Nuclear Facilities and Cyber Threats

Silvia Tolo

Resilience Engineering Research Group, University of Nottingham, U.K.
E-mail: silvia.tolo@nottingham.ac.uk

John Andrews

Resilience Engineering Research Group, University of Nottingham, U.K.
E-mail: john.andrews@nottingham.ac.uk

The exponential growth of digital technologies experienced in the last decades has shaped contemporary societies so thoroughly to earn the definition of digital revolution or third industrial revolution. Along with the penetration rate of digital technologies, concerns about systems' vulnerability and the disruptive potential of malicious attacks have rapidly risen among governments and industries as much as in the eye of public opinion.
Such concerns are all the more motivated when referring to the nuclear power industry which, due to historical and safety reasons, appears to be more unprepared and vulnerable to cyber threats than its industrial counterparts. While the isolation of plants' control network from the public internet, generally referred as air-gap, has for long nurtured the belief of security of nuclear power plants, recent events (e.g. Stuxnet worm) have shown the inadequacy of this countermeasure. Moreover, the progressive shift from obsolete analogue industrial and control systems to digital solutions, and the growing capabilities of attackers, are exacerbating the urge for novel strategies able to overcome the inadequacy of traditional risk assessment techniques in addressing such threats.
This study focuses on cyber security challenges peculiar to the nuclear industry and argues the need for novel tools and radically new approaches to assess and mitigate the vulnerability of nuclear facilities to cyber threats. In order to achieve a full understanding of common attack mechanisms, relevant cyber threats targeting the instrumentation and control system of a generic nuclear power plant have been modelled graphically using a Petri net approach.

Keywords: Cyber Attacks, Security, Nuclear Power, Petri Nets, Threat modelling, System Resilience

1. Introduction

The nuclear power industry has long relied on the physical isolation of facilities' computer networks from unsecured networks (e.g. public internet or local area networks) as the main security measure, generally known as *air-gap*. The confidence surrounding the efficiency of such protective barrier has been consolidated also by the large deployment of analogue systems typical of nuclear power generation, which seemed to exclude the possibility of reaching and compromising physical systems through cyber attacks. However, past incidents have uncovered the inconsistency of similar claims, highlighting the vulnerability of facilities to cyber attacks regardless of their isolation from external networks.
Even discarding the shortcomings of air-gap protection altogether, the concerns regarding the adoption of digital technology to inflict malicious actions on nuclear installations are fast growing in the industry as well as among authorities and regulators. This can be traced back to different factors. Firstly, the decline in air-gap designs due to the increasingly intertwined operational technology and information technology, and the growing deployment of digital systems in place of obsolete analogue solutions. This trend implies indeed the loss of protection 'by antiquity', generally provided by analogue systems, but also an alleged reduction in redundancy levels characterizing current facilities. Since digital systems are not independent, many have raised doubts on the veracity of any redundancy claim [Baylon et al. (2015)]. A further argument supporting the thesis of the growing vulnerability of nuclear installations is the loss of protection 'by obscurity'. While nuclear plants built before the 1980s are characterized by highly customized supervisory control and data acquisition systems, generally designed for the only purpose of that specific plant's operations, the nuclear power industry has more recently opened its doors to the adoption of off-the-shelves third party software. These latter provide unquestionable economic advantages and reliability guarantees, but the resulting conformity and accessibility of computer languages and proprietary protocols contributes to increase the exposure of the system to cyber threats.
What is probably more concerning is the growth,

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio
 Published by Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0_output

along with nuclear facilities' vulnerabilities, of cyber criminals abilities and specialized tools. This latter category covers a wide variety of solutions, from search engines able to locate internet-connected industrial systems (e.g. Shodan [Bodenheim et al. (2014)] which is partly freely available [Matherly (2009)] contributing to its fast popularity increase, ERIPP focusing on critical infrastructure) to automated exploit toolkits enabling even low-skilled actors to identify and exploit relevant system vulnerabilities. Alongside this, several sophisticated methodologies adopted with success in the past for the execution of cyber attacks, e.g. Stuxnet computer worm, are in the public domain and hence within reach of any malicious agent regardless of their abilities or expertise.

In this complex and increasingly concerning landscape, a growing number of companies are focusing on the discovering of software vulnerabilities and exploit designs, with the final goal of selling them to paying customers rather than reporting them for patching. Quite surprisingly, this activity is not illegal due to the lack of regulation of the market and allows companies (e.g. ReVuln) to sell zero-day vulnerabilities to the highest bidder [Fidler (2015)].

However, the most problematic aspect concerning potential attackers targeting nuclear facilities remains the rise of state actors ranging from intelligence agencies to military and state-sponsored groups McConnell et al. (2014). The economic and technical resources available to these actors are by far superior to those generally accessible to other types of attackers and provide a fertile ground for long-term campaigns and sophisticated, coordinated attacks. While current state-driven cyber activities focus mainly on cyber espionage, the escalation to cyber conflict is becoming an increasingly realistic prospect (e.g. the already mentioned Stuxnet worm is a perfect example of the emerging cyber warfare capabilities).

