Defensive Computer Security Architectures for Facilities with Radioactive Materials

Gregory A. Herdes
Apogee Group LLC, for NNSA
gregory.herdes@nnsa.doe.gov

Gregory K. White
Lawrence Livermore National Laboratory
white6@llnl.gov

Michael T. Rowland
Sandia National Laboratory
mtrowla@sandia.gov

John A. Sladek
john.sladek@canada.ca
Canadian Nuclear Safety Commission

ABSTRACT

The cybersecurity of physical protection systems protecting radioactive material should be based on solid fundamentals. Defensive Computer Security Architectures (DCSAs) are a key element for the provision of Defense-in-Depth (DiD). Specifically, DCSAs provide protection against previously unknown or undisclosed attacks (e.g., zero-day attacks). Many Nuclear Power Plants (NPPs) have implemented DCSAs either as required to comply with regulatory requirements (e.g., NEI 08-09 Rev 6 [1]) or to adopt international best practices and standards (e.g., IEC 62645 [2]). Facilities with Radioactive Materials (FRM) typically have fewer resources than NPPs and consequently may not be able to implement the same complex and expensive DCSAs as NPPs. Many FRM may face some or all of the following challenges: (i) They treat physical protection systems as a monolithic/single zone system at one level of security which precludes the application of a graded approach or DiD; (ii) they have multiple regulations and legal requirements (e.g., U.S. Health Insurance Portability and Accountability Act (HIPAA), EU General Data Protection Requirements (GDPR)) that must be met; and (iii) they may utilize contracted support for information technology and security which involves risk transfer and sharing agreements that require appropriate management.

Effective DCSAs are established through specification and implementation. The specification process results in the DCSA requirements based on a graded approach. These requirements are applied to the boundaries of systems and networks that contribute to the protection of radioactive materials. DCSA implementation involves the construction, operation, and maintenance of the DCSA. It is through implementation of the DCSA requirements that DiD is established. We will discuss the theoretical basis for DCSAs and propose a practical implementation of DCSAs and the graded approach for physical protection systems at facilities with radioactive materials. We will describe how the DCSA was implemented in physical protection systems at facilities with radioactive materials that are supported by National Nuclear Security Administration's Office of Radiological Security. Finally, we will provide insights into the regulatory considerations of this approach, including considerations from the Canadian Nuclear Safety Commission (CNSC), and provide an evaluation of the impact of the arrangements with contractors or outside organizations.

INTRODUCTION

The International Atomic Energy Agency (IAEA) Nuclear Security Series (NSS) No. 20 – Nuclear Security Fundamentals – Objective and Essential Elements of a State's Nuclear Security Regime [3] details the objective and essential elements of a State's Nuclear Security Regime. Essential elements of particular importance for information and computer security are:

- Element 3: Legislative and Regulatory Framework, which recommends that the State establish regulations and requirements for information and computer security;
- Element 6: International Cooperation and Assistance, which recommends the establishment of arrangements that allow for the secure exchange of sensitive information; and
- Element 9: Use of Risk Informed Approaches, which recommends the use of risk assessments to specify graded requirements and recommends the implementation of consistent DiD approaches.

Other IAEA publications on computer security provide greater guidance on essential element 9. IAEA NSS 42-G [4] introduces the concepts of computer security levels (i.e., sets of graded requirements) and computer security zones (i.e., logical and physical areas that contain computer-based systems having common computer security protection requirements). IAEA NSS 42-G further describes the concept of a Defensive Computer Security Architecture (DCSA) that is a practical way to arrange computer security zones to provide the greatest protection to computer-based systems associated with the greatest consequences. The rationale of the DCSA is that the outer zones provide layers of defense that are independent and mutually supportive of the layers of defense associated with the inner zones.

BACKGROUND

A significant part of IAEA computer security guidance is focused on nuclear facilities (i.e., NPPs, Research Reactors, and Fuel Cycle Facilities) that have potential consequences of theft of nuclear material or sabotage resulting in High Radiological Consequences. However, other radioactive material and associated facilities are generally accepted as being associated with significant but less severe consequences as compared to nuclear facilities.

