SAND2019-5166R

Safeguards Information Assurance by Design

Dianna S. Blair
F. Mitch McCrory

Sandia National Laboratories
PO Box 5800
Albuquerque, NM, USA 87185
dsblair@sandia.gov
fmmccro@sandia.gov

Abstract:

The assurance of Safeguards Information is crucial to meet IAEA obligations. Information can be potentially at risk for alteration when it is generated, stored, transmitted, or manipulated (such as in a calculation). Where, when, and how information is assured can vary depending on where in the information lifecycle it exists. Often, information protection measures are not considered until after a system is architected and built or are only applied to a portion of the information system. This typically limits the effectiveness of information assurance, can increase the cost of assuring the information, and can reduce the trust in the information received. Designing information assurance into the architecture of a system can significantly reduce information vulnerability at an affordable cost while improving the trust of the information. This paper discusses safeguards information assurance by design and architectural approaches from a lifecycle perspective including potential tools that can be utilized to help define information assurance requirements and help validate the effectiveness of these requirements as the system transitions through the lifecycle. The tools discussed include risk management tools, architectural approaches, modeling approaches, and red teaming benefits.

Keywords: safeguards, information assurance, design, risk

1. Introduction

To support informed choices while working to optimize economic, operational, safety, security, and safeguard factors in the design of nuclear facilities, the International Atomic Energy Agency (IAEA) has been promoting Safeguards by Design (SBD) for more than 10 years. “Defined as the consideration of safeguards throughout the lifetime of the facility from preliminary conceptual design to decommissioning” [1] it encourages the consideration of continual integration of safeguards obligations throughout the facility lifecycle. A U.S. DOE National Laboratory project team developed a SBD framework that was dependent upon three pillars: requirements definition (for safeguards performance), design processes, and design toolkit. It was recognized that “successful implementation of SBD is a project management and coordination challenge,” articulating the need for continued integration between the key elements [2].

Similar to integration into the design process of objectives for safety [3] to reduce accidents and security to minimize the risk of malicious acts [4], SBD brings a systems-level perspective to the problem. However, most of the SBD open literature focuses on the integration of safeguards hardware into nuclear facilities and not the protection of digital assets, information, and data collection systems critical to safeguards systems. This paper will focus on approaches designed to address the need to protect information from compromise in these complex systems.

2. Safeguards Information Assurance by Design (SIAD)

IAEA safeguards are those technical measures used to independently verify that nuclear materials and activities are not diverted from peaceful purposes or misused. It is an essential component of the international nuclear security regime. The independent verification relies on a large volume of data and information from a variety of sources that is collected, stored, integrated, transmitted, and analyzed. The quality of conclusions and decisions that the IAEA can make is based on the timeliness, relevancy, and accuracy of data and information it collects. The timeliness detection goals are well understood and are determined based on nuclear material categories such as: one month for uneradicated direct use material, three months for irradiated direct use material, and one year for indirect use material when no additional protocol is in force [5]. Relevancy of information is determined by the IAEA based on objectives and conditions [6] . Whereas timeliness and relevancy are metrics used and defined by the goals of the IAEA, accuracy is fundamental to the quality of their conclusions and decisions.

Accuracy is commonly viewed for data as the quality or state of being correct. For physical measurements this is understood to be how close the results come to a true value and is typically addressed through calibration measures, traceable standards [7], chain of custody of samples, etc. Present in this definition is the underlying assumption that the instruments or data streams have not been modified by an adversary. There are also other characteristics that describe the data that need to be considered by the IAEA based on how the information will be used such as its confidentiality, integrity, or availability. The term that is often used to describe those measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation, is Information Assurance (IA) [8]. Integrating risk identification and assessment methods early in the design process to eliminate information compromise throughout the life of the system is information assurance by design (IAD). For Safeguards systems we will refer to this as Safeguards Information Assurance by Design (SIAD).

2.1. SIAD is a Lifecycle Challenge

It is never too early in the lifecycle of a system to begin thinking about IA. As early as the conceptualization phase, maintaining IA as a key system objective could influence what approaches and options are available to the IAEA (i.e. joint use equipment versus IAEA owned and operated). This could help eliminate wasting resources researching and developing approaches that could never provide the information confidence needed by the system.