In spite of the current security practices being far from effective or robust, the nuclear industry seems to be in two minds regarding the actual severity of cyber threats. Indeed, notwithstanding the increasing concerns of some, most personnel remain reticent in recognizing the weaknesses of current systems and still confident in the air-gap protection. As for many of the sources of concern discussed above, the disbelief is mainly due to a lack of understanding of digital industrial control systems and their evolution.

The proposed study spreads from the conviction that such an issue is rooted in the shortage of technical tools and methodologies able to measure and highlight the possible mechanisms of interaction within cyber-physical systems and their consequences. This void has to be filled by adequate research efforts, tailored on the specific requirements and challenges of the nuclear power industry. In light of these considerations, this study aims to provide an outline of the issue, a measure of its severity and a brief overview of the currently available solutions. Section 2 analyzes the nature of cyber threats targeting nuclear facilities and offers a brief summary of relevant cyber incidents occurred in the past. Section 2.2 shifts the focus to the architecture of nuclear power plants' information systems and their vulnerabilities. Section 2.3 briefly introduces the most common methodologies adopted for threat modelling, inside and outside the nuclear sector. Finally, Section 3 discusses five relevant cyber threats, generally enclosed in the STRIDE methodology, and provides graphical Petri net models aimed at enhancing their interpretation and assessment.

2. Nature of the Threats and Challenges

IAEA has highlighted three main possible risk scenarios involving cyber attacks and nuclear facilities: *cyber sabotage*, when the attack results in physical equipment damage or loss of availability, *cyber espionage*, when the focus of the attack lies with the theft of sensitive nuclear information, and *cyber aid* in the unauthorized removal of nuclear material. In spite of the growing concerns and guidelines provided by nuclear regulatory bodies, the industry remains still somehow confident of the air-gap security allegation and reluctant to treat cyber threats as though traditional physical security threats [Baylon et al. (2015)]. This can be traced back to several cultural (e.g. lack of understanding and training of nuclear power plants (NPPs) personnel, difficulties communicating with cyber security experts, lack of proactive approaches and regulations), technical (e.g. existent industrial control systems *insecure by design*, complexity of patches implementation, supply chain vulnerability) and industry-wide challenges (paucity of regulatory standards, inadequate risk assessment, insufficient investments on cyber security). However, the main issue frustrating the efforts to overcome such challenges lies with the infrequency of cyber incidents disclosure and with the traditional hesitancy of nuclear industry over information-sharing. Similar issues are also affecting other industrial sectors, where the concerns surrounding professional reputation motivate the unwillingness to disclose cyber security breaches. In the nuclear sector this trend is exasperated by the public perception of nuclear risks and the national security sensitivities which have nurtured a rather hermetic industry culture. This results in the impossibility to capture the true extent of cyber vulnerabilities, the inability to learn from past occurrences and the fostering of a false belief of security.

2.1. *Recent Incidents*

In spite of the very limited literature, an overview of major disclosed cyber incidents provides large evidence of the existent vulnerabilities of NPPs to cyber attacks and the shortcoming of the air-gap claim. The first of these events dates back to 1992, when a technician working at the Ignalina nuclear power plant in Lithuania introduced a virus in the computational system devoted to the control of the plant's auxiliary systems. The attack was claimed to be intended to highlight the vulnerability of the facility to possible cyber attacks and did not result in major damage for the installation. However, the potential consequences of a similar offensive has been recognized to be catastrophic [Bukharin (1997)].

In July 2002 Microsoft reported a software security vulnerability in SQL server. Despite the awareness of the vulnerability and the provision of a patch, six months later the computer worm known as SQL slammer was launched and spread rapidly, exploiting the buffer overflow bug in Microsoft's SQL Server and Desktop Engine database products. The worm triggered a denial of service on several Internet hosts dramatically slowing down internet traffic worldwide. Among the networks affected by the Slammer worm there was the corporate network of First Energy Nuclear, which had been infected by the worm spreading from a consultant's network. The infected First Energy Nuclear network was directly connected to the supervisory control and data acquisition (SCADA) system of the Davis-Besse NPP in Ohio, which the company still operates. In January 2003, the Slammer worm found its way to the SCADA system from the corporate network, overwhelming the system with an abnormal amount of traffic and resulting in the unavailability of the safety parameter display system (i.e. for the monitoring of core coolant system, temperature and radiation) for several hours [Kesler (2011)]. The attack did not result in major damages, thanks to the reactor being non operational at the time. However, the event brought to the fore the lack of adequate defenses of industrial control systems to external threats, even when not specifically designed for or targeting nuclear facilities.

In August 2006, the failure of the reactor circulation pumps and condensate demineralizer controller triggered the risk of a core meltdown at Browns Ferry NPP, requiring the manual shutdown of Unit 3. Even if not classifiable as a cyber attack, the incident exposes the lack of preparedness and robustness of nuclear facilities against the failure of few plant components. Indeed, both the devices, i.e. programmable logic controller (PLC), failed due to the excess traffic produced by the Ethernet network used by the devices' microprocessors to send and receive data.

