SAND2019-14148C

APPLICATION OF A SIMPLIFIED FIVE STEP PROCESS TO IDENTIFY AND CLASSIFY SENSITIVE DIGITAL ASSETS

Michael T. Rowland
Sandia National Laboratories
Albuquerque, New Mexico, United States of America
Email: mtrowla@sandia.gov

John Sladek
Canadian Nuclear Safety Commission
Ottawa, Canada

Michael StJohn-Green
Mike StJohn-Green Consulting Ltd
Cheltenham, United Kingdom

Robert Anderson
Idaho National Laboratory
Idaho Falls, Idaho, United States of America

Abstract

The identification of digital assets and their classification (i.e. assignment to security levels) within computer security programmes at nuclear facilities has historically been a complex process. The current approaches use a system or asset-centric approach with the aim of applying cyber-security retro-actively. An example of such an approach is provided in US NRC Reg Guide 5.71 whereby Licensee systems are classified as critical systems if they have meet one or more of the following criteria: (i) Performs Safety, Security or Emergency Preparedness (SSEP) functions; (ii) Affects critical systems, functions or pathways; or (iii) Supports critical systems.

This paper outlines a simplified approach for identification and classification of digital assets, and provides opportunities to identify strategic improvements and efficiencies in achieving the computer security goals. The paper outlines a 5-step process: (1) identify and enumerate the nuclear security goals; (2) identify the functions that provide, support, or assist in realizing the security goals; (3) identify the digital assets (or systems) that perform or support these functions; (4) assign a computer security level to the digital assets upon the potential consequence as well as the level of support the digital asset provides (i.e. directly performs function, supports function, or indirectly supporting function/auxiliary); and (5) evaluate the effects of compromise using an adversary profile and characterization.

No matter how capable the team performing the analysis, or how accurate the results are, compromise of digital assets can lead to indeterminate effects. Indeterminate effects reduce the confidence in the functional analysis that dominates elements (1) to (4), and necessitates element (5). The process for element (5) is to bound the potential for compromise resulting in indeterminate effects to those that are bound to an adversary profile and to a credible scenario. This process will never be as accurate as the results of analysis of (1) to (4) since both the scope bounding the adversary and the credible scenarios will not have high confidence, but when used to verify element (4) it is effective.

1. INTRODUCTION

Protection of computer-based systems (including digital I&C systems) is recommended by the Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [3], paragraph 4.10, which states that “computer based systems used for physical protection, nuclear safety and nuclear material accountancy and control should be protected against compromise (e.g. cyber-attack, manipulation or falsification) consistent with the threat assessment or design basis threat”. This same requirement is often used as a basis for national computer security regulation for nuclear facilities.

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.

The identification and classification of sensitive digital assets (SDAs) is a key process to ensure that security requirements are appropriately specified and imposed as well as ensuring that effective measures are put in place to protect either the significant function and/or the sensitive information.

This process demands as its primary objective that the inherent value of an SDA is captured completely. This necessitates the owner/operator of the SDA to undertake significant effort to identify attributes and elements that contribute to the value of the SDA.

Furthermore, cyber-attacks have provided adversaries with a potential capability to place I&C systems in indeterminate states, where the function of the system can no longer be guaranteed [2]. This, coupled with the potential that an owner/operator may not correctly determine the value the SDA (i.e. the adversary might be able to discover its true value; arbitrage), results in a need for a final adversary-focused step to confirm or raise confidence in the determined SDA value.

Computer security levels will be used to capture the 'value' of the SDA [3].

2. CURRENT PRACTICES

2.1. IAEA Classification of Safety Functions

For safety, IAEA NST047 assigns facility functions to security levels using the safety consequence arising from the compromise of the facility function as the prime consideration. Facility functions differ from system or component functions as facility functions exist independently from the implementation. The significance of the facility function is the primary consideration in the application of a graded approach using the concept of security levels. NST047 describes the relationship between facility functions, security levels and systems as shown in FIG 3. This results in systems having safety consequence to be assigned to security levels between one (highest) and three.

