UNDERSTANDING NUCLEAR CYBER SECURITY MEASURES, RISKS AND CONSEQUENCES: FROM TANK LEVELS TO PLANT PROCESSES

R. A. BUSQUIM E SILVA
University of Sao Paulo - Sao Paulo, SP, Brazil
Massachusetts Institute of Technology - Cambridge, MA, USA
Navy Technological Center in Sao Paulo - Sao Paulo, SP, Brazil
Email: busquim@alum.mit.edu

J. R. C. PIQUEIRA
University of Sao Paulo - Sao Paulo, SP, Brazil

R. P. MARQUES
University of Sao Paulo - Sao Paulo, SP, Brazil

P. SMITH
Austrian Institute of Technology GmbH – Vienna, Austria

M. HEWES
International Atomic Energy Agency - Vienna, Austria

J. LI
Tsinghua University – Beijing, China.

R. ALTSCHAEFFEL
Otto-von-Guericke University of Magdeburg – Magdeburg, Germany.

Abstract

Cyber security has been object of study since the beginning of the digital era. However, until the 2010 Stuxnet case in the Iran's enrichment facility at Natanz, most of world's cyber security concerns were directed to the theft of sensitive information. The desire for understanding the impacts of cyber-attacks - and how they propagate - in cyber-physical systems led to the development of operational technology (OT) simulators. Many of these simulators use industrial tank liquid level controllers that are common to industries such as energy, oil & gas, chemical and metallurgy. These controllers maintain the level of boilers, condensers or pressurized tanks. They usually work by having a piece of software checking and adjusting the balance between inputs and outputs: digital programmable logic controllers simulate or control pumps and valves that maintain the level between predefined values. Therefore, tank level controllers, due to their simplicity, are the tools-of-choice to represent the effects of a cyber-attack in real world equipment. However, nuclear power plant (NPP) are complex systems that must be represented by complex simulators. Moreover, with the massive use of digital technology, NPPs are becoming more tightly integrated. Therefore, preliminary research results suggest that the development of computer security measures, to prevent and protect against cyber-attacks on OT systems, could be favored by studies carried on NPP simulators, like the Asherah Nuclear Power Plant Simulated (ANS) developed under the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) J02008. ANS was designed to be able to survive cyber-attacks, to allow the capture of data for "*a posteriori*" analysis, and to have flexibility in terms of network communication and hardware in the loop integration.

1. INTRODUCTION

Given the complexity and large scale of current digital based industrial systems, especially in the Nuclear Industry, a state-of-the-art critical infrastructure cyber-physical assessment should consider test beds and simulation environments with up-to-date Information and Technology (IT) and Operational Technology (OT) systems.

From the teaching point of view, a comprehensive and immersive simulation environment improves training capabilities by allowing a better understanding of the digital systems security and safety constraints, as well as evincing the physical interconnections between different systems and equipment. Moreover, realistic simulations as part of a live-fire exercise (LFX) are an effective tool to teach the specificities of OT and IT cyber security.

After the Iran enrichment facility cyber-attack [1-3], many digital specialists - and countries – started focusing their attention in real world cyber-physical systems that may be the subject of sabotage. Following this trend, especially in the last few years, cyber defence exercises and training courses started using simplified (sometimes improvised) test beds with IT and OT equipment. Cyber-physical systems are integration of computation and physical processes where computers and feedback loops, connected by digital networks, monitor and control the behaviour of real world processes.

Tanks and tank level controllers are very common to industries such as energy, oil & gas, chemical and metallurgical. Programmable Logic Controllers (PLC) employed in such systems regulate and maintain the level of boilers, condensers or pressurized tanks within operational limits. They usually work by having a piece of software implementing algorithms that check and adjust the balance between inputs and outputs, for example by driving pumps and operating valves that maintain the level between predefined values. Given their widespread use and their simplicity, tank level simulators are commonly the tool-of-choice to illustrate the effects of cyber-attacks in real world equipment.

