



Using the Information Harm Triangle to Identify Risk-Informed Cybersecurity Strategies for Instrumentation and Control Systems

Michael T. Rowland, Lee T. Maccarone & Andrew J. Clark

To cite this article: Michael T. Rowland, Lee T. Maccarone & Andrew J. Clark (2023) Using the Information Harm Triangle to Identify Risk-Informed Cybersecurity Strategies for Instrumentation and Control Systems, Nuclear Technology, 209:3, 471-487, DOI: [10.1080/00295450.2022.2087841](https://doi.org/10.1080/00295450.2022.2087841)

To link to this article: <https://doi.org/10.1080/00295450.2022.2087841>



This material is published by permission of Sandia National Laboratories, 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 No. DE-NA0003525, SAND2022-9116J. The U.S. Government retains for itself, and others acting on its behalf, a paid-up, non-exclusive, and irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.



Published online: 07 Sep 2022,



Submit your article to this journal 



Article views: 1598



View related articles 



View Crossmark data 



Using the Information Harm Triangle to Identify Risk-Informed Cybersecurity Strategies for Instrumentation and Control Systems

Michael T. Rowland,^{ID*} Lee T. Maccarone,^{ID} and Andrew J. Clark

Sandia National Laboratories, P.O. Box 5800, Albuquerque, New Mexico 87185-0748

Received December 15, 2021

Accepted for Publication June 2, 2022

Abstract — *The Information Harm Triangle (IHT) is a novel approach that aims to adapt intuitive engineering concepts to simplify defense in depth for instrumentation and control (I&C) systems at nuclear power plants. This approach combines digital harm, real-world harm, and unsafe control actions (UCAs) into a single graph named “Information Harm Triangle.” The IHT is based on the postulation that the consequences of cyberattacks targeting I&C systems can be expressed in terms of two orthogonal components: a component representing the magnitude of data harm (DH) (i.e., digital information harm) and a component representing physical information harm (PIH) (i.e., real-world harm, e.g., an inadvertent plant trip). The magnitude of the severity of the physical consequence is the aspect of risk that is of concern. The sum of these two components represents the total information harm.*

The IHT intuitively informs risk-informed cybersecurity strategies that employ independent measures that either act to prevent, reduce, or mitigate DH or PIH. Another aspect of the IHT is that the DH can result in cyber-initiated UCAs that result in severe physical consequences. The orthogonality of DH and PIH provides insights into designing effective defense in depth. The IHT can also represent cyberattacks that have the potential to impede, evade, or compromise countermeasures from taking appropriate action to reduce, stop, or mitigate the harm caused by such UCAs. Cyber-initiated UCAs transform DH to PIH.

Keywords — *Cybersecurity, operational technologies, data, harm, information.*

Note — *Some figures may be in color only in the electronic version.*

*E-mail: mtrowla@sandia.gov

This material is published by permission of Sandia National Laboratories, 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 No. DE-NA0003525, SAND2022-9116J. The U.S. Government retains for itself, and others acting on its behalf, a paid-up, non-exclusive, and irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

I. INTRODUCTION

Modern nuclear power plants (NPPs) are becoming increasingly dependent on the integration of digital technologies and plant processes. While digital technologies enable many benefits such as advanced instrumentation and control (I&C) systems and state-of-the-art monitoring and diagnostics techniques,^{1,2} the introduction of these technologies introduces the potential for cyberattacks within operational technology (OT) environments. The potential consequences of a cyberattack on an OT system extend beyond those consequences associated with cyberattacks targeting traditional information and communications technology (ICT) environments. While cyberattacks on ICT systems may impact data confidentiality, integrity, and availability, cyberattacks in OT environments may

also impact physical processes.³ As commercial NPPs become increasingly reliant upon digital I&C systems, new methods of security analysis are required that consider the impact of cyberattacks on both digital information and physical processes.

This work proposes a novel approach to characterizing cyberattacks on NPP I&C systems and identifying effective cybersecurity strategies. The Information Harm Triangle (IHT) is an abstraction of cyberattack scenarios that decomposes the impact of the attack into two components: data harm (DH) and physical information harm (PIH). Data harm is the harm to information that requires interpretation by digital systems whereas PIH is harm to information that does not require interpretation by digital systems. An example of DH is modifying a control law in a digital controller, and an example of PIH is manipulation of water level in the reactor vessel. These concepts are discussed in greater detail in Sec. III.

The application of the IHT is presented for several case studies. These case studies complement existing risk analyses conducted using System-Theoretic Process Analysis⁴ (STPA). STPA is a systems-theoretic approach used to analyze complex systems holistically to identify unsafe control actions⁴ (UCAs). Some UCAs associated with digital I&C systems may be initiated when the adversary causes DH to the system. In turn, the UCA converts the DH to PIH to the NPP. By using the IHT to study the relationships among DH, UCAs, and PIH, security teams can identify effective security strategies. These strategies include appropriate prioritization of DH protection or PIH protection and the elimination of specific UCAs associated with unacceptable levels of PIH.

II. CURRENT APPROACHES TO NPP SECURITY

Current approaches to cybersecurity of NPPs involve the development, implementation, and maintenance of a cybersecurity program. NEI 08-09, Rev. 6 (Ref. 5), provides guidance for operators of NPPs on how to develop and implement Cyber Security Plans (CSPs) for protection of digital computer and information systems for U.S. Nuclear Regulatory Commission (NRC) licensing under 10 CFR 73.54 (Ref. 6). NEI 08-09, Rev. 6^a

(Ref. 5), also contains a list of security controls that are based on the second revision (December 2013) of National Institute of Standards and Technology (NIST) SP 800-53 (Ref. 7) and the final draft (September 2008) of NIST SP 800-82 (Ref. 8).

IEC 62645 (Ref. 9) is the international standard equivalent of NEI 08-09 (Ref. 5) that details cybersecurity programs for international audiences. Unlike NEI 08-09, IEC 62645 (Ref. 9) does not list security controls, which are provided in IEC 63096 (Ref. 10). The security controls in both NEI 08-09 and IEC 63096 are focused primarily on the protection of confidentiality, integrity, and availability of information, specifically, information that is important to the correct operation of critical (significant) systems. The World Nuclear Association has compiled the relationships among these international standards.¹¹

Programs based on NEI 08-09 (Ref. 5) or IEC 62645 (Ref. 9) rely upon defensive strategies that consist of a defensive architecture and a set of security controls deployed within that architecture. These programs may assign assets or systems to security levels, security degrees, or other classifications (e.g., balance of plant, safety, and emergency preparedness) that are associated with graded security requirements. The assignment methods take into consideration the safety, security, or other consequences related to compromise of the asset or system. For assets or systems having safety consequences, the assignment to a security level is often correlated with the safety classification of the asset or system (e.g., safety related, Safety Class 1); however, there is no direct one-to-one relationship between safety and cybersecurity classifications. The World Nuclear Association has compiled the system safety classifications of many countries.¹²