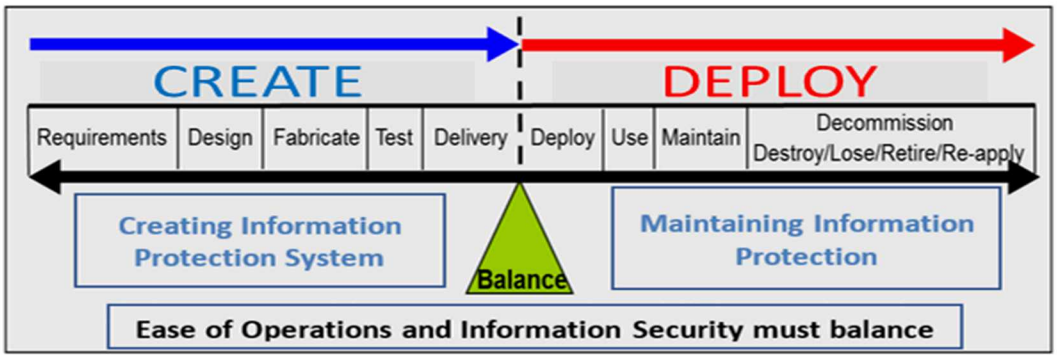

Figure 1 – Technology/system lifecycle with focus on information protection

As shown in Figure 1, the lifecycle of technology can be viewed as a series of discrete steps. Each step presents unique challenges and opportunities for the system or equipment to possess strong IA characteristics and features. During the Create Phase the system is designed and fabricated. This is the best time to establish and implement information security requirements due to the design flexibility of the systems and components. Effective communication of requirements with vendors and other stakeholders establishes the expectations that information security is a key element of the system. This is extremely important. From a vulnerability standpoint the Create Phase is a prime time for inserting birth defects or attack vectors so strong protections of information and supply chain should be used.

In Deploy phase, SIAD is tested against anticipated requirements based on intentional attacks or system failures. Being aware of the new attack vendors that can be introduced during the Use and Maintain stages through communications and system updates contributes to the overall system design. In the Deploy phase, upgrades and modifications to a facility that has not previously used a SIAD phase have the opportunity to initiate a SIAD process for the upgrades/modifications.

High security systems can be the most cumbersome to use with passwords, biometrics, processes and procedures designed with one end in mind: security for information and the system. Unfortunately, there is still a job that must be done and workers have been known to disable features or disregard rules if they find the security systems burdensome [9]. The balancing of requirements, costs, and performance of systems where IA is needed should be focused on throughout its lifecycle and is supported by SIAD.

2.2. Safeguards Information Risks

The types of risks that should be taken into consideration for safeguards information are implied in the pillars of IA and include but are not limited to:

- Interruption
- Alteration
- Substitution
- Theft

Understanding risk related to safeguards system failure is a key component of the SIAD concept. While there are many types of failures to the system that need to be evaluated, such as reliability of components and other non-malicious failure mechanisms, this paper primarily focuses on the intentional intervention into the safeguards system by an actor with malicious intent. This has significant implications in how risk is evaluated. Risk is generally defined as the product of Likelihood and Consequence (*Risk = Likelihood · Consequences*) with Likelihood generally treated as a probability function related to failure of a system or component. When dealing with an intentional act, the probabilistic nature of an event typically is considered 1.0 and, as such, the risk equation doesn't provide useful information. There have been many papers that have described Risk related to an intentional event and it is often described as Risk is the product of Threat, Vulnerability, and Consequences (*Risk = Threat · Vulnerability · Consequences*) [10]. In this representation, the earlier Likelihood variable is replaced with the product of Threat and Vulnerability. This representation assumes Threat and Vulnerability are independent variables but the relationship between them can be complex due to potential inter-dependencies. Wyss, et al., [11] discusses many of the complexities of determining malicious risk to information enterprise systems. Wyss introduces the concept of Difficulty to the risk determination process. Using Difficulty to execute an attack as a surrogate for Likelihood of an attack for an adversary, Wyss postulates the difficulty (work effort) can be approximated and provide some level of quantification for likelihood of an attack.