Within this context, Nuclear Power Plants (NPP) are the most emblematic example of a critical infrastructure cyber-target. NPPs consist of several complex industrial processes with a large number of information technology and automation systems, implementing process control, safety and security functions. In addition, the consequences of a NPP accident can range from financial loss due to sabotage or sensitive information theft, to equipment damage or even the release of radiological material and environment contamination. Therefore, NPPs, more than any other critical infrastructure facilities, are accountable to extremely rigid safety and reliability requirements that demand redundancy, diversity, and long lifecycles.

A Coordinated Research Project (CRP) was proposed in 2016 by the International Atomic Energy Agency (IAEA) and counts with seventeen institutions from thirteen countries. The CRP, entitled *Enhancing Computer Security Incident Response Analysis at Nuclear Facilities* (J02008), is the first coordinated project proposed by the IAEA on computer security [4]. In view of the presented above, University of Sao Paulo (USP), under CRP J02008, developed a hardware-in-the-loop (HIL) simulator, the Asherah NPP Simulator (ANS), suitable for digital research, cyber security assessment and computer security measures development. The ANS, compared to a standard tank level controller test bed, allows a much better understanding of the consequences of a cyber-attack, including the impact on the facility in physical terms.

Also, under the CRP J02008, a control room human-machine-interface (HMI) was developed by Tsinghua University and integrated with the ANS. This HMI adds the operator perspective to security research and assessment as well as to training exercises. Other institutes, like the Austrian Institute of Technology (AIT) and the Otto-von-Guericke University of Magdeburg, have been integrating the ANS within HIL test beds and developing anomaly detection tools using the ANS.

2. SECURITY SAFETY INTERFACE

Safety issues linked with instrumentation and control (I&C) systems have historically been the subject of much attention by the nuclear industry (see for instance [5]). Safety is directed at preventing accidents at NPPs or other nuclear facilities. Security, on the other hand, is aimed at preventing intentional acts against the normal nuclear facility operation or that may result in theft of nuclear material. In the last decade, cyber security added new dimensions to the problem, but approaches were usually biased to information theft and IT systems and equipment. With the Stuxnet cyber-attack, more attention was given to the link between cyber threats and I&C systems and eventual safety impacts.

Although much effort has been made to guarantee the safety of digital I&C systems, cyber threats pose new safety challenges for which current approaches and postulated principles may not be effective. For instance:

- Compromised I&C system behaviour may be very different from that of faulty systems in the sense that they may present unexpected functionalities instead of mere functionality loss. A set of systems could even act in conjunction with the objective of maximizing damage while preventing mitigation actions by other systems.

- A single attack can affect multiple systems and provoke many simultaneous effects, so system resilience to single failures may not provide an effective defence.

- Evaluation tools commonly employed in safety assessments like Probabilistic Risk Assessment (PRA) may not be adequate to cyber threats, given their intentional characteristic and planning.

- Functional independence may not increase safety if the independent systems present similar vulnerabilities and exposure levels.

On the other hand, security measures like regular software updates, deployment of firewalls, etc. may have safety impacts, by degrading I&C systems functionality or increasing overall complexity. A key point in understanding this more complex context is that when dealing with I&C systems, the safety/security interface involves the physical behaviour of the plant and related equipment, evincing the need for tools capable of taking this characteristic into account.

3. FACILITY IMPACT ASSESSMENT

The physical behaviour of a NPP is rather complex and involves a large number of variables dynamically coupled. Moreover, the control system implements several feedback loops in order to regulate the process that increase the coupling and add to the general system complexity.

In order to reproduce the plant behaviour and assess facility impact after a cyber-attack, computer simulation of dynamic models of the plant and controllers is arguably the best tool currently available.

3.1 From tank levels to functions

The ANS model is based on the 2,772 MWt Babcock & Wilcox (B&W) design pressurized water reactor (PWR) implemented using Matlab/Simulink. The ANS simulates the nuclear processes and thermohydraulic relations in the plant along with the control system dynamics and it is the heart of a comprehensive HIL simulation environment. The ANS was used for the first time as a training tool during the *Second Brazilian Cyber Guardian Exercise* (EGC 2.0) event in July 2019 in Brasília, Brazil. It was also employed later in 2019, during the *International Training Course (ITC) on Protecting Computer-based Systems in Nuclear Security Regime* (Daejeon, Republic of Korea, November 2019).