The International Atomic Energy Agency (IAEA) also provides recommendations for the security of nuclear facilities and nuclear material, including information and computer security,^b in IAEA Nuclear Security Series (NSS) NSS 13 (Ref. 13). The IAEA further provides guidance on risk-informed approaches that support the development of a cybersecurity program covering all digital systems (e.g., traditional ICT systems, physical protection systems, and I&C systems) throughout the NSS. NSS 17-T (Ref. 14) provides technical guidance for developing cybersecurity programs at nuclear facilities. NSS 33-T (Ref. 15) provides technical guidance for cybersecurity programs specific to I&C systems and is the security complement to the Specific Safety Guide

^a NEI 08-09, Rev. 6, is the publication that assists licensees in constructing and implementing their CSP as required by 10 CFR 73.54. NRC Regulatory Guide 5.71, “Cyber Security Programs For Nuclear Facilities,” and NEI 08-09, Rev. 6, are two similar but not identical approaches for meeting “the rule”; however, the vast majority of the security controls in both guides are taken from the NIST publications.

^b The term “computer security” is equivalent to “cybersecurity” in IAEA publications.

SSG-39 (Ref. 16). Outside of the NSS, the IAEA Nuclear Energy Series also provides security considerations for the design of NPP I&C systems in NR-T-3.30 (Ref. 17). These publications provide recommendations for the development of a risk-informed cybersecurity program for both ICT and OT systems but do not specify the method by which risk is to be evaluated.

Risk is traditionally calculated as the product of the likelihood of an event and the consequence of that event. Security risk assessments at NPPs typically assume that an attack on the facility is certain. This assumption is necessary due to two factors: (1) attacks do not occur with a predictable frequency (i.e., black swan events) and (2) the potential consequences of such attacks may be severe or unacceptable. Assuming that an attack is certain results in risks being analyzed and prioritized (i.e., assignment of a system to a security level/degree) solely based on the severity of its potential consequence.^{13,18}

Further, NIST SP 800-82, Rev. 2, Sec. III.C. (Ref. 8), states that when performing an industrial control systems (ICS) risk assessment, there are special considerations for I&C systems since a cyberattack against I&C can have physical effects as well as digital effects. An information security risk assessment is primarily concerned with digital effects (i.e., DH) and is complemented by safety assessments that are primarily concerned with the physical effects (i.e., PIH). However, the guidance does not provide a method to assess the safety risk arising from cyberattack relying mostly on the expertise of the individual or organization performing the assessment.

III. INFORMATION AND DATA

IAEA NSS 23-G, paragraph 2.2 (Ref. 19), states the following:

Information is knowledge, irrespective of its form of existence or expression. It includes ideas, concepts, events, processes, thoughts, facts and patterns. Information can be recorded on material such as paper, film, magnetic or optical media, or held in electronic systems. Information can be represented and communicated by almost any means. In the nuclear domain, there is a vast amount of information in many forms. Information assets are the equipment or components (including media) that are used to store, process, control or transmit information.¹⁹

III.A. Data

Data are information processed, transmitted, or stored on digital systems. Data are “Information in a specific

representation, usually as a sequence of symbols that have meaning.”²⁰ Data within digital systems are information that is encoded using various standards and methods. Data may be stored in databases for use by autonomous, semiautonomous, or manual OT systems. Data cannot be observed or measured without interpretation by a digital system acting as an intermediary.

III.B. Physical Information

Physical information is information that can be measured or observed by humans or equipment. Physical information may exist as pressure, temperature, flow, or other physical phenomena that capture information. The critical part is that physical information does not have to be interpreted to verify its existence or to be observed correctly.

III.C. Data Versus Physical Information

Physical information and data coexist within OT systems. A hypothetical nondigital observer would be able to measure the physical information within a cell of a solid-state drive by measuring the amount of electric charge (in coulombs) that is stored on the capacitor (i.e., floating gate transistor), where a digital observer would measure the data by determining the absence of significant change (i.e., level of charge that exceeds the threshold to register as “high”).

This relationship has a significant effect on finding a common scale upon which to measure harm. As in the example above, the physical information provides a quantity of information that is equal to some real number (i.e., the measured charge in coulombs) versus case for the data. If the digital observer used a binary comparator, the provided information is 1 bit (i.e., high, or low).

To further the disparity between digital and physical information measurements, the real number if converted to a binary representation of that number (e.g., floating point) would convey much more than 1 bit of information. This deviance in the quantity of information conveyed by the real number versus the single bit demands an exploration of the meaning of the information.

III.D. Information Versus Meaning

The separation between meaning and information is critical to understanding the IHT. In some branches of philosophy, meaning is “a relationship between two sorts of things: a sign, and the kinds of things they intend, express, or signify.”²¹ The information is a sign, and it is

the interpretation of these signs (i.e., their intension, expression, or significance) that provides meaning.

The IHT does not aim to explicitly convey meaning to the practitioner; it aims only to intuitively capture harm to information that has relevance to meaning, which is the initiation of UCAs that may lead to consequences that have importance (i.e., significant meaning to the organization).

It is critical that information within the system or person not be assumed to have a specific meaning; this is a constraint that limits intangible information to data only. Information is considered as separate from meaning, as the UCA and its associated physical consequence are representative of the meaning, and this can be ascertained only by the controller or observer (e.g., system or person). Note the following example. The temperature outside is 35°C. This represents physical information. However, the meaning to the person (i.e., controller) is that the weather outside is hot. The meaning of this information will inform the actions the person takes to remain comfortable while outside during the day (e.g., choice of clothing, shade, and water).

III.D.1. Example: Data Versus Meaning (OSI Model)

As stated in Sec. III.A, data are information encoded in digital form. In order to ascertain the meaning of data, they first must be interpreted by digital systems based upon the relevant standards, specifications, or requirements (i.e., consensus). One example of this consensus-based approach is the open systems interconnect (OSI) model (ITU-T X.200)

(Ref. 22). The OSI architecture model consists of seven layers that allow for two digital communication systems to exchange data between each other. The OSI model is summarized in Table I.

III.D.1.a. OSI Layer 1: Physical Layer (Physical Information)

The physical layer provides for the physical transmission of physical information between two open and networked systems. The source converts data provided by the data link layer and transforms it into physical information based on the protocol requirements (e.g., RS-232, 10BASE-T, Bluetooth). The receiver receives the physical information and encodes it to data (e.g., bits/symbols) based on the applicable requirements, specification, or standard of the selected protocol.