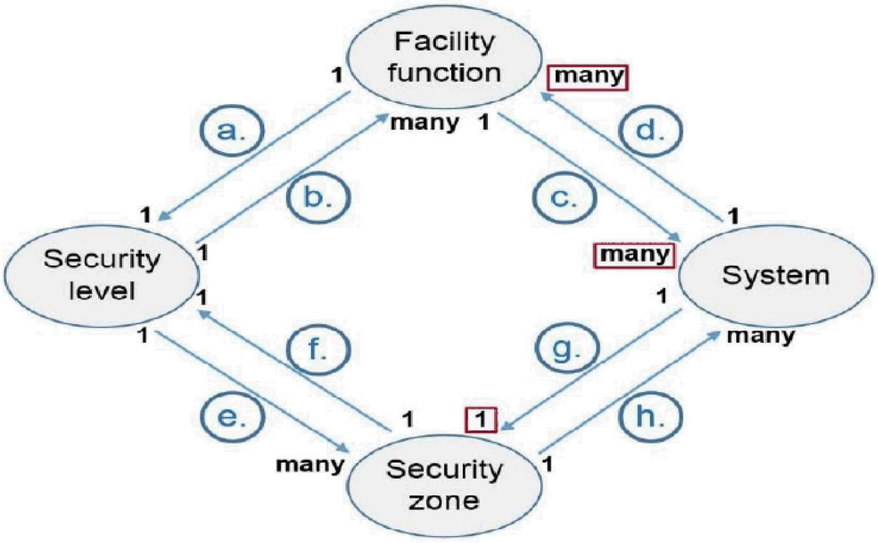


Fig. 3 – Relationships between Computer Security Concepts [3]

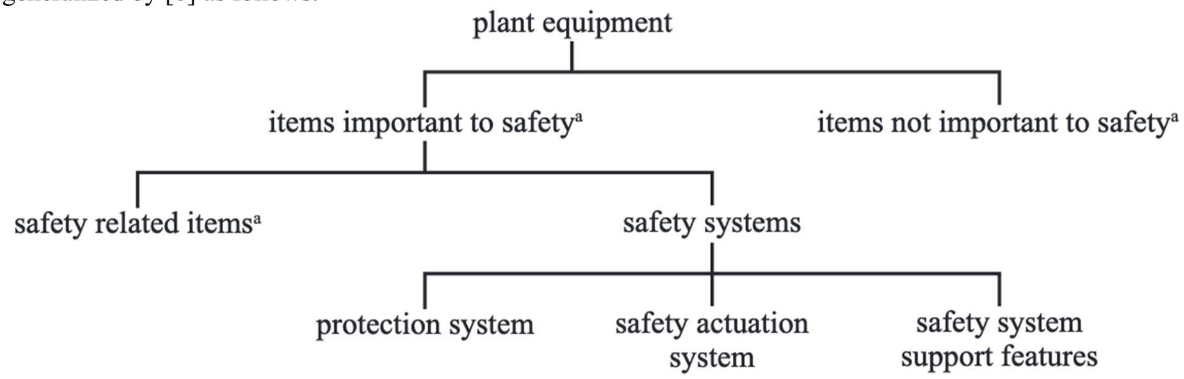
For Nuclear I&C systems, a mature process is used to categorize safety functions and classify safety systems. I&C systems important to safety are identified on the basis of their necessary I&C safety functions and the definition of systems that perform certain combinations of these functions [4]. The systems important to safety are based on the following fundamental safety functions that are required for all plant states [5]:

- Control of reactivity;
- Removal of heat from the reactor and from the fuel store;
- Confinement of radioactive materials, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

Para 5.34 of [5] specifies the method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, with due account taken of factors such as:

(a) The safety function(s) to be performed by the item.
(b) The consequences of failure to perform a safety function.
(c) The frequency with which the item will be called upon to perform a safety function
(d) The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function

The evaluation of the function first is a critical element in determining the safety classification. This approach is generalized by [6] as follows:



[a] In this context, an 'item' is a *structure, system or component.*

Fig. 1 Plant Equipment in Terms of safety function [6]

Current, international consensus categorizes functions of Safety Systems as Category A (with minor exemptions), while those of important to safety are categories B and C. Based upon these categories correspond to system classes as shown in the table below.