From this perspective, IAEA NSS No. 11-G Rev 1, Security of Radioactive Material in Use and Storage and of Associated Facilities, [5] defines three *overall security levels* based on the categorization (type and quantity) of radioactive material. These levels define appropriate levels of protection of radioactive material against unauthorized removal based upon consequences and risk. This applies a graded approach to the functional requirements of *deter, detect, delay, and respond* to a potential malicious act.

United States Department of Energy's Office of Radiological Security (ORS) has also performed a risk assessment of domestic and international radioactive materials. ORS prioritizes support to facilities based on the quantity and type of the radioactive material, the country/geographical region in which the material is located, and other factors. ORS then provides consistent protection at a single security level. In facilities with quantities of radioactive material that do not meet ORS threshold quantities, ORS is not a stakeholder to the protection of the material.

FUNDAMENTAL CONCEPTS

The computer security levels and computer security zones[1] concepts originated from IAEA guidance specified in NSS 17 [6] and is more fully detailed and documented within NES NP-T-3.21 [7] and NSS 17-T Rev. 1 [8]. These two concepts are part of a larger facility context represented in Figure 1, which shows an idealized relationships between facility functions, security levels, systems, and security zones.

Facility Function: An objective or purpose that needs to be achieved. For example, control of physical access to a radioactive source during maintenance activities on the device.

Level: The strength of security protection required for a facility function and consequently for the system that performs that function (adapted from NSS 17-T Rev. 1). Each security level is a distinct set of requirements that are necessary to protect the safe and secure performance of the facility function. A graded approach demands more than one security level, each with its own distinct set of distinct requirements. It may be necessary for requirements to be duplicated within multiple levels or applied to equally to all levels (i.e., baseline or generic requirements; typically policy requirements).

Zone: A group of systems having common physical and virtual (logical) boundaries and, if necessary, arranged using additional criteria. Systems within a zone are assigned a common security level to simplify the administration, communication, and application of computer security measures (adapted from NSS 17-T Rev. 1).

System: An integrated set of equipment or components that are used to perform a facility function (adapted from NSS 20, sensitive information assets and NSS 13 physical protection system).

[1] For the remainder of the paper, we will refer to levels and zones as the IAEA's computer security zones and levels and not IAEA's overall security levels for radioactive material as defined in IAEA NSS No. 11-G Rev 1.

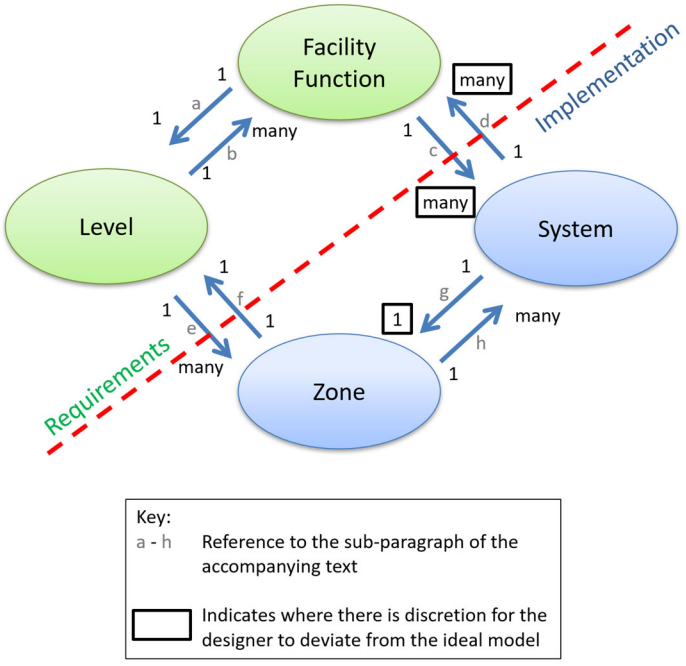


Figure 1: Fundamental Concepts [NSS 17-T Rev. 1]

a – Each *Facility Function* is assigned to a single *Level*

b – Each *Level* may be applied to one or more *Facility Function(s)*

c – Each *Facility Function* may be assigned to one or more *System(s)*[2]

d – Each *System* may perform one or more *Facility Function(s)*[3]

e – Each *Level* may be applied to one or more *Zone(s)*[4]

f – Each *Zone* is assigned a *Level*

g – Each *System* is placed within a single *Zone*, where possible

h – Each Zone may consist of one or more System(s)

Idealized relationships connect all four entities in a logical manner and allow for the separation of analysis of computer security (including specification of requirements) and implementation and maintenance of computer security. These relationships are key to using risk informed approaches for computer security as well as understanding how to protect against a threat actor with cyber-attack capabilities.