III.D.1.b. OSI Layers 2 to 7: Data Link to Application Layer (Data)

The data are then passed up the layers where the data are further interpreted by the receiver and then presented to the application. The application may infer meaning directly and take autonomous action or present this information to the user via a graphical user interface (GUI) or command line interface (CLI) in a manner that allows for the user to derive meaning and act.

The difference between data and meaning is implicit within the OSI layers. A service data unit (SDU) is how layers in a single system communicate with one another.

TABLE I
OSI Architecture Mode*

Layer			Protocol Data Unit	Function ^a
Data	7	Application	Data	End user layer control system application HTTP, FTP
	6	Presentation		Interpretation of data Encryption/decryption
	5	Session		Session management sockets
	4	Transport	Segment, datagram	End-to-end connections TCP, UDP
	3	Network	Packet	Intermediate routing IP, ICMP
	2	Data link	Frame	Transfer of data on a physical link Ethernet
Physical Information	1	Physical	Bit/symbol	Transit and receipt of raw bit streams in physical form

*Adapted from Ref. 23.

^aHTTP = Hypertext Transfer Protocol; FTP = File Transfer Protocol; TCP = Transmission Control Protocol; UDP = User Datagram Protocol; IP = Internet Protocol; ICMP = Internet Control Message Protocol.

The SDU is data generated by the user of a service transmitted to a peer service user in a way that does not change the meaning of the data. However, communicating peer entities (i.e., systems in the same OSI layer) can interpret the data and derive meaning from these data. The protocol data unit is composed of protocol-specific information (i.e., context and metadata). It is this composition that allows the peer entity to derive the correct meaning of the data.

IV. CYBERSECURITY PRINCIPLES

Anderson's seminal paper, "Computer Security Technology Planning Study," Vol II, Appendix I (Ref. 24), states the following:

The traditional statement of security threat has had the classical objectives of:

- a. information recovery
- b. manipulation of information
- c. denial or degradation of service.²⁴

This basis is critical in applying the concept of harm as the primary objective of cybersecurity for OT systems.

IV.A. Information Security Triad

Protection against these threat objectives is commonly referred to as the information security triad, which consists of confidentiality, integrity, and availability. Confidentiality is protection against information recovery by the adversary, integrity is protection against manipulation of information, and availability is protection against denial or degradation of service.

Anderson²⁴ describes these goals in terms of the harm to information that is achieved by the adversary. This harm to information forms the basis of the IHT. All violations of a computer lead to at least one of the three means by which harm is achieved. Anderson aimed to protect classified multiuser U.S. Air Force systems that prioritized confidentiality. However, NPP operators aim to protect OT that performs safety or security functions, and consequently, they prioritize integrity and availability. Prioritization of integrity and availability is critical to the protection of OT and fundamental to understanding the IHT.

IV.B. Operational Technology Cybersecurity

Operational technology systems are combinations of analog and digital components. Analog components

interact with physical information while digital components interact with information encoded in data.

Data are of particular importance as they are the bridge between computer systems and physical information and computer security. Generally, protection of information is elusive as it can exist in intangible forms and is therefore replaced with the protection of data as they exist on computer-based systems and associated networks.²⁴ Data have importance for both services and products. Additionally, data, especially sensitive information, are generally unique and irreplaceable.

Manipulation of data can lead to (1) initiation of UCAs and (2) modification or disruption of data-dependent operator interfaces (i.e., GUI or CLI) that either spoof or impair the ability of human intervenors to correct UCAs. In the case of UCAs, the DH is converted to PIH, which may be captured by analog equipment and provide this information to the operator. However, the modification or disruption of operator interfaces may limit the value of the provided physical information.

V. SYSTEM-THEORETIC PROCESS ANALYSIS

System-Theoretic Process Analysis⁴ is a relatively new hazard analysis technique that is based on system theory. STPA has several advantages over traditional techniques, one of them being its ability to cope with complex systems, such as the integration of digital and nondigital systems. Rather than decompose a system into individual components and analyze each component in isolation, STPA analyzes the system as a whole by considering how each subsystem and component contributes to the overall system function. STPA is used to identify "unknown unknowns" of digital systems as well as identify emergent properties, i.e., properties arising from relationships among the parts of the system by how they interact and fit together.

The increased use of digital components, systems, sensors, and software to control process components such as valves and pumps should lead to the realization that systems engineering processes and approaches are needed for digital modernization. Systems engineering seeks a safe, secure, and balanced approach for the design, realization, management, operation, and retirement of a system. Traditionally, safety and security implementation can face conflicting constraints, and existing hazard methodologies do not provide an objective assessment for decision makers to understand the trade-offs in designing and operating a system. By leveraging STPA and systems engineering, decision makers can methodically, efficiently, and systematically allocate resources (e.g., staff time and money) toward areas of highest risk.

In brief, the steps of STPA are the following^{4,c}:

1. *Define the purpose of the analysis.* In this stage of STPA, the losses, hazards, and constraints are identified. Losses are consequences that are unacceptable to system stakeholders. For NPP systems, losses may include core damage or release of radioactive materials. A hazard is a system state that may lead to a loss under certain conditions. An example of a hazard in an NPP system is the reactor coolant system failing to provide adequate flow to cool the fuel. An example of DH leading to this hazard is a change in a controller setpoint that causes a pump control action to not be provided when needed. Constraints are the conditions that must be met to prevent hazards.

2. *Model the control structure.* In this stage, hierarchical control structures (HCSs) are developed to describe the control structure of the system. HCSs show how digital assets of the system interact with the underlying physical processes and with other digital assets. The control system provides control actions to manipulate the physical process and receives feedback from the process. Process variables that may be affected by DH include pressure, temperature, and flow rates. This type of PIH may be detectable through feedback if DH has not been caused to the feedback system.

3. *Identify UCAs.* UCAs are control actions that may lead to a hazard under certain conditions. UCAs generally fall into one of four categories: (a) control signal not provided when needed, (b) control signal provided when not needed, (c) control signal provided at the incorrect time, and (d) control signal provided for the incorrect duration. Adversaries with sufficient access and privileges on a digital controller can select the UCA that causes the greatest impact (i.e., greatest PIH).

4. *Identify loss scenarios.* Loss scenarios describe the progression from UCAs to hazards and losses. This stage of STPA explains how manipulation of digital information can lead to physical consequences. The losses are often highly correlated with PIH.

The relationship between STPA and the IHT is represented both implicitly and explicitly. The HCSs developed in STPA model the flow of information—both physical information and data—between controllers and process components. For a digital controller, meaning is ascertained from this information based upon the control system application (e.g., programmable logic). The

function of the digital controller is to act upon this meaning by sending commands and actions to other controllers or process components. In the STPA lexicon, information is “feedback” from sensors, and meaning is the “process model” and “control algorithm.” Thus, from a security perspective, the harm (i.e., alteration) of the physical information or data can result in a UCA, and the magnitude of the UCA is the result of adversary harm to the physical information and data.