Another example of a cyber incident not motivated by malicious purposes but still highlighting the inadequacy of current solutions occurred in March 2008, at the Hatch NPP in Georgia. This was initially provoked by the installation of a computer update on the plant's business network by a contractor. The update was designed to synchronize data between the plant's Instrumentation and Control (I&C) system and the computer. This resulted in the temporary resetting of the I&C system data to zero, which led the plant operators to believe the water level to be insufficient to cool the reactor, triggering an automatic 48 hours shutdown of the plant's Unit 2 [Krebs (2008)]. This demonstrates the lack of understanding and training of NPP personnel and the potential for easy access to I&C systems from business networks, which are largely vulnerable to cyber attacks. More recently, the sophistication of the Stuxnet worm has raised the bar for cyber attacks and boosted the awareness of their potential. The malware was designed to target specific Siemens industrial control systems reprogramming the connected PLC devices, so to be able to modify system operation. The ultimate objective of the attack is believed to have been Iranian uranium enrichment facilities whose I&C system, due to their sensitivity on a national scale, was not directly connected to the Internet. According to reconstructions of the attack, the Stuxnet worm may have entered the facility I&C system through the connection of an external device (e.g. USB drive), which in turn could have been infected due to the propagation of the worm throughout the corporate network. This was achieved through the exploitation of several Windows vulnerabilities and at least four zero day exploits [Kriaa et al. (2012)]. In June 2010, the Stuxnet worm finally found its way to the Bushehr NPP and the Natanz nuclear facility in Iran, where it detected the target Siemens system and subsequently reprogrammed the centrifuges PLCs to increase the spin speed over the design point, providing false feedback to avoid detection. This led to the partial destruction of about 1000 centrifuges, fully exposing the destructive potential of similar technologies. Morevoer, the worm is believed to have propagated well over the designed objectives, affecting a not better identified Russian NPP and confirming that an air gap is in no way a sufficient protection [Kaspersky (2013)].

While events exposing the potential of cyber attacks to damage physical systems are relatively rare and generally require some degree of disclosure, incident motivated by extortion purposes, despite rarely reported to the public, are believed to be rather frequent and even on the rise. To this category belongs the attack to the Korea Hydro and Nuclear Power Co., where hackers gained access to the commercial network of the company through phishing emails and were able to steal sensitive data (e.g. blueprints and manuals of

two reactors). The data were leaked in December 2014 and March 2015: the attackers demanded a ransom not to release further stolen information and threatened to damage the facility (the threat later proved to be empty) [Baylon et al. (2015)].

2.2. *Nuclear I&C systems*

Regardless of the attacker's nature and objective (e.g. data theft rather than sabotage etc.), the vulnerability of technological installations to cyber threats lies with the design and security of I&C systems. The definition of I&C systems embraces all those subsystems and components designed to contribute to the collection, process, display and transmission of information as well as to the dispatch of control commands to remote equipment. The evolution of these systems has been driven by the breakout of digital engineering, which has revolutionized the usage and design of I&C systems far more abruptly and radically than any other NPP technologies. However, the intrinsic inertia of nuclear industry in adopting new technologies, mostly attributable to the rigid safety standards, has contributed to the creation of an unique landscape and subsequently to unparalleled challenges in terms of cyber security. A large part of the currently operational facilities relies on process technology dating back to the 1950s and 1960s [IAEA (2011)], failing to capitalize on the functionality and performance enhancement experienced by the I&C industry. The use of analog-based technologies has long been motivated by the isolation, and hence protection, that they provide against external malicious actors, which may instead be able to hack computing and communications systems to their advantage. This has resulted in the claim of NPPs to be "air-gapped", namely perfectly secluded from the internet and then virtually unreachable to cyber attackers. However, the occurrence of past cyber incidents has discredited such claims altogether, highlighting the full extent of NPPs vulnerability to cyber attacks. Moreover, I&C systems have much shorter life cycles than NPPs, implying the unavoidable need for multiple upgrades during a facility's life and hence fostering the debate on the suitability of I&C solutions. This has contributed to a progressive - albeit slow - change in design philosophy, with new Gen III+ plant designs fully exploiting the benefits that the I&C industry offers and existent facilities gradually shifting towards digital systems as analog-based technologies become obsolete. Nonetheless, the deployment of digital I&C systems and general IT-technology has the potential to open up facilities to security threats, hence exacerbating the need for tailored and robust solutions along the entire I&C system life cycle.

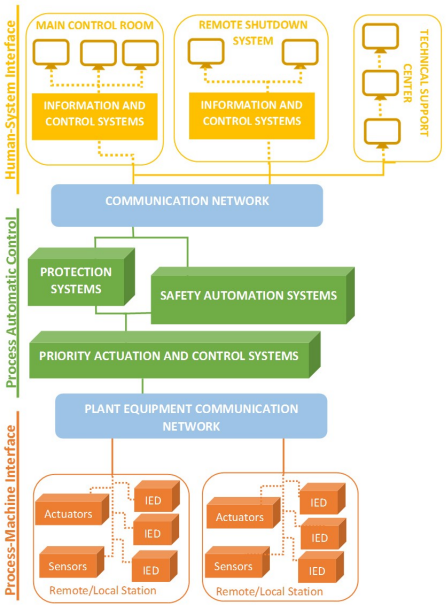

Fig. 1. Example of I&C system architecture for nuclear facilities

2.2.1. *System Anatomy*

Regardless the scale of the technological spectrum characterizing current nuclear I&C systems, generally their architecture encompasses three levels:

- Process-Machine Interface: embraces field instrumentation, namely all those components such as sensors and actuators, designed to directly interact with the ongoing physical processes. This implies continuous data collection through the measurement of plant variables such as neutron flux, temperature, pressure, flow, etc., and the activation of actuators to adjust the plants physical processes. Data acquisition covers all signals for control, safety and monitoring purposes, while the actuator activation functionality addresses control and safety tasks. Field communication follows strict protocols, which can be either analog, digital or hybrid. Analog signal is still the standards most commonly deployed in NPPs. The Highway Addressable Remote Transducer (HART) protocol offers the possibility to superimpose a digital signal to the analog one, allowing for digital data communication between the the transmitter and the signal processing systems while keeping the analogue output still available. Although still widely used in digital bus systems, this has been more recently flanked by numerous other

digital wired simplified protocols which limit the need for cabling installation. Finally, digital wireless communication protocols are available even if currently generally restricted to diagnostic signals transmission. Even if their deployment is still very limited in the nuclear sector, wireless technology has already been adopted in few NPPs, e.g. at the Exelon Nuclears Limerick Generating Station in Pennsylvania (for vibration and temperature signal transmission) or San Onofres NPP in California, where several plant motors are monitored remotely by wireless temperature sensors and transmitters [et al. (2008)]. However, due to reliability and security concerns, wireless field communication is generally restricted to the transmission of plant equipment diagnostics signals.

- Process Automatic Control: consists of systems dedicated to the processing and controlling of plant parameters, with the ultimate goal of ensuring plant safety and efficiency. Signals from sensors are indeed received from the former to be automatically conditioned (i.e. normalized) with the ultimate goal to be uniformly processed according to the nature of process parameters and detection methodology. This can entail scaling, linearization, filtering and the estimation of the deviation between the parameter measured and its design value or threshold. The resulting information is used to adjust the plant behaviour accordingly through the control of actuators. The automation of both safety-related and operational control processes reduces the operators' workload and the risk of human error, and can be carried out through the adoption of analog as well as digital I&C systems. The first rely on electric voltages or currents and analog electronics, while the second make use of computer processors, hence using a binary representation of both incoming and outgoing signals.
- Human-System Interface: provide a platform for the interaction between the operators and the systems included in the former levels, providing the ultimate plant supervision and control. This supplies relevant system state monitoring information to the control room for human surveillance and diagnostics, alarm management for detecting process abnormalities and manual control. The location of such systems can be either central (i.e. main control room) or remote. Solutions currently deployed cover a very wide technological range and can be classified as hard-wired or computer based. The first strongly relies on the cognitive capability of the operators (e.g. pattern recognition) and on the use of simple devices such as indicators, recorders, switches, pushbuttons etc. While hard-wired solutions may interface to both analog and digital I&C systems (or more often to a mixture of both), computer-based interfaces are coupled only with digital I&C systems or otherwise limited to plant information systems. Differently from the previous case, in computer-based system the information is not permanently presented in fixed positions and the control interaction elements are generally not continuously available in parallel, relying instead on the wide use of video display units. However, digital systems can still be coupled with traditional human-system interfaces through the use of additional hardware to convert the conventional indication: such approach, generally more expensive, characterizes hybrid control rooms.

2.3. *State of the Art and Current Practice*

Because of the relative novelty of cyber security threats and the wide range and variety of systems and interaction mechanisms, to define an universally agreed response and mitigation strategy results extremely challenging. However, the limitations in addressing cyber security in nuclear facilities go well beyond the response stage and instead affect the threat-system mechanism in its entirety. Regulatory bodies such as IAEA, NIST (National Institute of Standards and Technology), WINS (World Institute for Nuclear Security) have invested significant efforts in the provision of best practice, guidelines [IAEA (2016), ONR (2017), IAEA (2009)] and risk assessment frameworks [Stoneburner et al. (2002),Stouffer et al. (2011)] for securing the I&C systems of nuclear facilities. Nevertheless, rarely the recommendations and guidance provided go as far as providing technical and detailed procedures specific to the NPPs architecture [Masood (2016)]. There is indeed a lack of well defined standards to identify the compliance of the facilities and provide a security baseline against which to compare and update existent systems. Even the available design basis threat profiles fail to address cyber protection, focusing instead mainly on the plants' physical safety for the definition of threat levels and security strategies. This can be partly traced back to the limited maturity of the ongoing efforts but also to the lack of well-established universally agreed approaches to cyber threat modelling and assessment. Novel tools and approaches have hence to