The systems requirements for implementation of the lumped parameters PWR simulator and the inexpensive HIL test bed for cyber security assessment included the use of standard OT and IT systems. The key communications protocols are Modbus TCP/IP and OPC Unified Architecture (OPC UA) providing the necessary infrastructure for interoperability across the test beds (machine-to-machine, machine-to-enterprise and everything in-between).

Even well-established analog legacy plants have recently been including digital systems. This is a trend associated with the license extension for older plants and the unavailability of replacement parts. These new systems need to be well-suited to face cyber security challenges.

In order to improve its flexibility and facilitate its use in different situations with diverse configurations, the Asherah test bed (ATB) was designed to allow the incorporation of physical equipment with the same functionalities as that of their simulated counterparts. This is done by the use of analog/digital electrical interfaces or through network communication over Ethernet. It is noticed that a simulated controller replacement by its real counterpart requires the correct reconfiguration of the interface responsible for analog and digital inputs and outputs.

The simulation of a complex NPP for cyber-security assessment, including all security levels – or at least security levels 2 to 5 - allows a deeper understanding of the interconnection between the non-nuclear and other non-safety critical systems based on IT and the nuclear OT network.

3.2 Further integration

Adequate NPP operation requires the whole plant and the control system to function properly. Therefore, a HIL test bed implementation of any of the control subsystems in physical devices requires simultaneous

simulation of related control subsystems that may require information exchanges and plant processes that present coupled dynamics. Therefore, to adequately reproduce functional and facility impacts of an OT cyber-attack, the NPP primary, secondary and tertiary loops must be integrated in a model comprising different degrees of complexity, depending on each modelled subsystem relevance to the system as a whole. The implementation of the NPP subsystems independently would lead to the loss of significant information related to plant behaviour and operation, so relatively complex simulators are required for proper NPP simulation.

ANS research activities are based on the premise that currently available simulators which were not designed for cyber-attacks would not survive or provide accurate results of the effects arising from simulated cyber-attacks; would not have the capability of properly capturing the data in the volume an rate needed for intensive computer security forensics and analysis; and would not allow realistic hardware and software integration for testing purposes.

Figure 1 presents the ATB architecture with both electrical and network interfaces. Notice that communication is performed in different channels: one for process information (PROC I/O INTERFACE) and another for controller information exchange (CTRL DATA INTERFACE).