SECURITY LEVELS

For this paper, only levels and zones for facilities where ORS is a stakeholder for the security of radioactive material will be discussed.

The IAEA publication NSS 17-T Rev. 1 [8] provides for an example implementation for a nuclear power plant (NPP) that includes a graded set of five security levels. The five levels (with a sixth undefined level being external

[2] e.g., a function may be assigned to two independent, diverse, shutdown systems.

[3] e.g., a human–machine interface. Ideally from a security perspective, a single system performs a single facility function, but designers may assign more than one facility function to a system if deemed necessary to support human, operational, or safety performance.

[4] Ideally from a security perspective, each facility function would be defined to be performed by a single system which is within a single zone and therefore assigned a single level, but designers may deviate from the ideal due to other considerations, e.g., fire protection or physical protection systems that span the entire (or a significant portion of the) facility and therefore may pass through physical areas that contain zones assigned to different levels.

to the facility) are reflective of the different categories of functions (based on significance) needed for the safe and secure operation of NPPs and leverages the graded categorization of safety functions (e.g., IEC 61513 [9]). These categories are based upon the potential consequence associated with the loss or improper execution of the facility function.

The potential consequences of a compromise to systems that perform a facility function are from worst to best case (adapted from NSS 33-T [10]):

- The function is indeterminate. The effects of the compromise result in an unobserved alteration to system design or function.
- The function has unexpected behaviors or actions that are observable to the operator.
- The function fails.
- The function performs as expected, meaning the compromise does not adversely affect system function (i.e., it is fault tolerant).

When applying this approach to FRM, the most severe potential consequences associated with an NPP (namely sabotage resulting in High Radiological Consequences) are not possible for these facilities. The absence of the most severe consequences lowers the computer security requirements of the functions with the highest significance at FRM. Therefore, while this paper recommends the same similarly number of levels (i.e., 1 to 5), it is clearly evident that the associated sets of requirements for each level for FRM are not identical or equivalent to the requirements for the similarly numbered level for NPPs in NSS 17-T Rev. 1 [8].

ZONES

Zones are implementation artifacts of a computer security program. Zones exist and can be directly observed (e.g., physical boundaries) or determined using network security tools (e.g., network scanning/mapping). Zones simplify the administration, communication, and application of computer security measures and provide the building blocks for DiD when arranged within a DCSA. DiD is a security concept where multiple independent and redundant defensive layers are created to delay the attacker, deter them from attacking, increase the probability of detection, and support effective response. Zones are established such that systems that are assigned within the same zone maintain trust relations with each other. All systems within a zone are assigned to a single level based on the most significant function performed by systems within the zone and consequently the same computer security requirements are applied to all systems within a zone. Zones involve internal networks, network perimeter security, and physical security. Segmentation and isolation of networks provides key network locations at which network intrusion detection measures can be installed.

Some reasons for separating systems into zones may be:

1. Preservation of trusted communication.
2. Different organizational responsibilities, for example: Information Technology department vs. medical staff vs. physical security staff.
3. Separation, for example: different zones for redundant systems.
4. Existing zones for other purposes, for example: utilizing an existing administrative or communication zone.

It is important to note that typically each zone forms an internal “trusted” area where communications between systems within the same zone do not require cyber security measures. This implies no need for communication de-coupling devices such as a firewall or any other isolation type device within the zone. However, communications between zones, assigned to different security levels have different protection requirements and therefore have different levels of trust. This will require cyber security measures to protect against malicious attacks originating from less trusted zones. Some of these measures may be implemented at the zone boundaries or within the zone.

RECOMMENDED PROCESS FOR SPECIFYING A DCSA

The DCSA consists of two parts: (i) a specification or set of overall requirements that imposes conditions or constraints on the overall facility or system design; and (ii) the actual implementation and construction of the facility or system.

The key steps within the DCSA specification process are:

1) Identify and describe facility (or system) functions.
2) Assign each function to a security level.
3) Identify systems (or parts of the system) that perform a facility function.
4) Identify zones and establish boundaries (logical and physical) in which systems are contained.
5) Develop requirements for arrangement of zones, interzonal computer security measures, and restrictions on interzone communications.