To adequately determine the risks from a malicious actor, there are several approaches and tools that can be applied to better address the malicious risk to a system and inform design requirements.

2.2.1. Threat Model

Threat models are an important part of any SIAD process as it is a key driver for the types of IA design features that need to be implemented into a system. A common approach used for designing a secure system is to bind the threat variable by creating a design basis threat (DBT). IAEA Nuclear Security Series 13 [12] encourages States to develop a DBT for protection of nuclear facilities and IAEA Nuclear Security Series 17 (NSS17) [13] further uses the DBT in guiding computer security for nuclear facility information systems. The State DBT's as well as IAEA processes can be used to create a set of adversary metrics for use by safeguards' designers in their threat model. For example, F. McCrory, et al., [14] combined the generic IDART™ [15] Threat Matrix with the NSS17's attacker profile to create a table on attacker profiles and reproduced it here.

Table 1 shows the NSS17 attacker profiles in the first column and the assigned the generic IDART™ threat model (GTM) level to each profile in column two. Columns three thru eleven combine the two sources' metrics with the result giving a more detailed set if metrics for potential adversary profiles. From this table, a determination of which adversary profiles the system is to be designed to be defended against can be made and the metrics used as inputs to the SIAD requirements.

Table 1 Potential NSS Attacker Profiles Adversary Threat Matrix *[14]*

		Commitment Category			Resources Category					
NSS Name	GTM #	Intensity	Stealth	Time	Technical Personnel	Computer Knowledge	Physical Security Knowledge	Nuclear Engineering Knowledge	Access	Motivation
Covert Agent	6	Medium	Medium	Weeks to Months	Ones	Medium	Medium	Medium	Medium	Theft of business information, technology secrets, personal information. Economic gain (information selling to competitors). Blackmail.
Disgruntled employee /user	6-	Low	Low	Weeks to Months	Ones	Medium	Medium	Medium	Medium	Revenge, havoc, chaos. Theft of business information. Embarrass employer/other employee. Degrade public image or confidence.
Recreational hacker	8	Low	Low	Days to Weeks	Ones	Low	Low	Low	Low	Fun, status. Target of opportunity. Exploitation of 'low hanging fruits'.
Militant opponent to nuclear power	3 to 7	Medium	Low	Months to Years	Tens	Medium	Medium	Medium	Low	Conviction of saving the world. Sway public opinion on specific issues. Impede business operations.
Disgruntled ex-employee /user	7+	Low	Low	Weeks to Months	Ones	Medium	Medium	Medium	Low	Revenge, havoc, chaos. Theft of business information. Embarrass employer/other employee. Degrade public image or confidence.
Organized Crime	4-5	Medium	Medium	Months to Years	Tens of Tens	Medium	Medium	Medium	Medium	Blackmail. Theft of nuclear material. Extortion (financial gain). Play upon financial and perception fears of business. Information for sale (technical, business or personal).
Nation State	1 or 2	High	High	Years to Decades	Hundreds	High	High	High	High	Intelligence collection. Building access points for later actions. Technology theft.
Terrorist	2 or 3	High	Medium	Months to Years	Tens of Tens	Medium	Medium	Medium	Medium	Intelligence collection. Building access points for later actions. Chaos. Revenge. Impact public opinion (fear).

2.2.2. System characteristics

If an adversary has knowledge of the information system, it enables them to tailor and focus their attacks on vulnerable elements. Control of system information is often an underappreciated aspect of IA and is a key component of the SIAD process. If an adversary has no information about the system, it is nearly impossible to craft a successful attack. Turner, et al., [16] discusses three essential elements that an adversary needs to plan a successful attack: Information, Access (Vulnerabilities), and Technology (Adversary Capabilities). This can be represented as a simplified Venn diagram, Figure 2. The overlap of the Venn diagram is where an adversary needs to get to be confident in a successful attack and can be considered the attack surface for implementing the attack. If information is limited as part of the SIAD, then the complexity of the work effort (difficulty) needed to achieve a successful attack increases and the risk of an attack decreases.