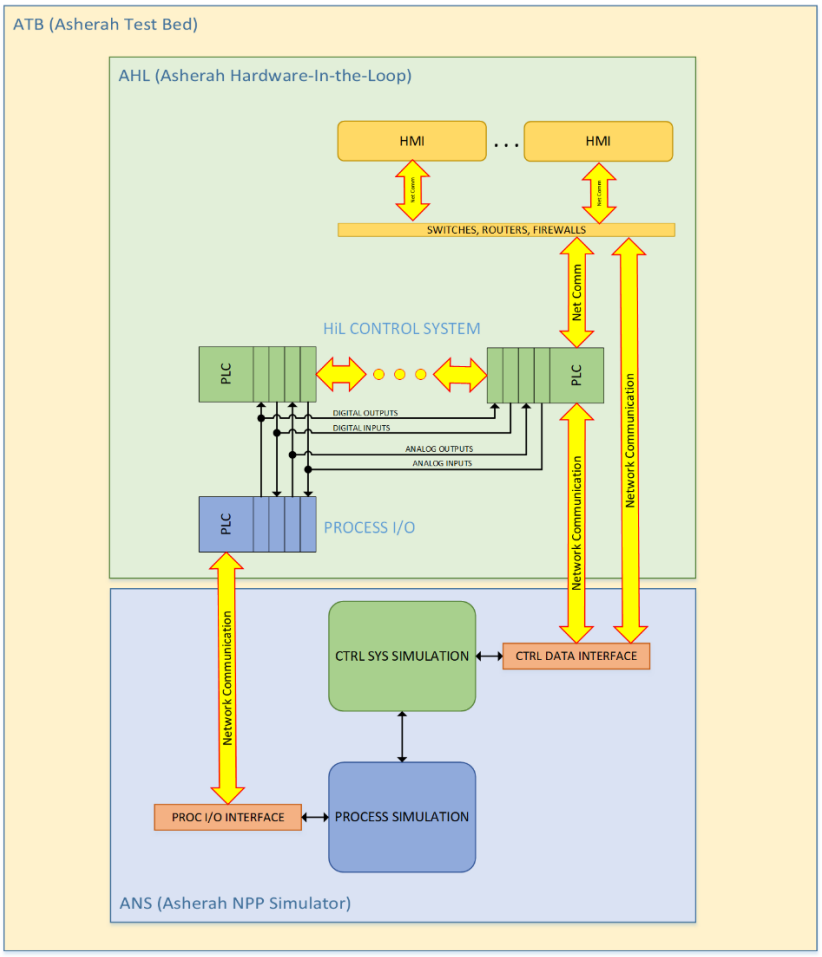

Figure 1 – ATB Architecture

Figure 2 presents the overall I&C layers and defence in-depth levels as related to the project platform (i.e. the ATB) in its current configuration. As research progresses, this context diagram is expected to suffer changes or updates.