Categories of I&C Functions important to safety			Corresponding classes of I&C systems important to safety
A	(B)	(C)	1
	B	(C)	2
		C	3

Table 1: Correlation between classes of I&C systems and Categories of I&C functions [7][1]

The categorization of I&C control functions and classification of systems have been captured in the Level 1 international standard IEC 61513:2011 [7], and further detailed in the Level 2 international standard IEC 61226:2009 [8]. The resulting classification then determines relevant design criteria and is applicable to all the information and command functions and the instrumentation and control systems and equipment that provide those functions [8].

The flow chart from [9] below highlights the overall approach for categorization and classification. This approach mirrors strongly with the process for SDAs.

[1] Parenthesis indicates that the category can be elevated to a higher corresponding class of I&C system, but this is not mandatory.

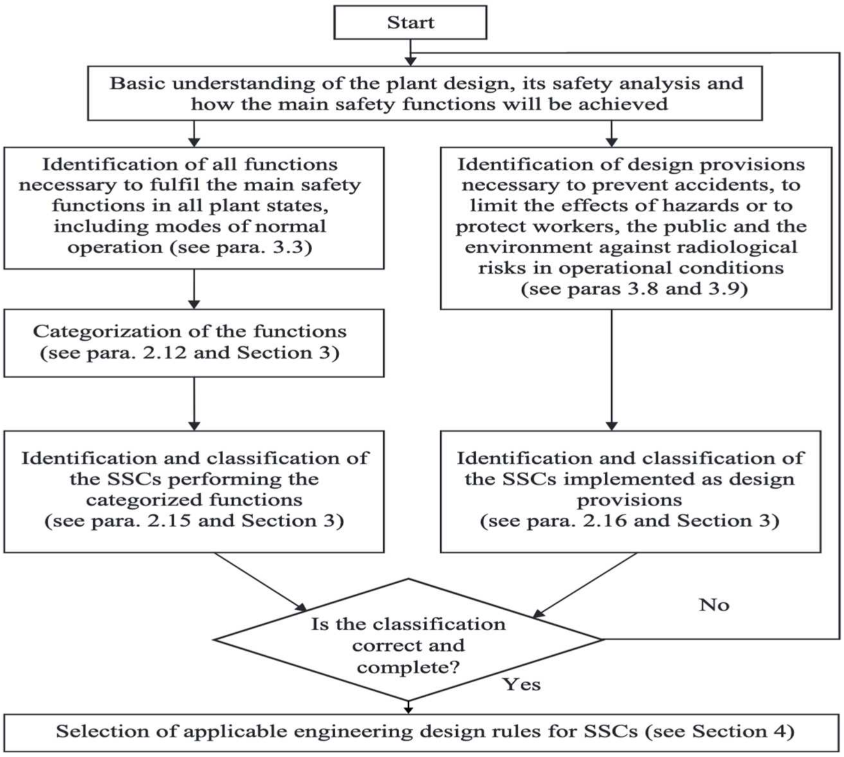

Start
Basic understanding of the plant design, its safety analysis and how the main safety functions will be achieved
Identification of all functions necessary to fulfil the main safety functions in all plant states, including modes of normal operation (see para. 3.3)
Identification of design provisions necessary to prevent accidents, to limit the effects of hazards or to protect workers, the public and the environment against radiological risks in operational conditions (see paras 3.8 and 3.9)
Categorization of the functions (see para. 2.12 and Section 3)
Identification and classification of the SSCs performing the categorized functions (see para. 2.15 and Section 3)
Identification and classification of the SSCs implemented as design provisions (see para. 2.16 and Section 3)
Is the classification correct and complete?
No
Yes
Selection of applicable engineering design rules for SSCs (see Section 4)

Fig. 2 Flow chart indicating the classification process [9]

Safety outlines key attributes such as (1) function, (2) consequence of failure, (3) frequency of performance of the function, and (4) time constraints to perform the function. This fails to meet security demands due to not considering the effects of compromise on the system function [2] of indeterminate states or unexpected behaviours or actions (e.g. loss of control) or malicious acts that impede actions taken in response to postulated initiating events (e.g. loss of view). This demands additional analysis, tools, and procedures to ensure these demands are accommodated.