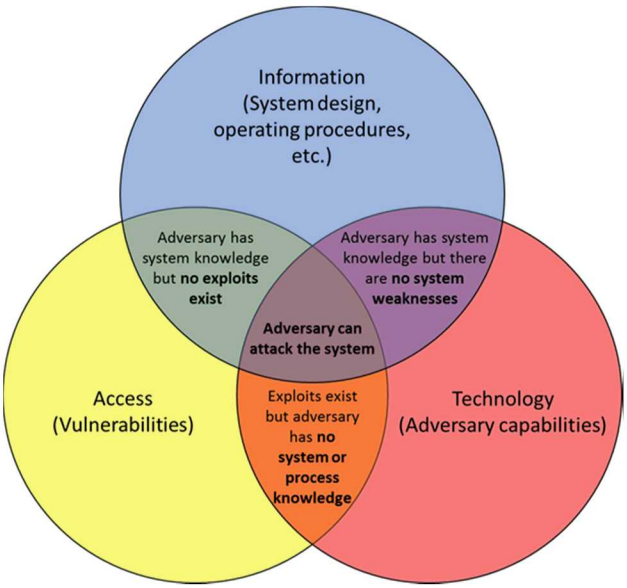

Figure 2 Elements Needed for a Successful Cyber Attack *[16]*

2.2.3. Vulnerabilities and Access

Vulnerabilities and Access (physical and logical) of IA systems is a widely studied area with multiple state generated documents on how to protect these systems. As such, this paper does not discuss the generalities of this related to SIAD.

3. SIAD Approaches, Methods, and Tools

Information assurance for IAEA Safeguards data and information is particularly challenging due to the limited community where the instruments are manufactured and deployed, increasing cyber skills of the adversary, growing reliance on digital systems, globalization of digital components and systems, and the growing safety and security responsibilities and concerns for plant operators.

3.1. Supply Chain Risk Management

Supply Chain Risk Management (SCRM) is a recognized critical element of any comprehensive cybersecurity systems [17] and has been addressed in detail by the authors [18]. The increased reliance on digital systems, subsystems, and components compounded with the increased functionality of hardware, complexity of software, and globalization of the digital supply chain has created a nexus of IA security concerns.

A particularly challenging aspect of securing the supply chain for IAEA technologies is the small number of equipment suppliers available and the unique equipment they deploy. Blind buys often are not an option for this community, equipment numbers are relatively limited, and they are expected to have long design life. These factors make IA particularly challenging and highlight the need for SIAD sharing information security requirements and objectives throughout the system lifecycle.

Creating a comprehensive SCRM program can be very cost intensive. A SCRM policy for safeguards should be created early in the SIAD process. Edwards [19] provides a high-level presentation on supply chain decision analytics and can be the basis for a SCRM program and includes a Decision Analytics Framework with the following attributes:

- Decision Analytics Framework
- Supply Chain Mapping
- Vulnerability & Mitigation Modeling
- Risk Assessment
- Optimization

3.2. Risk Management

Identifying, assessing, and controlling threats and vulnerabilities are a key part of any SIAD program and like SIAD should be addressed over the lifecycle of the safeguards systems. A risk management program, to address these threats and vulnerabilities, should evolve over time as threats advance and vulnerabilities become known. There are many risk management methods and frameworks that can be utilized with varying utility for information systems. The Electric Power Research Institute has published a technical assessment methodology [20] that provides a detailed method for assessing risk related to nuclear power plant critical digital assets. This method could be adapted to safeguards systems. Additionally, Clark, et al., [21] has published a paper on hazard and consequence analysis for digital systems that provides a risk method that leverages traditional Probabilistic Risk Assessments, Systems-Theoretic Process Analysis, and Fault Tree Analysis methods. These methods in conjunction with methods related to Table 1 provide some methodologies to support a rigorous risk management program.

3.3. Modeling and Simulation

Modeling and simulation (M&S) is used throughout engineering to provide insight to system design features, explore design space without physically building systems, evaluate various architectures to explore system resiliency to threats, perform optimization studies, explore impacts to current systems from modifications and upgrades, and many other purposes. As SIAD is a lifecycle problem, a Modeling framework that explores the M&S space from threat to consequence and recovery is needed.