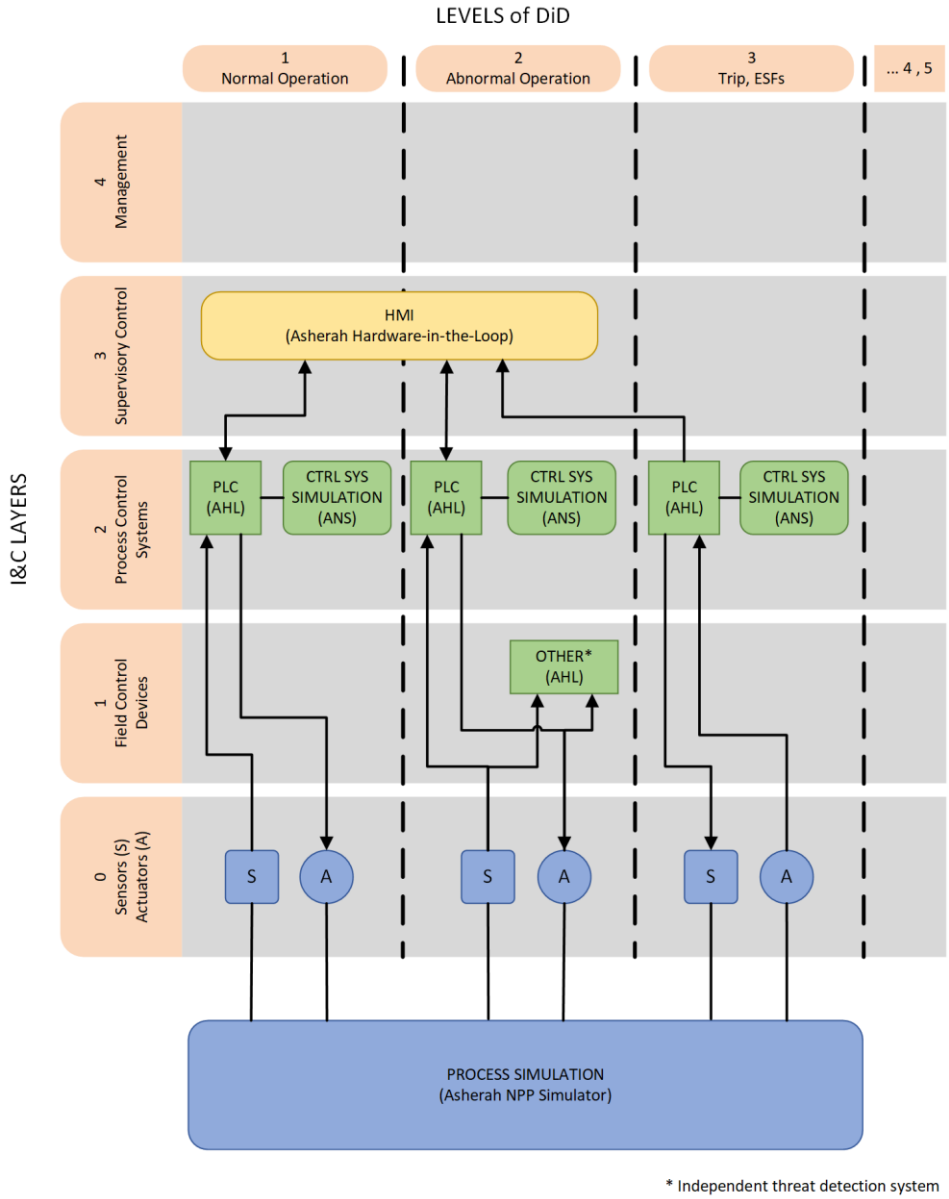

Figure 2 – I&C Defense in Depth

4. A SIMPLE APPLICATION EXAMPLE

In a typical PWR facility, like the one simulated in ANS, the reactor-generated heat is transferred from the primary loop to the secondary loop by the steam generators. The generated steam in the secondary loop is fed to the turbine, condensed in the condenser and refed to the steam generators. Condensing is performed by heat exchange with cooling water circulating in the condenser hull. The cooling water is circulated by a pump, referred as Condensate Cooling Pump (CCP).

During normal operation, this pump operates at rated speed (100%). A cyber-attack causes the CCP to shut down. Attack specifics like scenario/threat modelling are not considered here, the main interest being the immediate attack physical consequences and facility impact.

Normally this event would cause the Reactor Protection System (RPS) to shut down the reactor and initiate the Engineered Safety Functions (ESF) to extract the reactor residual heat. For the sake of illustration, two cases

are considered in the following figures: (a) without RPS actuation (red dashed lines) and (b) with RPS actuation (blue continuous lines).

For case (a) – red dashed lines, the sequence of events is as follows (all signals expressed in percentage of their rated values in the figures). Notice that the signals are not affected by the initiating event only, but also by the plant coupled dynamics and especially by the control system actuation, trying to maintain the plant normal operation parameters.

i) CCP shuts down at time *t* (see Figure 3).
ii) The heat extraction at the condenser ceases, increasing the hull pressure (see Figure 4).
iii) Steam expansion at the condenser discharges the condensate, decreasing the condensate level (see Figure 5). The condenser level control system reduces liquid extraction in order to try to maintain the condensate level.
iv) Turbine power generation ceases (see Figure 6). This is due to the pressure increase in the turbine outlet, propagated from the condenser.
v) Steam generator pressure increases, due to lack of heat extraction at the condenser (see Figure 7).
vi) Insufficient heat extraction at the condenser increases reactor temperature (see Figure 8). The reactor power control system extracts the control rods in order to try to maintain the reactor temperature within limits.
vii) Reactor power is maintained at least initially (see Figure 9), but since there is no heat extraction, despite the process control system actuation, the plant will eventually reach unsafe conditions.

For case (b) – blue continuous lines, the sequence of events is as follows (all signals expressed in percentage of their rated values in the figures).

i) CCP shuts down at time *t* (see Figure 3).
ii) The heat extraction at the condenser ceases, increasing the hull pressure (see Figure 4).
iii) Overpressure at the condenser activates the RPS at *t* + 2.8s (see the gray marker line in the figures), shutting down the reactor (see Figure 9).
iv) Reactor temperature decreases due to RPS actuation (see Figure 8).
v) Condenser pressure is eventually maintained within limits (see Figure 4).
vi) Condenser level decreases, but will eventually stabilize (see Figure 5).
vii) Turbine power production ceases, due to reactor shutdown (see Figure 6).
viii) Steam generator pressure is maintained within limits (see Figure 7).