There is an interdependent relationship between the UCAs and information. For instance, STPA and resulting UCAs are identified regardless of the measurement of the information needed to cause that UCA. When STPA has been performed a priori, the UCAs inform the amount of harm to physical information and data that are needed to initiate the UCA. The hazards identified by STPA can inform the type of PIH caused by the UCA (e.g., pressure, temperature, and flow rate changes).

VI. INFORMATION HARM TRIANGLE

Because of the high level of uncertainty in determining likelihood and consequences of a cyberattack, the current standard approaches^{5,9} require highly capable operators to design, implement, and sustain an effective program and expert-level staff competency to establish, install, and maintain security controls. These requirements for capability and competency highlight the need for a simple intuitive concept to gain insights into how to design effective defense in depth for OT systems.

The key postulates of the IHT are the following:

1. Data can only be interpreted and understood by digital systems.
2. Cyberattacks can only directly cause DH.
3. Physical consequences are directly caused by PIH.
4. Cyberattacks that result in physical consequences need an efficient transform function that converts DH to PIH (e.g., UCAs).

Further, since a cyberattack can only directly harm data and only OT systems can impact physical information,^d there is the potential for two types of orthogonal effects associated with a cyberattack. One type harms data, and the other harms physical information (i.e., information that exists

^cHAZCADS is a risk analysis approach that leverages the identification of UCAs as defined by STPA for analysis of digital systems.²⁵ The discussion regarding STPA is also applicable to HAZCADS, and the IHT is also compatible with HAZCADS.

^dOperational technology systems are those that control physical processes and therefore have greater potential for PIH. ICT systems may cause PIH (e.g., heat, sound, and electrical) but are unlikely with the magnitude necessary to effectively use the IHT concept.

independent of data in real time and space). Information harm is the deviation of information from its intended or true value. These effects are orthogonal because they exist in separate domains and cannot influence one another without a sufficient transform function.

When the magnitude of DH is sufficient to initiate a UCA, the UCA acts as a transform function, and PIH occurs. The risk of occurrence can be modified by measures that protect against DH or those that protect against PIH.

This paper proposes using the IHT to analyze the cybersecurity of OT systems. The purpose of the IHT is to simplify the understanding and evaluation of (1) the information harm arising from a cyberattack, (2) the physical harm arising from a cyberattack, and (3) the effect of security controls in reducing digital and/or physical harm. By analyzing the effects of security controls to both data and physical information, NPP cybersecurity teams can achieve defense in depth.

The IHT has the following three parts in which information is considered, as shown in Fig. 1:

1. *PIH*: Real plane (*x*-axis) representing harm that results in a physical hazard or loss.

2. *DH*: Complex plane (*y*-axis) representing potential for harm, assuming there is a transform function (e.g., UCA) that can be initiated by cyberattack.

3. *Apparent information harm (AIH)*: The sum of the orthogonal components that meet at a vertex representing the apparent harm generated by a UCA causing a harmful consequence. The UCA is represented as the upper vertex of the IHT.

A simplified sequence of harm effects from cyberattack and the effects of protective measures are shown in Fig. 2. The UCA transforms DH to PIH by causing changes to physical processes if DH thresholds are exceeded. Note that the simplified sequence does not show the potential for cyberattacks to harm measures.

VIA. Cybersecurity Implications for DH

The meaning of the data in the lower layers is interpreted and discovered within the digital system, which has large impacts for cybersecurity. If this interpretation and discovery are done incorrectly, or are maliciously altered, the meaning may be fundamentally altered. One example of DH is manipulation of data in a database.

In OT systems, there are three potential cases: (1) autonomous digital systems where the control system is an application that performs all critical actions automatically

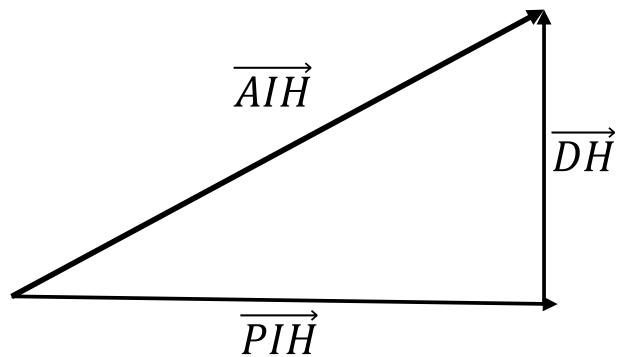


Fig. 1. Information Harm Triangle.

and without human interaction, (2) semiautonomous control systems where the control system performs functions with partial human involvement, and (3) supervisory control systems where human interaction is necessary to perform mandatory actions.

In the first case, there is no need for the system to provide physical information in the form of a GUI or CLI other than for routine maintenance or updates. The physical information of the process is converted to data, where processing and a control action are undertaken, thereby generating the required physical signals demanded by the control action (e.g., energize actuators).^e

In the second and third cases, these systems need to communicate the data to a human operator. In these cases, the GUI or CLI provides physical information (i.e., physical light information) to exchange information with the nondigital observer (i.e., human operator), but the information conveyed for which the observer is to derive meaning is nevertheless based upon the interpretation and processing of the data that represent the encoded information of the physical information within and/or captured by the OT system (e.g., at the lower levels of the OSI model).

VI.B. Cybersecurity Implications for PIH

In this paper, DH will be depicted as the relative amount of harm needed to initiate a UCA and additional amount of DH needed to deceive the operator. The PIH will be similarly depicted, with the maximum limit to physical harm that could result from the UCA shown.

In essence, the destruction of equipment or disruption of a process is the meaning conveyed by the harm to the

^e Although an autonomous system may not need to provide physical information to an operator to perform its functions, presentation of the physical information may be desirable for monitoring purposes.

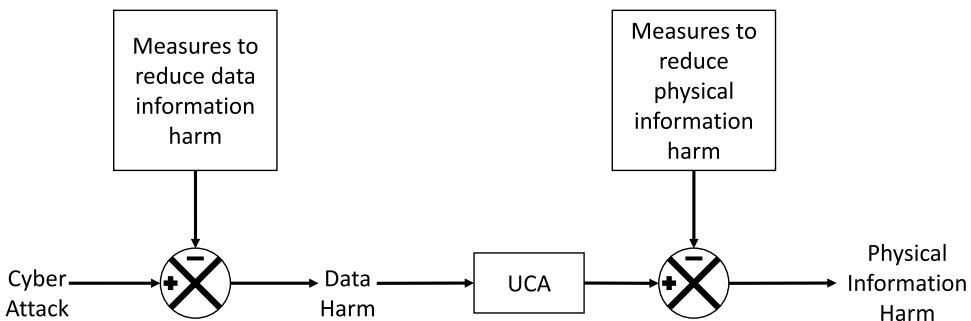


Fig. 2. Information Harm Triangle relationships.

physical information. The meaning of this information harm can be determined through analysis techniques such as STPA to identify UCAs. UCAs are the means by which information harm to the system is transformed into consequences that have significance to nuclear safety and security.

