiers for the cyber-attacks have also been developed.

3.7 National Research and Innovation Agency – Indonesia (BRIN)

The research undertaken by INS comprehends activities on LoRaWAN. A prototype of LoRaWAN-capable RDS to measure dose rate utilizing PIN-Photodiode detector based on Arduino platform [8], and communication module for integrating commercial RDS has been developed. INS has proposed an architecture of private LoRaWAN-based radiation monitoring system (RMS) both for indoor and outdoor measurement

[9]. The architecture aims to mitigate or reduce security threats for LoRaWAN-based RMS. Evaluation of the architecture effectiveness will leverage actual measurements of radiation dose rate, Signal-to-Noise Ratio (SNR), Received Signal Strength Indicator (RSSI) and communication coverage which were collected using developed nodes. Preliminary analysis of possible attack surfaces and vulnerabilities based on the proposed architecture was conducted using *ThreatGet* in collaboration with AIT. In addition, radionuclide spectrum data for Co-60, Cs-137, Cs-134 and Eu-152 were collected and can be used to develop data communication format, synthetic data generation algorithm, and algorithm to detect radiation and cyber events.

3.8 Ontario Tech University (Canada)

RDS are crucial for ensuring public safety during major events, so it is vital to maintain their integrity, availability, and the accuracy of the radiation data they produce. A major collaboration between OTU and the NRA has focused on the development a solution to help securying the proper operation of these systems. A researcher from the İstanbul University-Cerrahpaşa, Turke, has also joined the team. The collaboration has focused on securing against cyber threats to RDS, such as tampering or data manipulation, the implementation of a AI/ML-based Intrusion Detection System (IDS). The goal was to create an IDS capable of differentiating between authentic radiation data and altered data. The team focused on simulating a Denial of Service (DoS) attack to demonstrate how false data could be identified in RDS environments. To address the typical problem of class imbalance in training data sets, the team used a combination of *K-Means* clustering and SMOTE for oversampling. These investigations included optimizing and assessing the performance of several AI/ML models, including Random Forest, Support Vector Machine (SVM), logistic regression, and Light Gradient-Boosting Machine (LightGBM), to detect DoS attacks on RDSs. Several optimization models and TinyML techniques such as feature selection, parallel execution, and random search methods we are applied to improve the efficiency of the proposed IDS. Several experiments and tests using Safecast [10] data showed that the optimized LightGBM-based IDS can provide a high degree of accuracy in detection intrusions in RDS systems and can potentially be implemented on devices with limited computational power [11].

3.9 Sandia National Laboratories (SNL) and Lawrence Livermore National Laboratory (LLNL)

SNL/LLNL research efforts are focused on the cybersecurity and functional interdependency between physical protection systems (PPS) and RDS. The Gula Regional Hospital (GRH) has been modelled to investigate and evaluate candidate DCSAs, specifically focused on radiation detection sensors, logic controllers, intrusion detection sensors, biometrics, and video cameras. Radiation detection sensors virtualized and modelled by BME and baselined against GTU and NCBJ data will be incorporated into the GRH Model.

Several components of the GRH Model have been developed and integrated. Biometrics, intrusion detectors and other PPS sensors and associated logic have been implemented in MATLAB/Simulink [12] and containerized. These are integrated into the GRH 3D Unity model using a custom developed synchronizer program, which leverages the Data Broker to inject and extract information from shared memory of the Simulink models. This information is used to generate command packets for other simulator components based on Simulink results. The network emulation layer is provided by Sandia's MiniMega virtualization environment, allowing for configuration of virtual machines (VMs) that represent the digital assets whose physical representation is present in the GRH 3D model and computations are handled by Simulink. MiniMega's built-in command and control, MiniCC, is leveraged to control VMs representing the various digital assets. Finally, information is exchanged again with the Unity Engine via the synchronizer to enable state changes within the Model (e.g., Door Unlock).