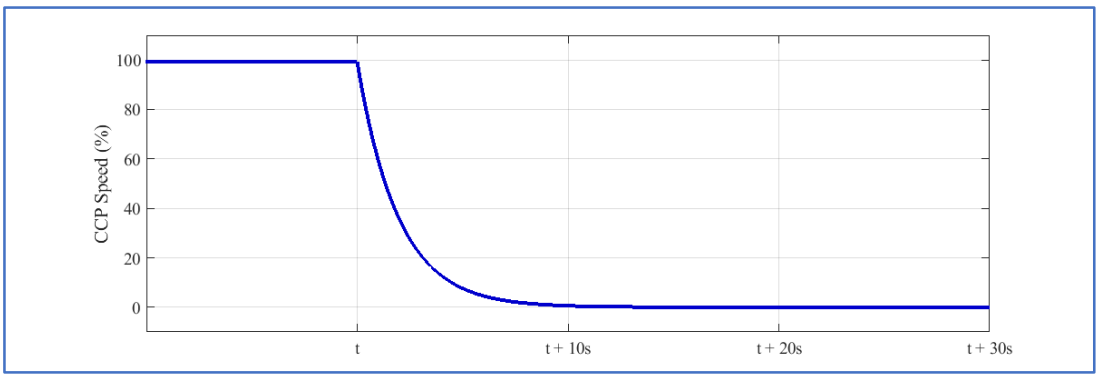

Figure 3 – CCP speed (the pump shuts down at time t)