3.3.1 Modeling Framework

A Modeling framework, that connects multiple types of Modeling domains, developed by Sandia National Laboratories to explore the impact of an event and the threat that could initiate it in the cyber and/or physical realms has been reported [22]. The framework, Integrated Cyber Physical Impact Analysis (ICPIA™), was first developed to explore cyber impact to critical infrastructures. This resulted from the many questions being asked regarding the possible impact of cyber events and the threats that could create particular consequences. This modeling framework covers the event from the threat capability needed to initiate the event and to recovery from the event.

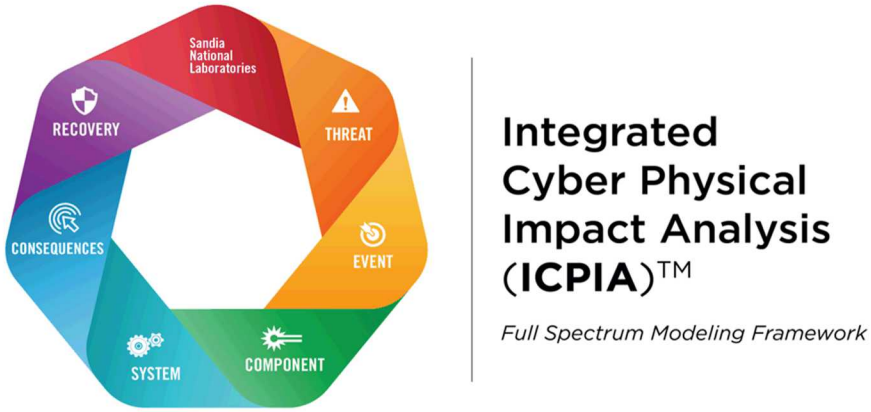

Figure 3 Integrated Cyber/Physical Impact Analysis Framework

A framework such as ICPIA™ can help a design process make architectural decisions and explore the impacts that various threats have on a system through their potential consequences.

Threat modeling, discussed in Section 2.2.1, is helpful in determining the types of vulnerabilities that the adversary could exploit and the resultant potential consequences (Event Model). For information systems this modeling of an exploit could have a physical or logical impact on a component within the system. This often requires its own component (sub-system) model (e.g. a field-programmable gate-array or programmable logic device). The exploited component behaviour would then result in a system response that would create a consequence of concern such as data interruption, alteration, substitution, theft, etc. After a consequence has been achieved, recovery from the consequence is another set of modeling tools.

For SIAD network modeling, there are many open source and for-purchase software packages that can be used to develop a relatively high-fidelity model of the network and often the vendors of various components, such as routers or switches, will provide a model of their component. Models of various operating systems can often be utilized directly using the software of concern or can be modelled with various fidelity for many end users within the overall model. For operational technology systems (OT) (control systems), modeling tools are relatively limited. Additionally, modeling of IT and OT systems impact on physical systems is even limited further. SCEPTRE [23] [24] is a modeling tool that couples digital systems to physical environments. Tools like SCEPTRE are useful in the transition modeling between a cyber event and an actual physical impact.

3.4. Architectural Approaches

Utilizing the SIAD approach for information systems could result in reduction of the overall lifecycle cost of implementing safeguards in a nuclear facility.

Understanding the likely threat that a system could face supports in the identification of threat vectors into the system. This then allows for designing an architecture not susceptible to the threat vector, identifying type and location of intrusion sensors needed to promptly identify when compromise occurs, developing redundant or diverse ways of providing the needed information should one channel be compromised, or other approaches based on the threats and their capabilities that are identified. Evaluation of the necessity to isolate the safeguards information system from business networks and/or internet potentially can have a significant impact to the overall security of the system. A system isolated from business networks and the internet remove certain classes of attack but can still be vulnerable from other classes of attacks such as the supply chain or insiders.

Designing the safeguards IA system in a tiered manner so that the most critical information, determined through risk-informed analysis and M&S, has layered protections, often called defense-in-depth. The IAEA recently published NP-T-2.11 [25] which focuses on architectural approaches for nuclear power plants and has many best practices that can benefit SIAD. These include discussions around defense-in-depth, independence, categorization of system functions, computer security zones, elimination of unnecessary complexity, etc.