The architecture, shown in the Figure 3, has been proof-of-concept tested and demonstrated to be sufficient for expected future research activities. One consideration going forward is whether computing resources will be sufficient to run the environment in near or at real-time. A possible configuration option being considered is whether to allow for simulation time to be configurable to align performance with the available computing resources. By lowering computing resource requirements for the simulation, the complexity of the GRH can be increased, while allowing other CRP organizations with limited computing resources to leverage the simulator for their coordinated efforts.

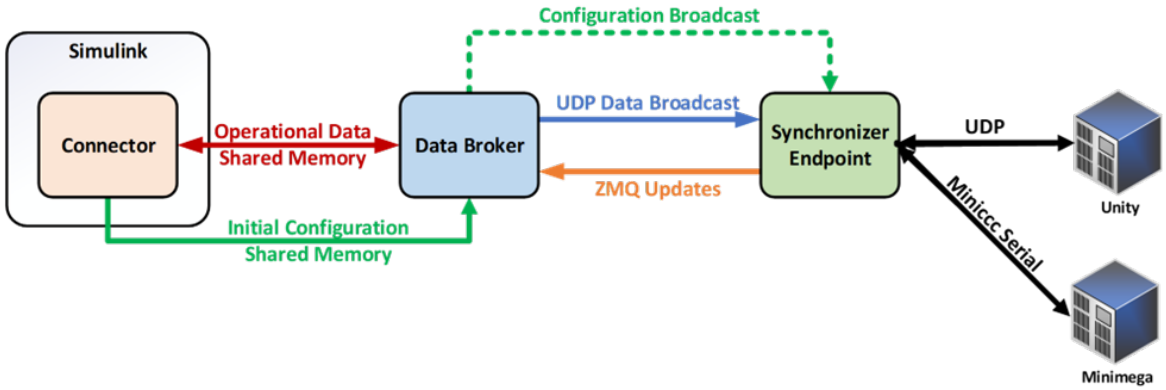

Figure 3. Gula Architecture Model

3.10 Tsinghua University (THU)

The work of THU's team focused on applying cyber-physical defense approach to secure RDS. This is because the cyber threat to RDSs would not only disrupt the computer-based systems, but also affect the functions of the RDSs and ultimately compromise nuclear safety and security. THU's results are divided into four parts:

- A characterization of the impact of threats on the functions of RDSs: The impact on RDS functions follows the D5 framework of Deny (deny of RDS functions), Degrade (degradation of RDS performance, such as accuracy, response time), Disrupt (manipulation of radiation data), Deceive (deceiving the operator by false alarms and missing alarms), and Destroy (damaging the RDS).
- A risk-based concept of "cyber-physical risk" for OT system assessment: The cyber-physical risk concept is for the assessment of the unaddressed intersection of cyber and physical security, such as cyber threats causing physical damage and the cyber compromise via physical approaches.
- A novel cyber anomaly detection technique based on raw signal monitoring of the RDS: The cyber anomaly detection based on raw signal monitoring focuses on the lower part of the RDS before the measurements are packed into network packets. The raw signal and measurements are as a new source to detect the anomalies in the network traffic. The technique is implemented using signal splitting [13].
- A hardware-in-the-loop (HiL) platform for the RDS to simulate the commonly used signal and fieldbus The HiL platform is built to simulate several commonly used signals and fieldbuses of RDS, such as analogue I/O (4-20mA current loops), digital I/O, and time-critical fieldbus including Modbus on RS485, etc. The simulation results show that the new technique is effective in detecting simulated attacks according to the D5 framework at the cost of adding signal splitters and convertors.

3.11 University of Sao Paulo (USP)

USP has developed software designed to simulate the propagation of malware within clustered large-scale systems, with the capability to adapt to various network topologies depending on the connectivity of the devices. A reference model based on the architecture of Ghana's MPE, detailing the number and connectivity of devices (PRDs, portals, backpacks, vans), was developed and simulated to analyze malware propagation, as can be seen in Figure 2. The team employed two approaches to modelling: (i) population models, which provide an overview of the propagation process in general terms by outputting predicted numbers of infected computers in each cluster [14], and (ii) cellular automata, which replicate the propagation process in a simplified dynamic model [15]. These approaches, used together, provide complementary insights.