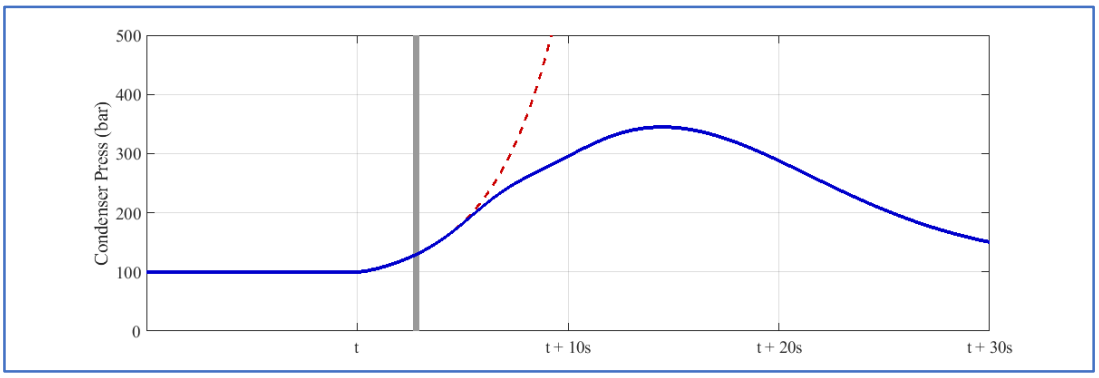

Figure 4 – Condenser pressure

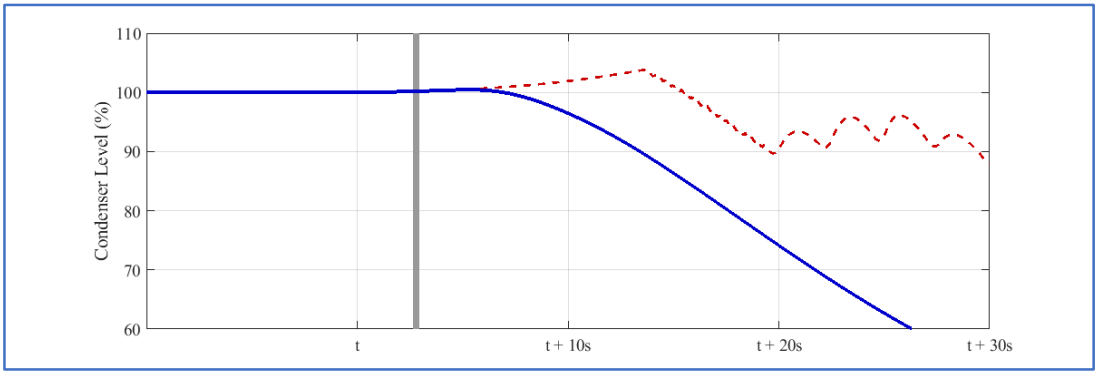

Figure 5 – Condenser level

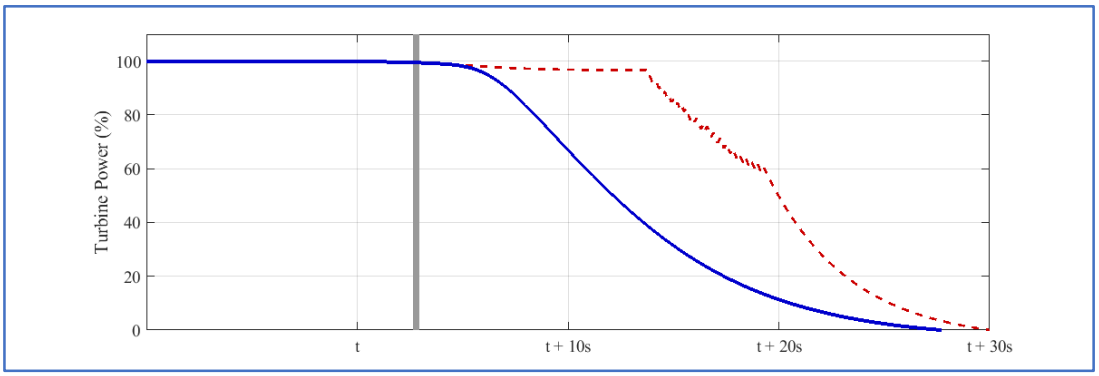

Figure 6 – Turbine power

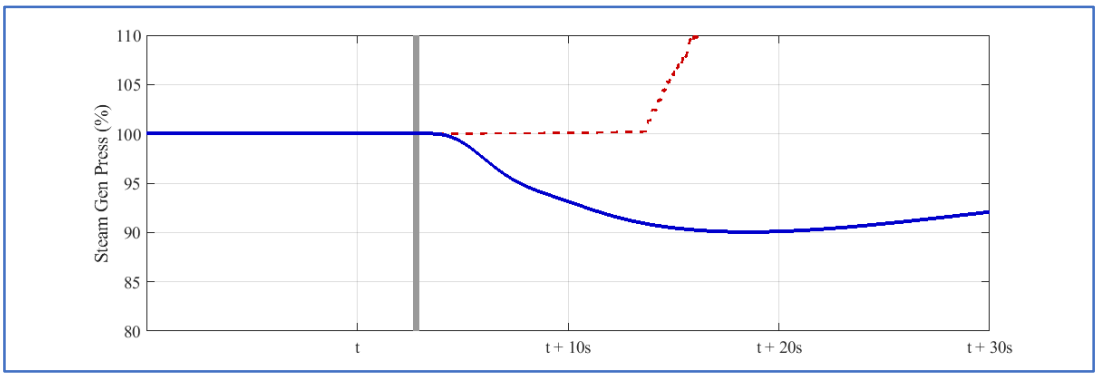

Figure 7 – Steam generator pressure (steam pressure at secondary side)