This specification leverages the graded approach (i.e., security levels) and contains the requirements for DiD against cybersecurity for the facility (or system).

ASSIGNMENT OF FUNCTIONS TO LEVELS FOR RMS

ORS implements a system with six levels where Level 1 provides the highest level of protection[5]. *RMS = Remote Monitoring System that protects the radioactive material.*

Level	Functions
1	Core RMS (inside the RMS enclosure) – This enclosure includes the RMS computer, external communications for the RMS, tamper detectors for the enclosure, a radiation sensor to monitor room background (in case the radiation source is removed from its shielding), and external connections to the room's physical security system.
2	Auxiliary RMS (RMS equipment inside the secure room) – This includes tamper seals around the equipment containing the radioactive source and video cameras to monitor activities in the room. This includes response/security personnel, along with the site operator.
3	RMS Security Response (RMS equipment outside the secure room) – This includes video cameras outside of the room that monitor activities near the RMS equipment. This includes response/security personnel, along with the site operator.
4	Facility Security Response (facility security and/or alarm monitoring company) – This includes the RMS security console and other physical security systems that help protect the radiation source.
5	Facility (the facility where the RMS is installed)[6] – This includes all other information technology (IT) and operational technology (OT) systems at the facility. This includes facility medical equipment, plant systems, computers, servers, peripherals, etc.
6	External to Facility (the internet) – This includes equipment and users that access the facility from locations not physically under the control of the facility. For instance, employees accessing systems from home, cloud-based services and patients accessing facility systems to communicate with facility personnel.

ORS has implemented a set of formal technical requirements for each level. ORS does not specify additional requirements on the facility. However, additional recommendations can be taken from ORS Cybersecurity Best Practices publications [11] (especially at levels 5 and 6) but are not listed here. ORS-supported facilities can obtain the mapping of requirements to levels.

[5] The number convention for levels is based upon the IAEA's standard where security level 1 is the highest level of protection. The US NRC implements a system where level 0 is the lowest level of protection and level 4 is the highest level of protection. Other countries have also implemented the NRC's standard.

[6] The facility may choose to divide this into additional security levels.

IDENTIFICATION OF ZONES

ORS implements six zones. As part of a DCSA, each zone must be mapped to a level. Because of this, the number of zones is greater than equal to the number of levels, but not less.

Zones	Description	Level
A	RMS enclosure/system	1
B	Auxiliary RMS equipment inside protected room	2
C	Auxiliary RMS equipment outside protected room	3
D	RMS security consoles	4
E	Facility security equipment	4
F	Facility equipment[7]	5
G	External Facility users	6