focus on capturing in detail the potential of threats and the possible mechanisms of interaction, taking into account both stand-alone and coordinated attacks against I&C systems.
The key to achieve a full understanding of cyber attacks and hence to be able to draw adequate mitigation measures, enhancing the resilience of nuclear facilities to this kind of threat, lies unquestionably with the availability of effective modelling tools. The scientific literature of the past two decades has witnessed several efforts aimed at identifying suitable simulation approaches to understand, explore and mitigate cyber attacks. However, there is a general lack of standard methodologies for the frameworks proposed and a general tendency to embrace in the same category methodological frameworks, computational tools for quantitative assessment and qualitative analysis.
Several generic threat modelling frameworks (e.g. PASTA [UcedaVelez (2012)], LINDDUN [Wuyts et al. (2018)]) have been proposed to capture the unfolding of cyber attacks. The most mature and established was proposed by Loren Kohnfelder and Praerit Garg in 1999 [Kohnfelder and Garg (1999)] and was named after the acronym of six types of security threats, namely Spoofing (i.e. impersonating something or someone else), Tampering (i.e. modifying data or code), Repudiation (i.e. Claiming to have not performed an action), Information disclosure (i.e. Exposing information to someone not authorized to see it), Denial of Service (i.e.Deny or degrade service to users) and Elevation of Privileges (i.e. Gain capabilities without proper authorization). The STRIDE framework has been successfully applied to several systems including cyber-physical [Khan et al. (2017)]. In terms of quantitative computational tools aimed at estimating the cost and likelihood of cyber threats, attack trees [Swiler and Phillips (1998)] are by far the most widely adopted technique for cyber attack analysis and one of the first to be applied to I&C systems [Byres et al. (2004)]. They rely on the use of conceptual tree-structured diagrams to capture the transition between different attack phases in order to identify possible attack paths. This methodology allows for both qualitative and quantitative analysis of the attack, the latter requiring the assignment of probability values to all the leaves of the tree in order to propagate the information and quantify the probability of different attack exploits resulting in the top event (e.g. similar to fault trees). However, while facilitating the methodical breakdown of threats this methodology comes with severe limitations in terms of flexibility [Dalton et al. (2006)], for example in the simulation of coordinated attacks or in the consideration of more simultaneous actors. This has stimulated the investigation of different approaches, for instance Bayesian networks [Mo et al. (2009)], Monte Carlo methods [Wang et al. (2018)] or Petri nets. The latter in particular have attracted increasing attention thanks to their capability to model asynchronous and concurrent processes and to analyze delays in timed systems. This has created a promising, although still limited, literature related to the use of Petri nets in security analysis [da Silva et al. (2017), Cho et al. (2016), Jasiul et al. (2014)] and has motivated the adoption of such methodology in the current study.

3. Cyber Attacks Modelling

The current study focuses on the modelling of cyber threats identified by the STRIDE methodology using Petri nets. The aim of such implementation is to provide low-level threat models tailored on the generic characteristics of a I&C system architecture of a NPP. The attack mechanisms outlined by the proposed models are based on attack tree models discussed in the study by Masood [Masood (2016)].
The use of Petri nets would facilitate the integration of threat models in larger existent frameworks for the modelling of nuclear systems, allowing to measure the resilience of such installations against cyber-physical failure or sabotage.
It is worth stressing that such threats are not necessarily isolated but can be adopted simultaneously or coordinated in a single attack to compromise one or more functions of the systems. They rely on similar resources and attack strategies but may direct these to different final goals. Among the five models proposed and discussed in this section, it is indeed possible to identify some common paths from which the attack may spread, such as:

- the initial use of social engineering strategies (e.g. phishing) to gather systems' or users' credentials;
- the exploitation of protocol vulnerabilities to introduce malicious code (aimed in turn at bypassing system authorization or tampering with relevant information);
- the acquisition of relevant system information through network eavesdropping which can be adopted to bypass further security protocol (e.g. man-in-the-middle attack);
- performance of brute force inference attack to gather illegitimate authorization or access;
- the use of decryption strategies to access critical credential or digital signatures.

All these options rely on some extent on existent vulnerabilities (e.g. poor personnel awareness and digital culture in the first case, protocol susceptibility in the second) or potential weaknesses (e.g. easy accessibility of the network, shortcoming of crypto-keys, predictability of credentials) of the system itself. The following sections are dedicated to illustrating the Petri nets models pre-

sented in Fig. 2-7, where rectangle shapes represent transitions and ellipse shapes refer to network places.

3.0.1. *Spoofing*

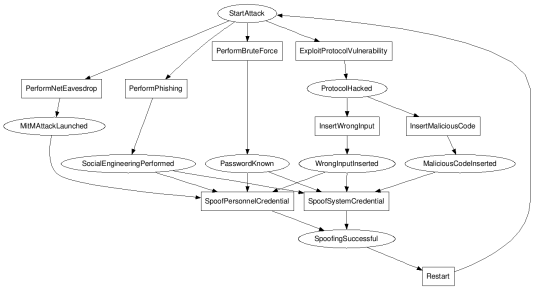

Fig. 2. Petri net model of elevation of spoofing attack

This category encloses those attack mechanisms aiming at gathering illegal access through the false impersonation of a legitimate user by the agents. In the specific case of NPPs this can result in the misuse or disruption of the I&C system, which can be achieved by targeting either the system's or operators' credentials. The first case refers to spoofing the credentials of an I&C system, that could have been obtained by exploiting protocol vulnerabilities (e.g. introducing malicious codes in a web browser) or from legitimate users (e.g. through social engineering practices). In the second case, attackers rely on the use of personnel credentials, which secrecy may be compromised through inference attacks (e.g. brute force attack) and man-in-the-middle attacks in addition to the already mentioned social engineering approach. The Petri net in Fig. 2 aims to capture the possible unfolding of a spoofing attack covering all the discussed options. An example of the use of this kind of interaction can be found in the design of the Stuxnet attack. Several reconstructions have indeed reveled how the computer worm relied on spoofed security certificates to mask its malicious activities in the long run.