2.2. Use of Safety Categorization to inform the assignment of Security Levels

2.2.1. IEC 62645 [10]

The IEC approach to assign security levels[2] follows strongly with the Safety Classification, but allows for an adjustment based on other factors. The categorization of function for safety is used as a baseline to establish a minimum security degree and the adjustment would allow for an upwards (more stringent) increase in Security Degree (generally equivalent to the IAEA computer security level concept). For example, a Category C/Class 3 system would be assigned a minimum security degree of ‘3’ but could be revised upwards to security degree ‘2’ or ‘1’.

The IEC standard however does not extend past I&C or Electrical Systems (leaving out Emergency Preparedness (EP), Nuclear Material Accounting and Control (NMAC), and Physical Protection Systems (PPS)), and possibly other systems based on the competency of the assessor, and the security culture of the organization.

2.2.2. Canadian Approach, CSA N290.7 [11]

The Canadian approach is captured within Canadian Standards Association CSA N290.7:2014 *Cyber security for nuclear power plants and small reactor facilities*. This follows strongly on safety as well, but does include EP and PPS, but not NMAC. Cyber Essential Assets (CEAs) are the Canadian equivalent of SDAs and are assigned a significance (i.e. high, moderate, low) based on safety categorization using a similar process to IEC 62645 [10]. However, CEAs associated with PPS are prescriptively assigned a moderate significance, while EP

[2] The IEC uses the term ‘Security Degrees’. This is equivalent to ‘Security Levels’

is handled separately and mostly assigned a low significance. This prescriptive approach to a single level once may introduce strategic weaknesses and deficiencies in the computer security programme of the owner/operator.

2.2.3. UK approach

The UK approach strongly aligns with that used for safety categorization with 3 elements that may raise the level of the SDA or system. These are:

- System provides main displays within the main control room;
- System has a large network;
- System if compromised may result in an extended plant shutdown.

If a category B system has any of these elements, the system is considered a 'significant category B' system and is assessed to meet the category A requirements [12]. This approach considers the potential for compromise (greater opportunity for systems with large networks) and consequences of loss of view (displays in main control room) or loss of control (extended plant shutdown)[3]. This approach is strongly based on the IEC 62645 approach and has similar limitations with additional guidance for category B functions.

2.3. IAEA Security Functions

IAEA NST047 uses the consequence of unauthorized removal and sabotage as the primary consideration in assigning facility security functions to computer security levels. Since theft of material cannot be accomplished solely by cyber attack and must also involve physical access to the material, this results in physical security systems being to the second highest security level (level 2).

3. SIMPLIFIED APPROACH SECURE BY DESIGN ELEMENTS

This simplified approach is outlined through a 5-step process: (1) identify and enumerate the nuclear security goals; (2) identify the functions that provide, support, or assist in realizing the security goals; (3) identify the digital assets (or systems) that perform or support these functions; (4) assign a computer security level to the digital assets upon the potential consequence as well as the level of support the digital asset provides (i.e. directly performs function, supports function, or indirectly supporting function/auxiliary); and (5) evaluate the effects of compromise using an adversary profile and characterization.

Each process step will be outlined below and then illustrated with three case examples.

3.1. Identify and enumerate the nuclear security goals

The nuclear security goals for a nuclear power plant at a high level are:

- *Physical Security* – protect against the unauthorized removal of nuclear material
- *Physical Security* – protect against sabotage resulting in unacceptable radiological consequences (URC)
- *Information Security* – protect against the unauthorized disclosure, alteration, modification, destruction or denial or use of sensitive information
- *Safety* – Control of reactivity;
- *Safety* – Removal of heat from the reactor and from the fuel store;
- *Safety* – Confinement of radioactive materials, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

These goals are graded based upon the associated consequences. For security, IAEA NSS No. 13 [13] provides graded requirements for protection against unauthorized removal and sabotage. For information security, IAEA NSS 23-G [14] provides a graded requirements for protection of sensitive information. For safety, SSG-

[3] The IAEA does not consider 'plant shutdown' as a consensus regulatory concern for safety, but Member States can determine other criteria upon which to regulate.

30 [9] and the aforementioned IEC standards [7][8] provide a categorization that may be used to impose graded requirements for systems providing these functions.