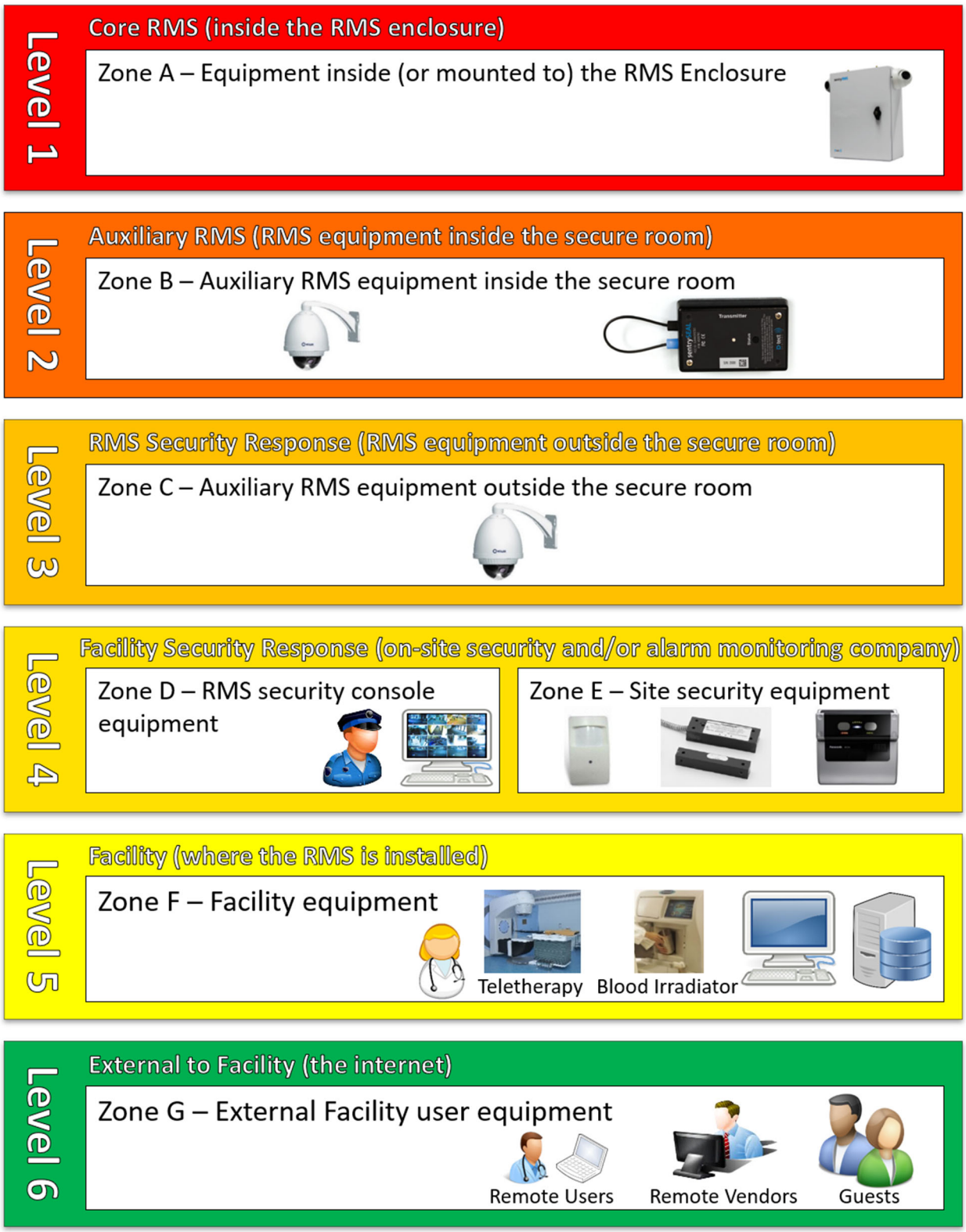
DCSA SPECIFICATION

The diagram below shows the requirements for arrangement of the Zones. There are additional requirements on the system to ensure that computer security measures are in place between each of the zones below.

Zone A is in the innermost physical areas of the RMS system. Zone A network does not physically extend outside of the enclosure and is only connected to Zone B networks. Computer security measures (e.g., one-way outbound only communications) ensure that the integrity of equipment inside the enclosure is maintained. Zone B is the next physical area (i.e., secure room) that is outside of the RMS Enclosure. Similarly, Zone B network does not physically extend outside the enclosure and is only connected to Zone A and Zone C networks. Zone B communications to Zone C are also protected by computer security measures.

These requirements are iterated until Zone G to ensure that Zone A is the most physically protected and offered the greatest network communication protections. The outer Zones are not required to have their physical and logical (network) boundaries tightly coupled. For example, it is likely for some services and equipment assigned to Zone F and G be provided via cloud infrastructure.

[7] The facility may choose to divide this into additional security zones.



CANADIAN REGULATORY CONSIDERATIONS

The Canadian Nuclear Safety Commission (CNSC) has identified ORS' *Cybersecurity Best Practices for Users of Radioactive Sources* [11] and ORS' *Procurement Requirements for ORS-provided Security Systems* [12] publications as potentially serving to inform expectations or provide guidance for the protection of physical protection systems. They are in the process of proposing changes to the Canadian regulatory regime to extend

cyber security requirements to other radiological material, specifically to sealed sources. Since there is very little Canadian or international experience with regulation of cyber security for other radiological the CNSC has prepared a public discussion paper [13] containing possible approaches and requirements for cyber security. The purpose of the discussion paper [13] is to solicit input from licensees and the public that will inform the development of regulatory guidance and requirements.

The CNSC discussion paper proposes that cyber security be applied to Category 1 and 2 sealed sources to protect functions involved in Safety, Security, Emergency Preparedness, and Safeguards. Since the facilities or locations where sealed sources are used are varied (e.g., medical facility, pool irradiator, industrial gauges or radiography), a flexible approach will be needed. For instance, not all Category I and II sealed source licensees will have automated systems used for emergency preparedness and response.