A virtual testbed is now under development for calibration and validation of the proposed models, based on simulators for the networked devices and systems. The testbed is configurable, designed to be capable of simulating the MPE and larger setups. The simulators are implemented in containers, connected by virtual networks. Associated communications, such as serial channels, Bluetooth, etc., will be simulated inside the containers if needed. Simulated devices include radiation portal monitors, gamma sensors, portable radiation detectors as well as conventional equipment such as gateways and routers. The device simulator basic functional diagram is shown in Figure 4.

The simulator includes two main modules: a physical module, which can reproduce physical and functional characteristics like radiation measures for different physical inputs (e.g. a radiation source approaching the sensor, the release of radiological material close to the sensor, etc.) and a cyber module, which during normal operation reproduces regular communication with other devices. It also processes cyber inputs and reproduces characteristics like vulnerabilities or propagation strategies, in case the device is compromised and actively trying to infect other network nodes. These characteristics are based on pre-defined templates both for normal operation as well as for infected status. The modular approach of the simulators will allow the further development of libraries of different devices that can be integrated into various architectures. The goal is to be able to integrate the models' outputs to an intrusion detection system to enhance its performance by associating a map of compromise likelihood for devices and clusters. This map could also be used as a real-time decision aid to suggest actions like decoupling networks or disconnecting or shutting down most vulnerable targets during an incident.

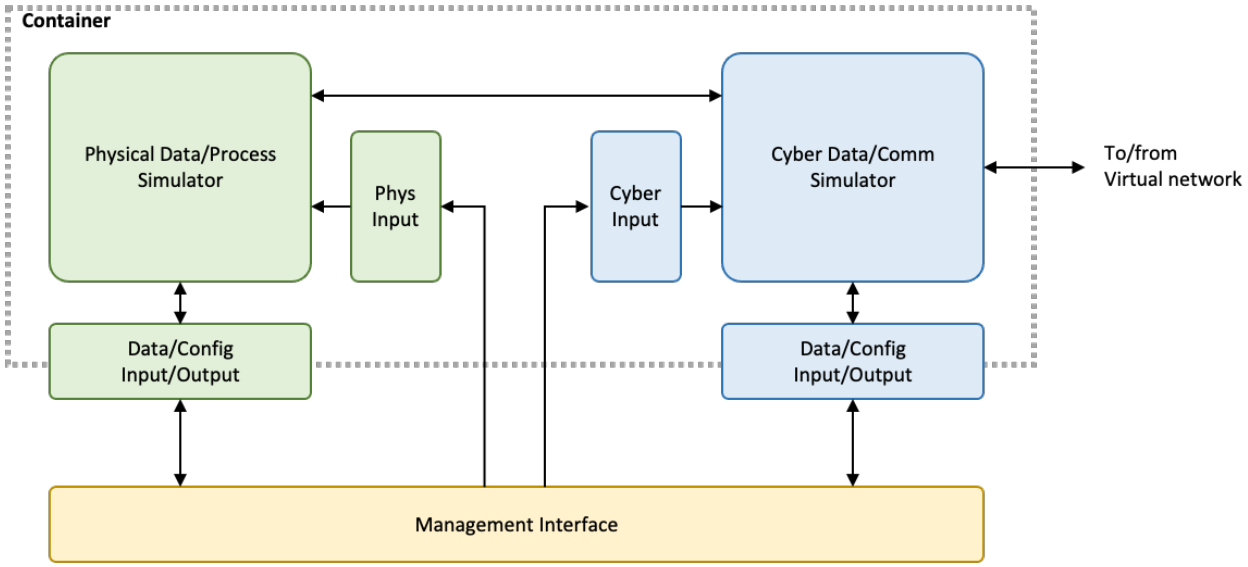

Figure 4. Simulated Device Architecture for the Virtual Testbed

4. CONCLUSION

The CRP on Enhancing Computer Security for Radiation Detection Systems brings together 11 organizations from 10 Member States to advance the computer security of radiation detection systems. Through their research, the participating institutes have explored various topics, including defensive computer security architectures, malware propagation in radiation detection networks, the use of sensor cloud computing, wireless technologies security, coupled physical protection and radiation detection systems simulations, the development of anomaly detection techniques, and threat modeling.