3.2. Identify the digital assets (or systems) that perform or support these functions

The next step is to identify the digital assets that perform or support these functions. In new designs, the assets, configuration, and architecture can be restricted to ensure that security requirements are met. However, in legacy designs, the assets are already in service and security needs to be retroactively applied.

The identification of assets must follow the approach outlined in the System Computer Security Risk Management Process detailed within para 5.5 of [3]. This approach analyses necessary information flows that exist within the implementation of the system to determine the 'connectivity[4]' and 'trust' of assets. Connected, trusted assets are assigned the same level as the function.

3.3. Assign a computer security level to the digital assets upon the potential consequence

This step looks at the potential consequences of mal-operation of the digital assets. The objective of this step is to determine the consequences on the function which are listed in para 2.21 of [13]. To bound the consequences, a graded effort to identify and analyze potential indeterminate states and unexpected behaviours or actions needs to be undertaken.

This should not consider the adversary but be taken from a designer perspective to enumerate specific asset states that would fail, degrade, alter, or provide opportunity to destroy or impact other functions. It is critical theat the designer enumerate fully all credible unexpected behaviours or actions and potential altered states (i.e. bound potential or likely indeterminate states).

3.4. Evaluate the effects of compromise using an adversary profile and characterization

This step is to raise confidence in the evaluation by applying a separate independent process that evaluates actions and sequences of the adversary but the specific focus is directed towards confirmation of the security level arrived to step 4. If an equivalent security level is not arrived to, then the most conservative security level should be assigned to ensure appropriate protection of the function. This step can only raise the security level (i.e. increase requirements) and not lower them.

4. CASE EXAMPLES

For all case examples below, Step 1 is captured in a sample subset of security goals in section 3.1 above.

4.1. Case Example 1: Safety Function – Control of Reactivity – Control of neutron flux during normal operation within the core via increase or subtraction of neutron absorption capability

4.1.1. Step 2

The security goal is *Safety – control of reactivity*; while the function being identified is the control of neutron flux within the reactor core during normal operation via addition or subtraction of neutron absorption of capability. This can be completed many ways (1) control rods, in most design; (2) light water in CANDU designs; or other options. The implementation elements will be detailed below.

For this step, the function is analyzed similarly to [8] and [9] which considers:

(a) The consequences of failure to perform a safety function.
(b) The frequency with which the item will be called upon to perform a safety function
(c) The significance of the contribution of the function to the [security goal]

[4] Assets are considered connected if there is any mandatory periodic information flow between them with no technical control measure in place to restrict or control this flow of information.

This results in a categorization of the safety function, would be Category B, as the consequences of failure to perform the function would result in transition from normal operation to abnormal operation. The function is required to reach and maintain a safe state during normal operation. Using a conservative approach, the failure to reach and maintain a safe state is high (i.e. unsafe reactivity) and therefore, using table 1 of [9], the safety category assigned is 2. This would imply an initial security level of '2'

4.1.2. Step 3

The function was assigned security Level 2 from step 2 of the approach. This step needs to consider the implementation of the function via digital systems. For example, in a system that uses both light water and control rods (graphite) to absorb neutrons. In a hypothetical system, containing a single network to control both the addition/removal of light water or control rods, consists of 'x' assets. It is assumed that there is one controller, one network, and a number of sensors and actuators (all digital).

All 'x' assets would then be assigned Security Level 2.

4.1.3. Step 4

The 'x' assets assigned security level 2 will now be analysed to ensure that the requirements will lead to the appropriately secure state. Based on the example, the Supervisory control is the asset that if mal-operated could lead to failure to reach or maintain a safe state. However, this system is not accredited for reaching a controlled states after anticipated operational occurrences or after design basis accidents. Therefore, the grouping of all 'x' assets within a single zone assigned to the security level 2 is appropriate at this step.

Nevertheless, the constraint of this function needs to be understood and documented to ensure that the correct requirements are specified and enforced.