3.1. *Tampering*

The Petri net in Fig.3 depicts the mechanism behind a tampering threat targeting a NPP I&C system. The common objective of malicious actions falling in this category is the unauthorized modification of data. The model proposed identifies the possibility of compromising the integrity of data offline (*TamperDataAtRest*), i.e. data stored in a database, or online. In this case, a further distinction is made between the tampering of system parameters (*TamperParameters*) or data flow (*TamperDataFlow*) accessed and modified bypassing

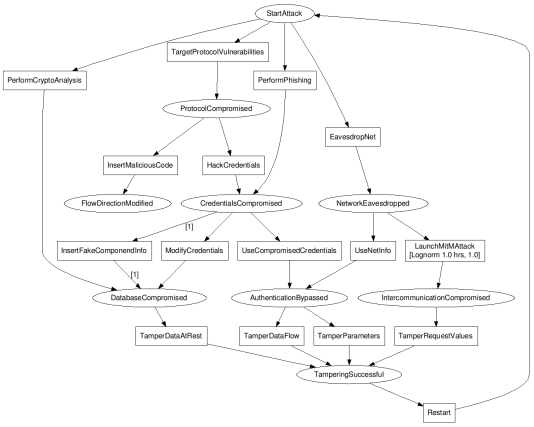

Fig. 3. Petri net model of tampering attack

the system's authentication protocol and the provision of counterfeit values for parameters requested by legitimate users (*TamperRequestValues*). The latter can be achieved through the launch of a man-in-the-middle attack, whose success depends directly on the ability of the hacker to gather relevant information through eavesdropping on the network in use. This kind of attack can result in serious physical damage: in the case of the Stuxnet worm, tampering with the code of PLCs resulted in the destruction of about a thousand centrifuges.

3.2. *Repudiation*

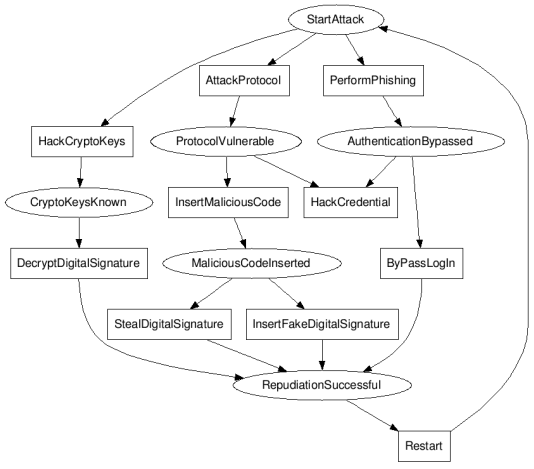

Fig. 4. Petri net model of repudiation attack

This category embraces the ability of users, both legitimate or illegitimate, to deny the performance of malicious actions. This kind of attacks rely on the lack of control of the digital

system and hence its ability to track and log user's action (e.g. due to the absence of audit information, or digital signatures). As shown in Fig.4, the proposed model takes into consideration different mechanisms through which repudiation may be achieved. These range from bypassing system's authentication (i.e. *ByPassLogIn*, *HackCredential*) through the use of social engineering techniques such as phishing or the exploitation of protocol vulnerabilities (*AttackProtocol*), to the use of fake (*InsertFakeDigitalSignature*), stolen (*StealDigitalSignature*) or decrypted (*DecryptDigitalSignature*) digital signatures to attribute the action to other users. Adopting one of these options can hence facilitate not only data manipulation for malicious purposes but also forging the ownership of new actions. This would allow modifying authoring information to cover the action of malicious users in order to introduce compromised data in log files or even to proceed to general data manipulation.

3.3. *Information Disclosure*

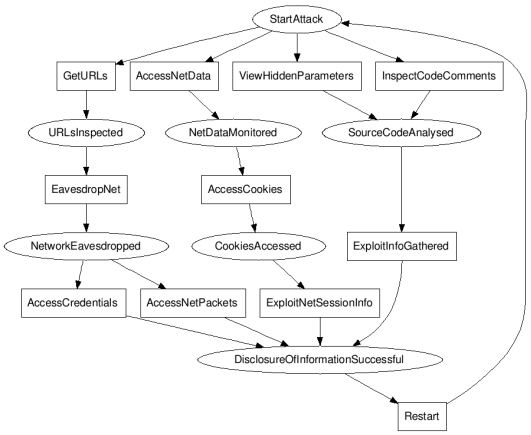

Fig. 5. Petri net model of elevation of information disclosure attack

In the context of the nuclear industry, the success of an information disclosure attack may result in the release of crucial information not only about the I&C system of the facility (e.g. logging details, essential parameters etc.) but also of the plant itself (e.g. documentation, workflow etc.). According to the proposed model (Fig.5), this can be achieved through the analysis of the accessible code (e.g. essential information may have been introduced by programmers in the form of comment, such as for the transition *InspectCodeComments*, or hidden parameters, such as for *ViewHiddenParameters*), the monitoring of the network data through the use of cookies (*AccessCookies*, *ExploitNetSessionInfo*) or through the inspection of URLs and the subsequent network eavesdrop (*getURLs*, *EavesdropNet*).