3.5. Red Teaming

Red teaming has many definitions. For the purposes of this paper, we use the Sandia National Laboratories definition from their Information Design Assurance Red Teaming (IDART™) [15] method. This states that red teaming is an “authorized, adversary-based assessment for defensive purposes.” IDART™ defines eight different types of red teaming: design assurance, hypothesis testing, benchmarking, behavioral red teaming, gaming, operational red teaming, penetration testing, and analytical red teaming. For SIAD, we will briefly discuss the most applicable red teaming types: design assurance, analytical, and penetration testing. It should be recognized that the other types of red teaming have potential value to SIAD depending on the questions that need to be answered.

3.5.1 Design Assurance Red Teaming

Design Assurance red teaming is conducted early in the lifecycle to provide an adversary’s perspective. It is typically applied as soon as a preliminary architecture of the system is defined. It is useful if the design basis threat or the threat actor is defined to ensure that the red team only simulates the adversary capability of concern. If the adversary level emulated is too high, then the red team may provide unnecessary suggestions that would increase the cost of the system. If the adversary is defined as too low of a level, the red team might not provide enough feedback and potentially leave the system inadequately protected. Design Assurance red teaming should be performed during lifecycle processes that include development of designs.

3.5.2 Analytical Red Teaming

Analytical red teaming performs a detailed adversary-based assessment of the system and uses threat-based M&S tools to help identify how an attacker would approach exploiting the safeguards system. Typically, the red team generates attack graphs that can be analysed for their difficulty in exploitation generating risk-informed information identifying the weakest components with an architecture. The red

team starts with the consequences of concerns on the right side of the graph and access points on the left side of the graphs. Working with the system designers and subject matter experts, attack paths between access points are identified that lead to a consequence of concern. The various attack paths are then rank ordered based on execution difficulty, providing critical information to designers. Often multiple attack paths go through a single node that once identified can be rearchitected to remove that series of attack paths. This method can result in large numbers of attack paths depending on the complexity of the system. This method should also be performed in the design stage before the final design is set.

3.5.3 Penetration Red Teaming

Penetration red teaming is performed once a design has been built, but before fielding if possible. Penetration testing uses a host of tools that looks for vulnerabilities within an information system and then attempts to exploit those vulnerabilities. Penetration testing should be performed periodically throughout the lifecycle on a system since new vulnerabilities to various IT systems are continuously being discovered that might be exploited by an adversary or the design basis threat could evolve.

4. Conclusions

Designing information assurance into the architecture of a safeguards system can significantly reduce information vulnerability cost effectively while improving the trust of the information. SIAD is the integration of risk identification and assessment methods early in the design process to eliminate information compromise throughout the life of the safeguards systems. Some approaches used in physical security can be adopted or leveraged for cyber security but there are critical differences when evaluating risk. Due to the evolving capabilities of adversaries and insertion of possible vulnerabilities throughout its lifecycle, continual risk identification and assessment methods for information systems is required to ensure information is not compromised.

It is important to remember:

- The information system present vulnerabilities and risks throughout its lifecycle. These do not end when design is finalized, built, deployed or even decommissioned.
- It is necessary to control distribution of details regarding information system operations or vulnerabilities. Knowledge of the system arms an adversary.
- Adversaries evolve over time and continual reexamination of the information system vulnerabilities and risks is critical to ensuring its dependable performance.
- There is no such thing as a standalone or isolated system. Protection is needed for all sensitive digital assets with a graded approach applied.

5. Acknowledgements

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

6. References

[1] International Atomic Energy Agency, «IAEA Nuclear Energy Series, NP-T-2.8, International Safeguards in Nuclear Facility Design and Constructionq,» IAEA, Vienna, 2013.

[2] T. Bjornard, R. Bean, P. C. Durst, J. Hockert e J. Morgan, «Implementing Safeguards-by-Design, INL/EXT-09-17085,» Idaho National Laboratory, Idah Falls, 2010.

[3] DOE-STD-1189-2016, «Integration of Safety into the Design Process,» U.S. DOE AU Office of Environment, Health, Safety and Security, Washington, 2016.

[4] C. J. S. J. a. C. S. M.K. Snell, «Security-by-Design Handbook,» SAND2013-0038, Sandia National Laboratories, 2013.