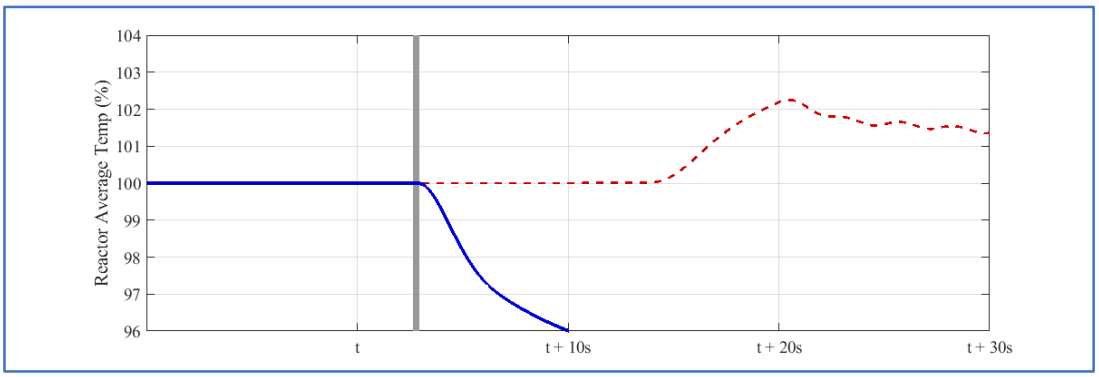

Figure 8 – Reactor average temperature

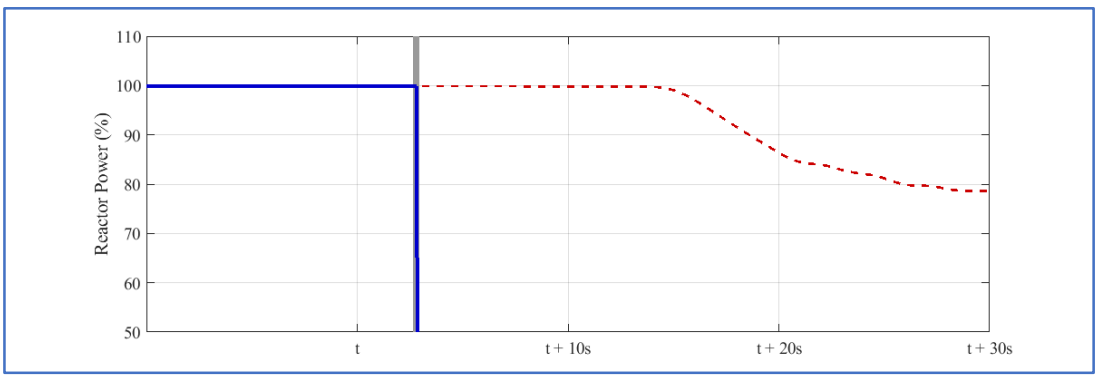

Figure 9 – Reactor power

5. CONCLUSION

ANS is still under development, but preliminary versions have already been used successfully in two training exercises. In addition, it has been shown by a simple application example how a cyber threat on I&C systems can affect system safety. This interaction is rather complex and involves the plant physical behaviour, control system actuation and dynamic couplings. Simulators, especially in a test bed environment as the ANS described here, are invaluable tools for cyber-security assessments, training and research. Compared with simple tank level setups such tools provide a much richer training experience, bridging the gap between operators with

strong nuclear background but no expertise in cyber security and computer experts with no in-depth knowledge of nuclear systems.

6. ACKNOWLEDGEMENTS

This work was supported by the São Paulo State Research Foundation (FAPESP) through Grant 2016/04600-0 and IAEA, through Research Contract No. 22527 (CRP J02008).

REFERENCES

[1] Sklyar, V. Cyber Security of Safety-Critical Infrastructures: A Case Study for Nuclear Facilities. Information & Security, Vol.28, No. 1, pp. 98-107, 2012.

[2] Stuxnet: Leaks or Lies? http://spectrum.ieee.org/podcast/computing/embedded-systems/stuxnet-leaks-or-lies. Accessed on May 12, 2019.

[3] Busquim e Silva, R.A.; Marques, A. L. F. Digital Instrumentation & Control (I&C) Systems and Cyber Security: Is Supply Chain the Weak Link? International Conference on Nuclear Security: Enhancing Global Efforts, Vienna-Austria, 2013.

[4] Rowland, M.T.; Busquim e Silva, RA. IAEA Coordinated Research Project on Enhancing Incident Response at Nuclear Facilities. 11th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies. Orlando-Florida, 2019.

[5] International Atomic Energy Agency. Design of Instrumentation and Control Systems for Nuclear Power Plants – IAEA Safety Standards Series No. SSG-39. Vienna, 2016.