3.4. *Denial of Service*

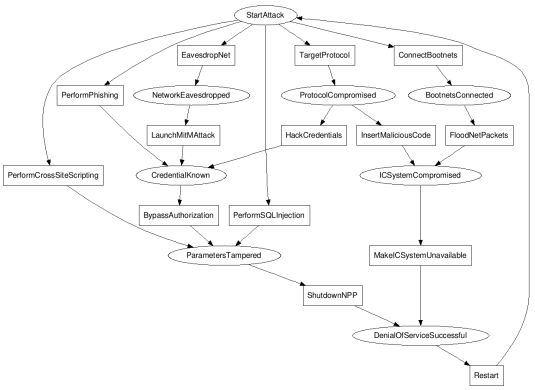

Fig. 6. Petri net model of denial of service attack

As mentioned in Section 2.1, in 2003 the infection of Ohio's Davis-Besse nuclear power plant system with the Slammer worm resulted in the unavailability of the safety monitoring system for nearly five hours. Similar attacks aiming at disabling one or more functions of the targeted system are generally referred as Denial of Service attacks. The model proposed in Fig. 6 considers two main scenarios resulting from such threat: the unavailability of the entire facility (*ShutdownNPP*) and the disabling of I&C critical functions (*MakeICSystemUnavailable*). The success of the first depends on the ability of the attackers to tamper critical systems parameters: this can be in turn achieved by performing cross site scripting (*PerformCrossSiteScripting*), compromising the system's database (*performSQLInjection*) or bypassing the system's authorization procedure through social engineering (*PerformPhishing*), man-in-the-middle attacks (*LaunchMitMAttack*) or the exploitation of protocol vulnerabilities (*TargetProtocol*, *HackCredentials*). The latter can also serve the purpose of compromising the I&C system through the insertion of malicious code (*InsertMaliciousCode*) which ultimately would hinder the availability of the system. This same purpose can be achieved also through the use of bootnets and the subsequent flooding of the network (*ConnectBootnets*, *FloodNetPackets*).

3.5. *Elevation of Privileges*

The definition of Elevation of Privileges attacks embraces all those malicious actions intended at gaining access to a system or resources which fall beyond the user's rights. This is generally a crucial step on which different kinds of attack

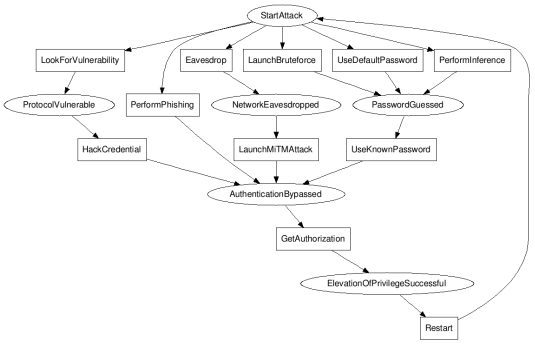

Fig. 7. Petri net model of elevation of privileges attack

rely, included those discussed above. As already mentioned, the system authentication can be bypassed targetting protocols vulnerabilities (*HackCredential*), performing social engineering (*PerformPhishing*), launching a man-in-the-middle attack (*LaunchMitMAttack*) or guessing legitimate credential (*LaunchBruteForce*, *PerformInference*, *UseDefaultPassword*).

4. Conclusions

The proposed study represents a preliminary step toward the implementation of a computational framework for threat modelling of instrumentation and control systems of nuclear facilities and the quantification of their resilience against malicious attacks. Recent cyber incidents occurred in the nuclear sectors have been briefly analyzed and a general overview of the anatomy of nuclear instrumentation and control systems provided. On the basis of these observations, graphical models for the simulation of relevant cyber threats have been implemented. The models offer a novel approach to the five threat categories embraced by the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privileges) methodology proposed by Microsoft in 1999 and rely on a Petri net approach. The motivation behind the adoption of such methodology lies with the potential of Petri nets in modelling coordinated attacks as well as concurrent actions. This indeed offers unquestionable advantages over the more popular and widely adopted attack tree technique in terms of modelling flexibility and reliability.
Further research will focus on the numerical characterization of the implemented networks for validation purposes and their integration into more comprehensive frameworks aimed at estimating the resilience of nuclear systems and at identifying effective enhancement and mitigation strategies.

Acknowledgement

This work has been supported by the UK Engineering and Physical Sciences Research Council with the project A Resilience Modelling Framework for Improved Nuclear Safety (NuRes), Grant No EP/R021988/1.

References

Baylon, C., R. Brunt, and D. Livingstone (2015, September). *Cyber security at civil nuclear facilities: Understanding the risks*. London: Chatham House.