[5] IAEA, «IAEA Safeguards Glossary, 2001 Edition, International Nuclear Verification Series No. 3,» International Atomic Energy Agency, Vienna, 2002.

[6] IAEA, «Safeguards Implementation Practices Guide on Provision of Information to the IAEA, IAEA Services Series 33,» International Atomic Energy Agency, Vienna, 2016.

[7] Chemicool Dictionary, «Definition of Accuracy,» 2017. [Online]. Available: https://www.chemicool.com/definition/accuracy.html. [Consultato il giorno 23 04 2019].

[8] National Institute of Standards and Technology, U.S. Department of Commerce, «Information Technology Laboratory, Computer Security Resource Center (CSRC), Glossary, information assurance (IA),» [Online]. Available: https://csrc.nist.gov/glossary/term/information-assurance. [Consultato il giorno 23 04 2019].

[9] Kaspersky Lab Daily, «The Human Factor in IT Security: How Employees ar Making Businesses Vulnerable from Within,» Kazpersky La, 2019. [Online]. Available: https://www.kaspersky.com/blog/the-human-factor-in-it-security/. [Consultato il giorno 05 05 2019].

[10] U.S. Department of Homeland Security Risk Steering Committee, «Risk Lexicon,» U.S Department of Homeland Secuity, Washington, D.C., September 2008.

[11] G. Wyss e et al., «A Method for Risk-Infromed Management of Enterprise Security (RIMES), SAND2013-9218,» Sandia National Laboratories, Albuquerque, 2013.

[12] International Atomic Energy Agency, «IAEA Nuclear Security Seeries No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision),» IAEA, Vienna, 2011.

[13] International Atomic Energy Agency, «IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities,» IAEA, Vienna, 2011.

[14] F. Mitch McCrory, R. Parks e R. Hutchinson, «An Adversary's View of Your Digital System,» in *IAEA-CN-228-54*, Vienna, 2015.

[15] Sandia National Laboratories, «Information Design Assurance Red Team,» [Online]. Available: https://idart.sandia.gov/. [Consultato il giorno 02 05 2019].

[16] P. L. Turner, F. M. McCrory e L. A. Dawson, «Nuclear Power Plant Instrumentation and Control Cyber Security High Value Access Points Leading to Relational Common Cause Failure,» in *10th International Topical Meeting on Nuclear Power Plant Instrumentation, Control, and Human Machine Interface Technologies*, San Francisco, 2017.

[17] S. R. Chabinsky, «Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line,» *Journal of National Security Law & Policy,* vol. 4, p. 27, 2010.

[18] F. M. McCrory, G. K. Kao e D. S. Blair, «Supply Chain Risk Management: The Challenge in a Digital World,,» in *International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange* , Vienna, 2015.

[19] N. J. Edwards, «Supply Chain Decision Analytics: Application & Case Study for Critical Infrastructure Security,» 2016. [Online]. Available: https://www.osti.gov/servlets/purl/1347081. [Consultato il giorno 02 05 2019].

[20] Electric Power Research Institute, «Cyber Security Technical Assessment Methodology: Risk Informed Exploit Sequence Identification and Mitigation, Revision 1,» EPRI, Charlotte, 2018.

[21] A. J. Clark, A. D. Williams, A. Muna e M. Gibson, «Hazard and Consequence Analysis for Digital Systems - A New Approach to Risk Analysis in the Digital Era for Nuclear Power Plants,» in *Transactions of the American Nuclear Society, Vol. 119*, Orlando, 2018.

[22] L. A. Dawson e F. M. McCrory, «ICPIA and Red Teaming,» in *ESARDA Symposium 2019, 41st Annual Meeting*, Stresa, 2019.

[23] Sandia National Laboratories, «SCEPTRE,» SNL, 2019. [Online]. Available: https://www.osti.gov/servlets/purl/1376989.

[24] Sandia National Laboratories, «SCEPTRE Demonstration,» Vimeo, https://vimeo.com/178492617, Albuquerque, 2017.

[25] International Atomic Energy Agency, «Approaches for Overall Instrumentation and Control architectures of Nuclear Power Plants, IAEA Nuclear Energy Series, NP-T-2.11,» IAEA, Vienna, 2018.