The following principles are proposed in the discussion paper:

- Use of a graded approach based upon five security levels (internal to facility) as discussed above.
- Specification and implementation of a defensive cyber security architecture that establishes defense in depth.
- Development of a computer security program to define the roles, responsibilities and procedures used to meet the cyber security objectives.
- Implementation of cyber security measures to prevent adversaries from completing malicious acts against the radiological material, associated facilities or associated activities.

CONCLUSIONS

The four concepts of Facility Functions, Security Levels, Systems, and Security Zones are key in specifying a DCSA that provides DiD. Facility Functions and Security Levels are essential for application of a graded approach. Through the definition of sets of graded requirements (i.e., Security Levels), implementation and conduct of computer security activities can be optimized with the greatest effort directed to protecting systems associated with the most significant consequences.

Once functions and levels have been specified, the systems can be identified and assigned to zones, after which zones are established. However, without requirements for a DCSA, any efforts to implement DiD would be ad hoc, and unlikely to build into the facility (or system) the DiD that is critical for computer security. Given current experience, previously unknown or undisclosed vulnerabilities will be discovered or used during a system's lifetime and exploited by adversaries in the conduct of cyber-attacks targeting key systems for security. A DCSA that specifies a layered defense and a facility that implements such a DCSA would be able to leverage a very effective measure that can reduce risks associated with these types of attacks.

Current publications [11,12] and the CNSC discussion paper [13] do not explicitly contain requirements on DCSAs. However, given its importance for DiD, DCSAs demand consideration within computer security plans and programs for facilities with radioactive materials. This paper provides a possible implementation of a defensive architecture to meet the requirements and inform expectations for DiD against cyber-attacks.

ACKNOWLEDGMENT

The authors wish to thank Robert Anderson from Idaho National Laboratory for his critical help in understanding these concepts and reviewing ORS' implementation.

[LLNL-CONF-824495] Lawrence Livermore National Laboratory is operated by Lawrence Livermore National Security, LLC, for the U.S. Department of Energy, National Nuclear Security Administration under Contract DE-AC52-07NA27344.

[SAND2021-8340 C] Sandia National Laboratories is a multi-mission 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.

[CNSC E-DOCS #6605969]

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

REFERENCES

[1] Nuclear Energy Institute, *Cyber Security Plan for Nuclear Power Reactors*, NEI 08-09 [Rev. 6], April 2010, Washington DC, USA

[2] International Electrotechnical Commission, Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity requirements, IEC 62645, November 2019, Geneva, Switzerland

[3] International Atomic Energy Agency, *Objective and Essential Elements of a State's Nuclear Security Regime*, NSS 20, 2013, Vienna, Austria

[4] International Atomic Energy Agency, *Computer Security for Nuclear Security*, NSS 42-G, Vienna, Austria (in preparation)

[5] International Atomic Energy Agency, *Security of Radioactive Material in Use and Storage and of Associated Facilities*, NSS 11-G (Rev. 1), 2019, Vienna, Austria

[6] International Atomic Energy Agency, *Computer Security at Nuclear Facilities*, NSS 17, 2011, Vienna, Austria

[7] International Atomic Energy Agency, *Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Facilities*, NES NP-T-3.21, 2016, Vienna, Austria

[8] International Atomic Energy Agency, *Computer Security Techniques for Nuclear Facilities*, Nuclear Security Series No. 17-T (Rev. 1), Vienna, Austria (in preparation)

[9] International Electrotechnical Commission, *Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems*, IEC 61513, August 2011, Geneva, Switzerland

[10] International Atomic Energy Agency, *Computer Security of Instrumentation and Control Systems at Nuclear Facilities*, NSS 33-T, 2018, Vienna, Austria

[11] National Nuclear Security Agency – Office of Radiological Security, *Cybersecurity Best Practices for Users of Radioactive Sources*, 2021, Washington DC.

[12] National Nuclear Security Agency – Office of Radiological Security, *Procurement Requirements for ORS-provided Security Systems*, 2018, Washington DC.

[13] Canadian Nuclear Safety Commission, Discussion Paper DIS-21-03, *Cyber Security and the Protection of Digital Information*, 2021