VI.C. Measuring Information Harm

One current challenge of using the IHT is defining the units of information harm. Potential approaches include Shannon entropy,^{26,27} Kolmogorov-Chaitin information theory,^{28,29} and machine learning approaches leveraging Euclidean distance measures.³⁰ This is an area of ongoing research that will be addressed in future work. For this reason, the case studies in Sec. VII are unitless and serve to illustrate the general application of the IHT.

VII. CASE STUDIES

The utility of the IHT is demonstrated using two previous applications of STPA to the digital I&C system of a generic pressurized water reactor (PWR). The first STPA application and IHT case study is conducted for the pressurizer system. The second STPA application and IHT case study examines the main steam isolation valve (MSIV).

VII.A. Case Study 1: Pressurizer System

The first STPA application analyzes a simple pressurizer system (shown in Fig. 3) (Ref. 31). The pressurizer digital controller is responsible for controlling the heaters and spray valves, which in turn control the level in the pressurizer and the pressure in the reactor coolant system. The controller not only relies on level, temperature, and pressure sensor feedback (or physical information) from the pressurizer but also relies on interfacing system information such as the residual heat removal and reactor vessel

level indicating system. A complete pressurizer STPA analysis is beyond the scope of this paper, but for the purposes of demonstrating the insights gained from STPA, a reduced and simplified set of UCAs is provided in Table II.

The UCAs have several attributes that are important to the IHT. Consider UCA 1.B.1; the physical information is “pressure is low.” This low pressure is an observable quantity, but during the collection and/or transmission of the observed quantity, the physical information may be lost or manipulated. This physical information is the only information available to the pressurizer controller such that pressure information can be translated to meaning. Also, consider the case of manipulated controller data or denial/degradation of service. These threats to the controller data can cause physical information—even if it is received accurately and precisely—to take on a different meaning such that a UCA is sent to the spray valve. Thus, the UCAs result in a hazard that can be explicitly related to how information alteration can result in a UCA. Note that the hazards presented in Table II do not represent a traditional sense of harm such as core damage or operator harm. Rather, these hazards result in an economical consequence from loss of revenue, regulatory consequence from loss of confidence, and potential societal consequences from loss of power.

UCA 2.D.1 is chosen as the case example. For simplicity, the initial analysis considers no cybersecurity controls other than a password, with no lockout of the “program” function of the pressurizer controller.

VII.A.1. Data Harm

The level of DH to initiate UCA 2.D.1 is very low. A simple, credible scenario would be to raise the setpoint within the logic that would turn off the heater. In the example, the normal setpoint for a Westinghouse PWR is 2235 psig (Ref. 32), and the upper limit of the setpoint span is 2500 psig (Ref. 32). If the adversary aimed to

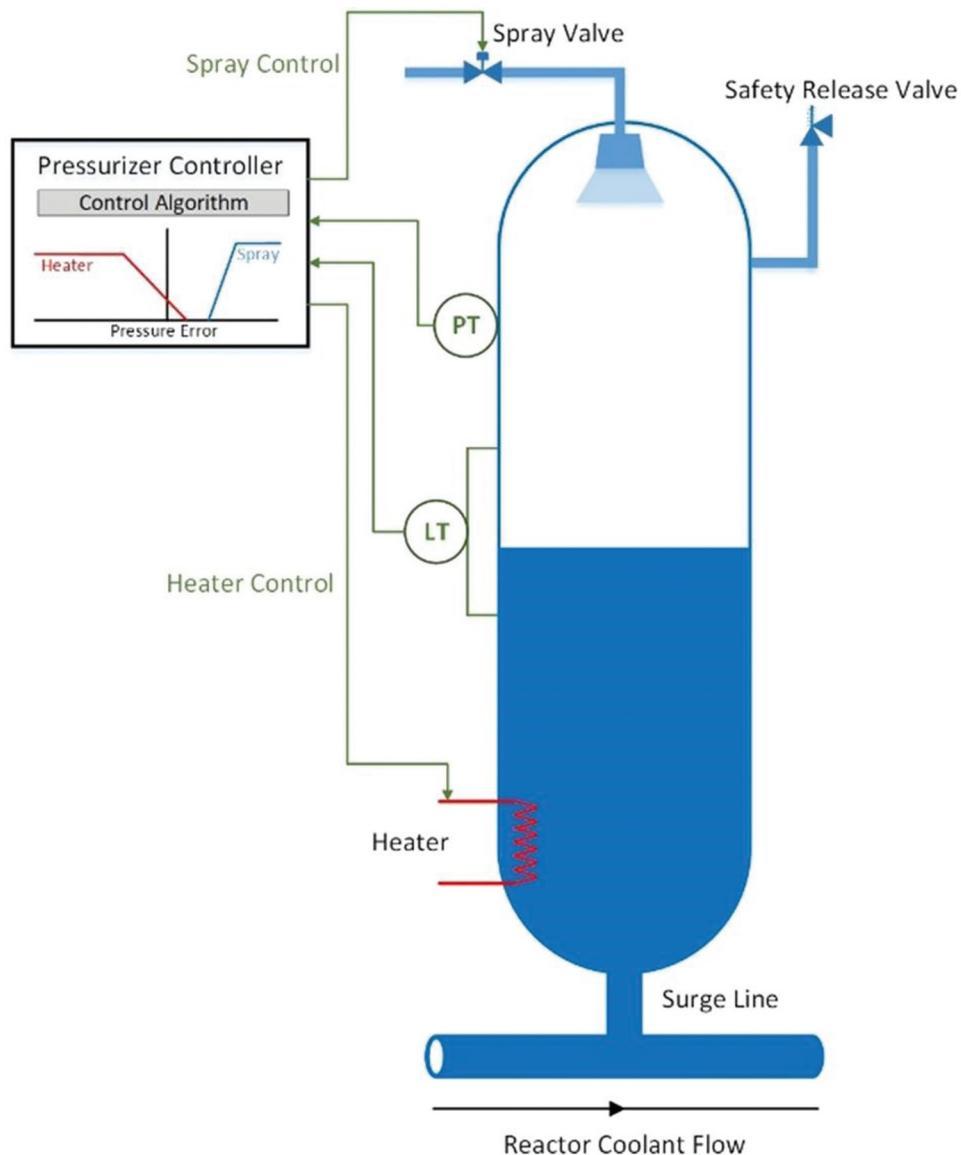


Fig. 3. Simple pressurizer system.

initiate UCA 2.D.1 in a manner that would maximize harm, it would require the ability to increase the setpoint to a limit beyond 2500 psig.