4.1.4. Step 5

The output of step 4, was to assign all 'x' assets to security level 2. However, given certain adversary capabilities, it is likely that large networks provide greater opportunity for them to access sensitive digital assets and affect their significant function. Additionally, large networks may use commercial of the shelf equipment or network communication protocols or services that have publicly known and critical vulnerabilities that reduce the level of effort required on the adversary to exploit these devices. These attributes would result in not only an increase in opportunity, but also an increase in the probability of success for an adversary that was able to access these devices or network.

Given the potential for indeterminate states (e.g. mal-operation) [2] resulting in amplification of the severity of consequences associated with failure to perform the safety function, or a credible scenario that the adversary can disable the Category A systems or degrade them to prevent them from recognizing certain conditions (e.g. mal-operation of the Category B system; 'x' assets); or become aware of latent design deficiencies not considered or known in step 4. This would necessitate, based on conservative decision making, in an increase of the security level from 2 to 1.

This assignment aligns with the UK ONR approach, with the 'significant category B' being an example of increasing the security requirements above that considered using safety assessment alone.

4.2. Case Example 2: Information Security - Enforcement of access controls for read and write operations across a zone boundary to protect integrity of sensitive information within a Biba trust model.

4.2.1. Step 2

The security goal of a Zone Boundary Technical Control Measure such as a Firewall (e.g. Security Gateway/Appliance), is *Information Security* – protect against the unauthorized disclosure, alteration, modification, destruction or denial or use of sensitive information.

Just as in Safety, which mandates consideration of the function with respect to plant state, the information security goal must consider the security level (sensitivity of information; trust model). In this case, the function is enforce access control rules for read and write operations across the boundary to protect the integrity of sensitive information of SDAs within the computer security zone being protected.

The failure to enforce access controls could result in the compromise of SDAs within the zone, but it is important to consider that the boundary technical control measure only gains significance based on the assets that are within the zone.

This function is a supportive function whose significance is implied based upon the information being protected. Functions providing decoupling of zones must be considered separately from other functions that can exist at a single level.

In this example, the function will provide boundary protection (i.e. decoupling) between zones containing assets at security level 2 and security level 3. This function would be initially assigned a security level of 2/3. It is critical that the assignment to a security level considers the functions/assets that are being protected. For example, a decoupling of a zone containing zero assets would result in no security level being assigned to this boundary protection function.

4.2.2. Step 3

The function of the enforcement of access controls at the level 2/3 boundary can be most readily implemented via one or more firewalls. However, if implemented by more than one firewall, it would be important to ensure that an equivalent level of protection is provided.

In this example, all firewalls would be assigned a level 2/3, the side of the firewall that connects to the protected area is level 2, with the outward facing being assigned level 3. Any privileged access would also be assigned level 2. The access controls detailed in NSS 17 [6] recommended for communications across a level 2/3 zone boundary are for write down, with limited handshaking allowed (e.g. TCP/IP). If the Firewall failed to provide the decoupling, the security requirements would not be met.

The decoupling assets (Firewall(s)) would therefore be assigned to security level '2'. But this does not take into account, other functions that may be assigned to the asset such as zone access control administration and interface with unprotected side.

4.2.3. Step 4

The one or more firewalls, that provide for decoupling at the boundary for zones assigned security level 2/3 are assigned security level 2 (based on the inside/protected side; administration) and level 3 (outside). However, the implementation and configuration will likely require remote connectivity and 'write-access' from the remote location to several level 2 functions.

Failure or misconfiguration of these firewalls could degrade or alter the function thereby exposing the protected digital assets to compromise. However, this is a pre-cursor or support event, and although having significance, is not accredited with a design basis function that would result in failure to reach a secure or safe state given other malicious actions that must be directed against those SDAs that perform safety or security functions and deliver either a Safety or Security goal.

However, this step illustrates why technical control measures demand specific requirements that impose different measures. For example, the access control rules for protection of Safety SDAs are based upon the Biba trust model, while the protection of the confidentiality of the configuration of the firewall needs to be based upon the Bell-LaPadula model (with separation of duties/Brewer Nash also to be considered).

In this example, the firewall could exist (or have) three distinct levels based on processes (1) '2' - for the protected zone, inferred from protected assets; (2) '3' or higher - for interface with the unprotected zone; and (3) '2' for the administration of the asset (inferred from (1)).