To summarize the project results to date, the participating institutes have collectively developed reference models for radiation detection system architecture, synthetic radiation data, and cyber data. They have also developed and tested various anomaly detection techniques using AI/ML, conducted vulnerability assessments of radiation detection systems, and created prototypes of testbeds, both virtual and hardware-in-the-loop, including a simulator featuring a 3D model of a hospital. Additionally, they simulated the propagation of malware in a virtual network and assessed the cybersecurity of wireless networks for transmitting radiation data.

As this coordinated project continues to progress, the collective efforts of the participating institutes are expected to significantly enhance the computer security of radiation detection systems, ensuring the confidentiality, integrity, and availability of transmitted, assessed, and stored radiation detection information.

References

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for Major Public Events, IAEA Nuclear Security Series No. 18, IAEA, Vienna (2012).

[2] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[3] IAEA Nuclear Security Training and Demonstration Centre. https://www.iaea.org/about/organizational-structure/department-of-nuclear-safety-and-security/division-of-nuclear-security/iaea-nuclear-security-training-and-demonstration-centre, accessed on 14 November 2024.

[4] C. Schmittner, A. M. Shaaban and G. Macher. ThreatGet: Ensuring the Implementation of Defense-in-Depth Strategy for IIoT Based on IEC 62443, IEEE 5th International Conference on Industrial Cyber-Physical Systems (ICPS), United Kingdom, 2022, doi: 10.1109/ICPS51978.2022.9816864.

[5] T. Holczer. Machine Learning Based Time Series Generation for the Nuclear Industry, International Conference on Computer Security in the Nuclear World: Security for Safety (CyberCon23), IAEA, 2023.

[6] I. Mahmoud and A. A. el-Hamid. Malicious Node Identification in WSNs for Radioactive Source Localization, International Conference on Nuclear Security: Shaping the Future (ICONS2024), IAEA, 2024.

[7] Python. https://www.python.org, accessed on 14 November 2024.

[8] G. Kusuma et al. Gamma Monitoring System based on BG51 PIN Photodiode Detector, 10th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Indonesia, pp. 287-292, 2022, doi: 10.1109/ICITACEE58587.2023.10276744.

[9] I. Susila et al. Development of Environmental and Radiation Monitoring System based on Private LoRaWAN Network, International Conference on Advances in Nuclear Science and Engineering (ICANSE), Indonesia, 2024.

[10] A. Brown et al. Safecast. Successful Citizen-science for Radiation Measurement and Communication after Fukushima, Journal of Radiological Protection 36.2 S82, 2016.

[11] N. Coolidge et al. An Efficient Intrusion Detection System for Safeguarding Radiation Detection Systems International Symposium on Future I&C for Nuclear Power Plant (ISOFIC), 2024.

[12] MathWorks. https://www.mathworks.com/products/simulink.html, accessed on 14 November 2024.

[13] J. Li and B. Li. Cyber Anomaly Detection based on Physical Raw Signal Monitoring, International Symposium on Future I&C for Nuclear Power Plant (ISOFIC), 2024.

[14] J. R. C. Piqueira, M. A. M. Cabrera and C.M Batistela. Malware Propagation in Clustered Computer Networks. Physica A: Statistical Mechanics and Its Applications V573, 2021.

[15] A. C. B. Godoi and J. R. C. Piqueira. Spatio-temporal Malware Containment Model with Alert, Chaos, Solitons and Fractals V173, 2023.