In a simple hypothetical attack scenario where alteration of setpoints requires only access to the system and knowledge of the password, a very low level of DH is incurred. It is important that the harm to the confidentiality of the password not be considered here. Only integrity or availability impacts are considered in the IHT.

This simple attack will likely be detected by the operator (i.e., the operator will ascertain the meaning of pressurizer pressure exceeding 2235 psig), and the operator would take manual action to intervene and turn the heater off. Therefore, the adversary will be required to prevent or impede operator response in correcting the

setpoint change or manually turning the heater off, thereby eliminating the presence of UCA 2.D.1. This increases the complexity of the attack, and more importantly, the amount of DH to cause the UCA increases significantly. The adversary must not only change the setpoint but also succeed in the following: (1) hide the setpoint change and any associated alerts and (2) spoof any operator interfaces in a manner that misleads the operator into incorrectly assessing and responding.^f

^fIn this example, the operator is treated as a security measure. An alternate approach is to consider the spoofing to be DH that causes the operator to commit an additional UCA in addition to UCA 2.D.1.

TABLE II
PWR Pressurizer UCAs and Hazards³¹

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing Causes Hazard	Incorrect Duration Causes Hazard
CA 1: Open spray valve.	UCA 1.A.1: Pressurizer controller does not send open signal to spray valve when pressure is high [H1.1].	UCA 1.B.1: Pressurizer controller sends open signal to spray valve when pressure is low [H1.2, H2]. UCA 1.B.2: Pressurizer controller sends open signal to spray valve when level is too high [H1.3].	UCA 1.C.1: Pressurizer controller sends open signal to spray valve after pressure becomes too high [H1.1].	UCA 1.D.1: Pressurizer controller stops sending open signal to spray valve before reaching fully open [H1.1].
CA 2: Heaters energized.	UCA 2.A.1: Pressurizer controller does not send energizing signal to heaters when pressure decreases [H1.2, H2].	UCA 2.B.1: Pressurizer controller sends energizing signal to heaters when pressure is high [H1.1].	UCA 2.C.1: Pressurizer controller sends energizing signals to heaters after pressure becomes too low [H1.2, H2].	UCA 2.D.1: Pressurizer controller applies energizing signal to heaters after pressure reaches setpoint [H1.1].
Hazards H1.1: Reactor trip on high pressure H1.2: Reactor trip on low pressure H1.3: Reactor trip on high level H2: Engineered safety features actuation				

The attacker would likely require changes to either the application software or kernel mode components to hide the setpoint change and mask any alerts. To mislead the operator, the attacker would also likely capture data between the programmable logic controller and the operator interfaces during normal operations and save it or regenerate it during the time for which UCA 2.D.1 is occurring (to hide the actual state of the physical system from the operator). This substantively increases the level of DH required to cause the UCA. The IHT for these two scenarios is shown in Fig. 4.

VII.A.2. Physical Information Harm

Given the example, and assuming that there are no measures to prevent or protect against PIH (i.e., there is no overpressure release valve), the effect of UCA 2.D.1 would be for the heater to continue to add heat to the primary loop, thereby increasing pressure. This addition of

heat impacts the physical information (temperature and pressure) in a harmful way and will continue to increase harm to this information until the new “malicious” pressure setpoint is reached. If the pressure boundary at the pressurizer instrument nozzles or heater sleeves is exceeded, harm to the physical information is increased substantially.

VII.A.3. Data Security Controls

Most common data controls are those measures that prevent, detect, or protect against harm to data. These are typically technical control measures. Firewalls, anti-malware scanners, and cryptographic mechanisms are examples of data controls as they all operate on data. However, there can also be controls that limit the amount of DH to be caused.

In the example above, perhaps the hypothetical system contains a control in the form of a design feature

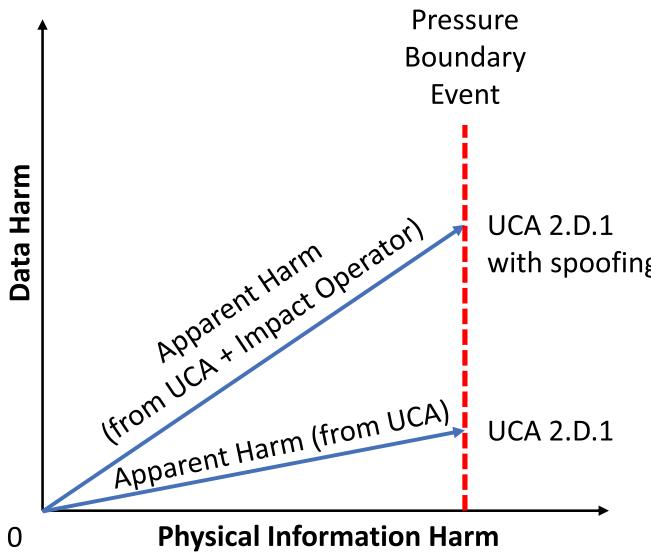


Fig. 4. Information Harm Triangle for UCA 2.D.1 for attacks with and without spoofing.

whereby the capability does not exist to record and archive the data needed to spoof the operator. This would limit the DH that is possible on the system and prevent the UCA 2.D.1 plus spoofing scenario; however, it would not limit the magnitude of DH necessary for the UCA 2.D.1-only scenario. However, this strict constraint on capability would increase the challenge of the adversary to mitigate or prevent the operator from responding to UCA 2.D.1. This effect is shown in Fig. 5.

VII.A.4. Physical Information Controls

A more applicable control for most pressurizer systems is the overpressure relief valve that ensures the pressure boundary is always maintained. This is generally a mechanical device that opens to relieve excess pressure in the primary loop.

Physical information controls protect against PIH. The overpressure relief valve is a control that limits the level of physical harm that can be caused by UCA 2.D.1 regardless of the amount of DH. This effect is shown in Fig. 6.

It is readily apparent that the PIH limit is much less than that necessary to cause a pressure boundary event, thus eliminating both the potential for large consequences associated with both scenarios, UCA 2.D.1 only, and UCA 2.D.1 plus spoofing. However, since the overpressure release valve relies on physical information to impose this limit on harm, it is imperative that physical tampering or sabotage of this device not occur to disable its effect.