4.2.4. Step 5

The output of step 4, resulted in three security level assignments based upon implementation of the control. However, an adversary could compromise the administrative console or a specific vendor (supply chain attack) to make ineffective the boundary protections. However, this degrades defence in depth because of the loss of independence, but does not degrade the ability of the SDAs to provide the function.

This step is therefore important to reinforce the demand for segregation of duties, but also the need for independence and diversity for boundary controls.

Also, critical is that technical control measures adopt their own configuration/QA practices that are complementary to the assets that they protect but are not identical. The need for agile deployment of countermeasures is necessary to adapt to ever-changing adversary TTP.

The requirements for the security levels and management are further refined by this step, but in this example, the security levels remain unchanged from step 4. This is based on the attribute that no credible scenario exists whereby the decoupling assets (i.e. Firewall(s)) can directly[5] lead to an impact on a Safety or Security goal. Additionally, it cannot directly impact the information security goal as the Firewall is not an SDA so long as it does not store, process, control or transmit sensitive information[6].

4.3. Case Example 3: Security – Protect against unauthorized removal of categorized nuclear material via control of access to inner areas

4.3.1. Step 2

The security goal is *Security – unauthorized removal*; while the function being identified is the control of access to inner areas. This requires (1) identifying authorized personnel; (2) authentication of identity; and (3) provision of access. This is only one function that would be part of an integrated physical protection system that provides prevent, detection, delay, and response functions.

The function does not detect malicious acts by insiders, but minimizes the number of potential malicious actors. In this instance the analysis is similar to that in Case Example 1, which would imply an assignment of Security Level 2 based on the determination that the function is required to reach and maintain a secure state and a failure to perform the function would be high, but it is not protective (i.e. detect, delay, response) and therefore simply maintains a secure state. The security level assigned is Level 2.

4.3.2. Step 3

Contemporary security designs apply a high degree of integration into all functions, including detection. Therefore, most PPS designs utilize a single ‘flat’ network to provide all functions. This results in a single zone assigned security level 2 encompassing hundreds of assets.

It becomes clear that a graded approach to provision of computer security to protect the functions is not possible, and without a gradation of requirements, an implementation of defence in depth becomes difficult. Based upon this example, all PPS assets would be assigned security level 2 based upon association with this function.

4.3.3. Step 4

Due to the current designs of PPS, the integrated flat network, would imply that mal-operation of access control function would degraded or alter the detection function. para 2.42 of [3] identifies ‘intrusion detection (including assessment) at the critical detection point’ as a function important to security.

It is then conceivable that mal-operation of access control networks having direct trusted access to assets providing intrusion detection would result in failure to reach, maintain, or return to a secure state. This would result in a high likelihood that the malicious act would be completed prior to interception by response forces.

Given that intrusion detection protects against unauthorized removal and sabotage especially against insiders (i.e. undetected access to inner areas or vital areas), it would be prudent to assign Security Level 1 to the entire PPS to be coherent with Safety processes.

[5] ‘directly’ implies that no additional step or action is to be completed by the adversary before the consequences of unauthorized removal of nuclear material or sabotage resulting in unacceptable radiological consequences is achieved.

[6] Definition of sensitive information assets is from IAEA NSS 20 [15]; the firewall is likely to have information that has importance for security, but if care is taken to compartmentalize information, as well as to implement independent and diverse controls within the overall DCSA, the consequences will not solely or directly compromise of nuclear security.

4.3.4. *Step 5*

The output of step 4, resulted in assignment of security level 1 to all PPS SDAs. This result will lead to fatigue of the computer security resources demanded to secure the assets to the highest level. This step therefore needs to consider and prioritize requirements to transition to a segmented architecture that is function based.

The segmentation would need to iteratively follow this simplified process to implement defence-in-depth and a graded approach to computer security.

This step does not change the security level from '1', as it is constrained to only elevate, but may provide insight into future designs that can segregate functions along a secure architecture while allowing for the necessary inter-functional information flows necessary for security.

5. CONCLUSION

This simplified approach relies heavily on the Facility and System Computer Security Risk Management processes detailed within [3] as well as the Safety Categorization and Classification processes outlined in the IAEA Safety Standards Series [5] [9]and aforementioned IEC standards [7][8].