Bodenheim, R., J. Butts, S. Dunlap, and B. Mullins (2014). Evaluation of the ability of the shodan search engine to identify internet-facing industrial control devices. *International Journal of Critical Infrastructure Protection 7*(2), 114–123.

Bukharin, O. (1997). Upgrading security at nuclear power plants in the newly independent states. *The Nonproliferation Review 4*(2), 28–39.

Byres, E. J., M. Franz, and D. Miller (2004). The use of attack trees in assessing vulnerabilities in scada systems. In *Proceedings of the international infrastructure survivability workshop*, pp. 3–10. Citeseer.

Cho, C.-S., W.-H. Chung, and S.-Y. Kuo (2016). Cyberphysical security and dependability analysis of digital control systems in nuclear power plants. *IEEE Transactions on Systems, Man, and Cybernetics: Systems 46*(3), 356–369.

da Silva, M. R., P. H. F. Machado, L. E. de Souza, and C. W. de Souza (2017). Modeling of a cyber-attack in an iec 61850 scenario using stochastic colored petri nets. In *2017 4th International Conference on Systems and Informatics (ICSAI)*, pp. 985–990. IEEE.

Dalton, G., R. F. Mills, J. M. Colombi, R. A. Raines, et al. (2006). Analyzing attack trees using generalized stochastic petri nets. In *Information Assurance Workshop*, pp. 116–123.

et al., K. K. (2008, December). Instrumentation and controls in nuclear power plants: An emerging technologies update. Technical Report NUREG/CR-6992, United States Nuclear Regulatory Commission (U.S.NRC), Washington, D.C. 20555-0001.

Fidler, M. (2015). Regulating the zero-day vulnerability trade: A preliminary analysis. *ISJLP 11*, 405.

IAEA (2009, May). Development, use and maintenance of the design basis threat. IAEA nuclear security series STI/PUB/1386, International Atomic Energy Agency, Vienna, Austria.

IAEA (2011, December). Core knowledge on instrumentation and control systems in nuclear power plants. IAEA Nuclear Energy Series NP-T-3.12, International Atomic Energy Agency, Vienna.

IAEA (2016, June). Computer security incident response planning at nuclear facilities. Iaea-tdl-005, International Atomic Energy Agency,

Vienna.

Jasiul, B., M. Szpyrka, and J. Śliwa (2014). Detection and modeling of cyber attacks with petri nets. *Entropy 16*(12), 6602–6623.

Kaspersky, E. (2013). Talk at the press club in canberra, australia. `https://www.youtube.com/watch?v=6tlUvb26DzI&feature=youtu.be`.

Kesler, B. (2011). The vulnerability of nuclear facilities to cyber attack. *Strategic Insights 10*(1), 15–25.

Khan, R., K. McLaughlin, D. Laverty, and S. Sezer (2017). Stride-based threat modeling for cyber-physical systems. In *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pp. 1–6. IEEE.

Kohnfelder, L. and P. Garg (1999). The threats to our products. *Microsoft Interface, Microsoft Corporation*, 33.

Krebs, B. (2008). Cyber incident blamed for nuclear power plant shutdown. *Washington Post, June 5*, 2008.

Kriaa, S., M. Bouissou, and L. Piètre-Cambacédès (2012). Modeling the stuxnet attack with bdmp: Towards more formal risk assessments. In *7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, pp. 1–8. IEEE.

Masood, R. (2016, August). Assessment of cyber security challenges in nuclear power plants security incidents, threats, and initiatives. Technical Report GW-CSPRI-2016-03, Cyber Security and Privacy Research Institute, The George Washington University.

Matherly, J. (2009). Shodan search engine. *Available at [Online]: https://www. shodan. io*.

McConnell, B., G. Austin, E. Cappon, and N. Kostyuk (2014). *A measure of restraint in cyberspace: Reducing risk to civilian nuclear assets*. EastWest Institute.

Mo, S. Y. K., P. A. Beling, and K. G. Crowther (2009). Quantitative assessment of cyber security risk using bayesian network-based model. In *2009 Systems and Information Engineering Design Symposium*, pp. 183–187. IEEE.

ONR (2017). Security assessment principles for the civil nuclear industry. Technical report, Office for Nuclear Regulation.

Stoneburner, G., A. Goguen, and A. Feringa (2002). Risk management guide for information technology systems. *NIST special publication*.

Stouffer, K., J. Falco, and K. Scarfone (2011). Guide to industrial control systems (ics) security. *NIST special publication 800*(82).

Swiler, L. P. and C. Phillips (1998). A graph-based system for network-vulnerability analysis. Technical report, Sandia National Labs., Albuquerque, NM (United States).

UcedaVelez, T. (2012). Real world threat modeling using the pasta methodology. *OWASP App Sec EU*.

Wang, W., A. Cammi, F. Di Maio, S. Lorenzi, and E. Zio (2018). A monte carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants. *Reliability Engineering & System Safety 175*, 24–37.

Wuyts, K., D. Van Landuyt, A. Hovsepyan, and W. Joosen (2018). Effective and efficient privacy threat modeling through domain refinements. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, pp. 1175–1178. ACM.