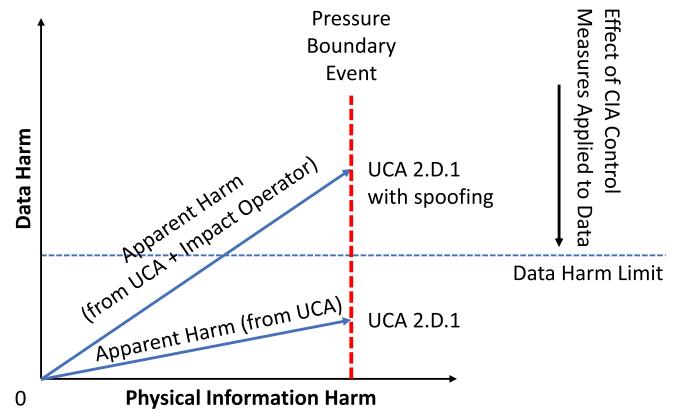


Fig. 5. Information Harm Triangle for UCA 2.D.1 indicating the effect of data control measures.

VII.A.5. Defense in Depth

The use case demonstrates that the IHT provides insights into defense in depth as DH and PIH are orthogonal to one another. This allows for the design and implementation of independent measures that have orthogonal effects and therefore will provide resilience from an attack that either harms data or physical information. Orthogonal security controls provide resilience because they limit PIH through independent means.

More importantly from this use case, the data (capability constraint) and physical information (overpressure relief valve) security controls provide for two independent

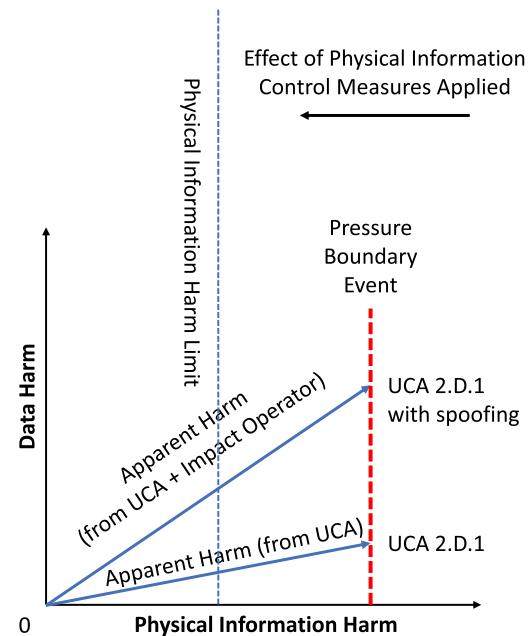


Fig. 6. Information Harm Triangle for UCA 2.D.1 with physical control measures.

measures that both guard against UCA 2.D.1 plus spoofing whereas UCA 2.D.1 is prevented by the overpressure relief valve.

Nevertheless, the increased difficulty of inhibiting or disrupting operator response to UCA 2.D.1 only, provides another layer of defense in depth with respect to the operator response that is not included in the IHT as the operator derives meaning from the information, as per the earlier discussion.

The insights derived from the IHT and this scenario have implications for risk. In this example, limitation of DH reduced the number of scenarios that could initiate UCA 2.D.1 from two to one. The IHT also showed that by limiting physical harm, the consequence of a cyberattack initiating UCA 2.D.1 can be decreased from a pressure boundary event to one where the pressure boundary integrity is maintained.

VII.B. Case Study 2: Main Steam Isolation Valve

The second case study focuses on the systems involved in closing the MSIV (Ref. 33). The MSIV is located on the main steam line from the steam generator (SG) (Fig. 7). The MSIV is normally open but can be closed to isolate the SG from the secondary system. Isolation of the SG may be necessary for several reasons: (1) if there is a break in the main feedwater pipe to the SG, (2) if a steam generator tube rupture (SGTR) leaks primary coolant into the secondary system, and (3) if there is a break in the main steam line exiting the SG

(Ref. 34). The UCAs of this STPA study are summarized in Table III.

UCA 3.C.2 is chosen as the case example. The execution of UCA 3.C.2 is considered in the context of an SGTR.

VII.B.1. Data Harm

The level of DH to initiate UCA 3.C.2 is high. In the event of an SGTR, the operator will be required by procedures to manually close the MSIV. Operators are highly involved in diagnosing and responding to SGTRs (Ref. 35). Indicators to the operator that an SGTR has occurred include the following³⁵:

1. High-radiation indications from the air ejection radiation monitor and blowdown line radiation monitors.
2. Low feedwater flow to the SG relative to the steam flow exiting the SG. The high water level in the SG from primary coolant leakage causes the feedwater flow to be reduced automatically.
3. Decrease in pressurizer pressure and level (large rupture) or mismatch in letdown and makeup rates (small rupture).

For this case study, these are assumed to be the only three indicators of SGTR.

To cause UCA 3.C.2, the adversary must cause sufficient DH to cause the controller (operator) to

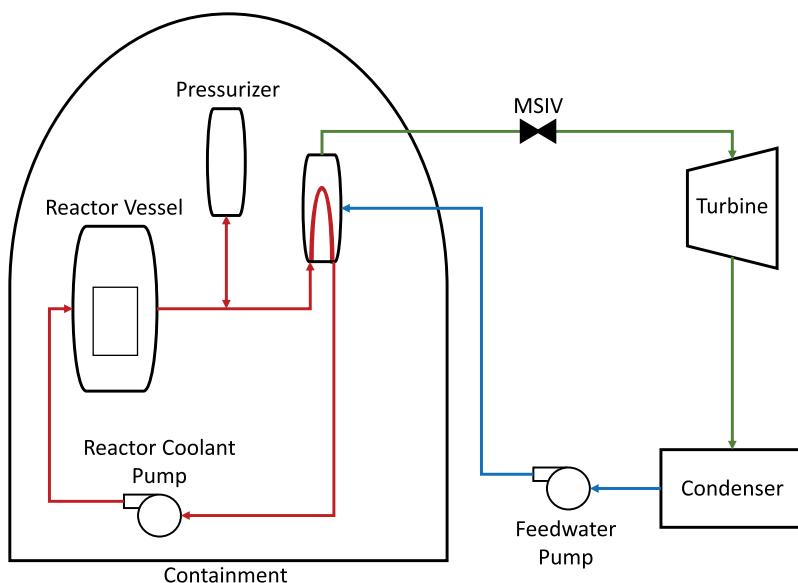


Fig. 7. Main steam isolation valve.³³

TABLE III
PWR MSIV UCAs and Hazards³³

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing Causes Hazard	Incorrect Duration Causes Hazard
CA 3: Close MSIV.	UCA 3.A.1: Close MSIV not provided when there is an SGTR, leak in main feedwater, or leak in main steam line [H3, H4, H5].	UCA 3.B.1: Close MSIV provided when there is no rupture or leak [H6]. UCA 3.B.2: Close MSIV provided when there is a rupture or leak if other support systems are inadequate [H3, H4, H5].	UCA 3.C.1: Close MSIV provided too early; SG pressure may rise, trigger relief valve, abrupt steam expansion [H4, H5]. UCA 3.C.2: Close MSIV provided too late after SGTR; contaminated coolant released into secondary loop, loss of primary coolant through secondary system [H3, H4, H5]. UCA 3.C.3: Close MSIV provided too late after main feedwater or main steam line leak [H3, H4, H5, H6].	N/A ^a

Hazards
 H3: Release of radioactive materials
 H4: Reactor temperature too high
 H5: Equipment operated beyond limits
 H6: Reactor shut down

^aN/A = This context is not applicable for this CA.

believe that the control action is not necessary. This involves spoofing a set of the aforementioned measurements in a manner similar to that described in Sec. VI.A. In contrast to the previous case study, here, spoofing is a requirement to cause the UCA. The more measurements the adversary can spoof, the more likely the operator is deceived and fails to provide the correct control action when needed.