This paper also attempts to show how the process is four steps based on a secure by design approach with a fifth step as a verification step to confirm the results of the previous steps. The goals, functions, design, and assets are all bounded by the designer. The difficulty is that mal-operation or indeterminate states of system functions is inherently unbounded. The competency of the designer (or evaluator) becomes critical in step 4 to identify the most likely and significant unbounded events and analyse them. Given that this process is knowledge-based it is necessary to add a final step (step 5) to use an adversary-centric approach to confirm or discover additional (i.e. unanalyzed) events. Requirements to ensure the independence of steps 4 and 5 would lead to better outcomes associated with the overall process.

There are different categories of facility functions, having differing computer security goals. Safety systems are most concerned with reliability which emphasises integrity and availability. Systems containing sensitive information have increased emphasis on providing confidentiality. Different physical protection functions have combinations of availability, integrity and confidentiality requirements that may be specific to each function. Boundary control devices which interconnect computer security zones having differing security objectives may also require specific security policies to be secured effectively.

For example, Security Level 2 requirements for Safety are not the same as those for Information Security and Security as the underlying Trust Models and demands in the delivery of security are different. Similarly, the processes for configuration control, quality assurance are also likely to be different to meet the competing demands of achieving the security goal.

A key element of this approach is to treat Safety, Security, and Information Security goals, functions, and SDAs using an equivalent process; but leading to different outputs. As a result, this approach supports the diverse security objectives because it recommends building security-goal specific policies and programmes as opposed to the safety-centred approaches (which would still be applied to safety functions). The impact of this for physical protection and information security is that we don't apply incompatible procedures and SDAs that would severely impede or restrict to their ability to contribute to the achievement of their security goals.

The sole focus must be on the overriding objective to protect the correct performance of the function and undertaking design and analysis activities to raise confidence that both the protection and resilience of the assets guarantee that the function will be performed in the period of time for which it is required.

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.

REFERENCES

[1] UNITED STATES NUCLEAR REGULATORY COMMISSION, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, January 2010

[2] ROWLAND, M. T. et al. “Computer Security for I&C Systems at Nuclear Facilities”, 116-19945, paper presented at 10th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies, San Francisco, United States of America, 2017

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, draft publication Computer Security Techniques for Nuclear Facilities, To be published.

[4] WORLD NUCLEAR ASSOCIATION, Safety Classification for I&C Systems in Nuclear Power Plants – Current Status & Difficulties – CORDEL Digital Instrumentation & Control Task Force Report No. 2015/008, WNA, England, Sept 2015, http://www.world-nuclear.org/uploadedFiles/org/WNA/Publications/Working_Group_Reports/safety-classification-for-iandc-systems-in-npps.pdf

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Standards, Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1 (Rev. 1), IAEA, Vienna, 2016

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Series, Technical Guidance, Reference Manual, Computer Security at Nuclear Facilities, NSS No. 17, Vienna, 2011.

[7] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear power plants - Instrumentation and control important to safety - General requirements for systems and standard, IEC 61513:2011, IEC, Geneva, 2011

[8] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions, IEC 61226:2009, IEC, Geneva, 2009

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Standards, Safety Classification of Structures, Systems, and Components in Nuclear Power Plants, Specific Safety Guide No. SSG-30, IAEA, Vienna, 2014

[10] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear power plants - Instrumentation and control systems – Requirements for security programmes for computer-based systems , IEC 62645:2014, IEC, Geneva, 2014

[11] CANADIAN STANDARDS ASSOCIATION, Cyber security for nuclear power plants and small reactor facilities, CSA N290.7, CSA, Toronto, 2014

[12] DYER, P. “Cyber Security on Nuclear Plant in the UK”, IAEA Technical Meeting on Engineering and Design Aspects of Computer Security in Instrumentation and Control Systems for Nuclear Plants, Gloucester, UK, May 2017

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Series, Recommendations, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), NSS No. 13, Vienna, 2011.

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Series, Implementing Guide, Security of Nuclear Information, NSS No. 23-G, Vienna, 2015.

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Series, Nuclear Security Fundamentals, Objectives and Essential Elements of a State’s Nuclear Security Regime, NSS No. 20, Vienna, 2013.