In Scenario A, the adversary spoofs one indicator of SGTR to deceive the operator; in Scenario B, the adversary spoofs two indicators of SGTR; and in Scenario C, the adversary spoofs three indicators of SGTR. For simplicity, it is assumed that the DH to spoof each indicator is equal; therefore, the DH is

directly proportional to the number of spoofs conducted by the adversary (i.e., $DH_B = 2DH_A$; $DH_C = 3DH_A$). In vector notation, the three possibilities for UCA 3.C.2 are given by

$$A = (DH_A, PIH_A) ,$$

$$B = (DH_B, PIH_B) = (2DH_A, PIH_B) ,$$

and

$$C = (DH_C, PIH_C) = (3DH_A, PIH_C) .$$

VII.B.2. Physical Information Harm

In this example, the effect of UCA 3.C.2 would be for the primary coolant to continue to leak into the secondary water via the ruptured SG tube. This leaking of coolant causes PIH by increasing the radiation level in the secondary water until the MSIV is closed. If unchecked, radiation levels may exceed regulatory limits (i.e., PIH_{reg}).

In this example, PIH increase is constant versus time as the rate of primary coolant leaking into the secondary water is dependent on physical attributes such as (but not limited to) the size and location of the SGTR and the flow rate of the primary coolant that is unaffected by DH. Therefore, the longer the MSIV remains open during an SGTR, the more PIH occurs. The less evidence the operator has for SGTR, the longer it will take the operator to diagnose the event and close the MSIV. This evidence is based on data and therefore is directly impacted by DH for which the magnitude is dependent on the number of indicators that need to be spoofed.

For Scenario A, only one indicator is compromised, and the operator still has two indicators to diagnose SGTR. Most indicators show that SGTR has occurred, so the operator is likely to diagnose SGTR in a timely manner. Although the control action may be provided later than needed, radiation release is likely to be as low as reasonably achievable (i.e., PIH_{min}) and likely to remain within regulatory limits.

For Scenario B, two of the three indicators are spoofed. Since more of the indicators do not indicate SGTR, this scenario has the potential to be more challenging for the operator to identify the SGTR. However, given conservative decision making of the operator, it is highly likely that given a single alarming indicator of an SGTR, the operator will diagnose the SGTR and respond in a timely manner, especially if required by procedures. Although the control action is likely to be provided later than needed, radiation release is likely to be higher than that for Scenario A. This is dependent on the assumption that an operator will require more time to diagnose SGTR when two indicators are spoofed than when one indicator is spoofed. It is assumed that a skilled operator will still be able to diagnose SGTR with one indicator and PIH_B will likely remain within regulatory limits (i.e., PIH_{reg}).

Finally, in Scenario C, all indicators are spoofed, leaving the operator with no evidence to diagnose SGTR and correct the UCA. It is assumed that the operator will be unable to respond in a timely manner, resulting in the exceeding of regulatory limits, and in the worst

case would allow for the maximum PIH (i.e., PIH_{max}) as allowed for by the aforementioned physical attributes of the SGTR.

In all scenarios, the magnitude of PIH is dependent on the performance of the operator. The PIH in each spoofing scenario can therefore be viewed as a range of possible PIH values, with the lowest PIH corresponding to the fastest detection (i.e., best performance) by the operator and the greatest PIH corresponding to the slowest or no detection (i.e., worst performance) by the operator.

The amount of PIH is proportional to the time that the MSIV remains open during SGTR, which in itself is dependent on the duration that the UCA exists (i.e., the time it takes for the operator to perform the necessary action), not the amount of DH that occurs. However, these scenarios show that spoofing of an increasing number of indicators requires an increasing amount of DH, which results in increased likelihood that the UCA will exist for a longer duration (possibly until the maximum PIH is incurred).

The ranges of PIH are represented as

$$\text{PIH}_{\text{min}} \leq \text{PIH}_A \leq \text{PIH}_{\text{reg}},$$

$$\text{PIH}_A < \text{PIH}_B \leq \text{PIH}_{\text{reg}},$$

and

$$\text{PIH}_{\text{reg}} < \text{PIH}_C \leq \text{PIH}_{\text{max}}.$$

VII.B.3. Information Harm Triangles

If the amount of PIH were directly proportional to the amount of DH, the IHTs for all three cases would be similar triangles only differing in the magnitude of AIH (i.e., $\text{DH} = m\text{PIH}$, where m is the slope). However, the conclusions described in the scenarios above do not provide for similar triangles as the amount of PIH is not linearly proportional to DH. The analysis above makes apparent that the PIH caused by Scenario C is likely significantly greater than three times that of Scenario A, even though the DH of Scenario C is assumed to be exactly three times the DH of Scenario A. This is because the operator has no information to diagnose the SGTR in Scenario C but has two information sources to diagnose the SGTR in Scenario A. The IHTs in Fig. 8 represent three spoofing scenarios to cause UCA 3.C.2.

Given the above analysis, Fig. 8 provides an illustrative example of IHTs representing all three spoofing scenarios that cause UCA 3.C.2. The following illustrative IHTs in vector notation were selected to show the greatest amount of variability of the IHTs:

$$A = (DH_A, PIH_A) = (DH_A, PIH_{min}),$$

$$B = (DH_B, PIH_B) = (2DH_A, PIH_{reg}),$$

and

$$C = (DH_C, PIH_C) = (3DH_A, PIH_{max}),$$

given that

$$DH_B = 2DH_A$$

and

$$DH_C = 3DH_A.$$

VII.B.4. Data Security and Physical Information Controls

Data and physical information control requirements can be identified using the IHT and physical safety or operational requirements. In this example, there is a regulatory limit of radiation in the secondary water (i.e., $PIH_{reg} = B$). Therefore, it is desirable to limit PIH below that of PIH_{reg} to ensure that regulatory limits are never exceeded. This restriction corresponds to a PIH

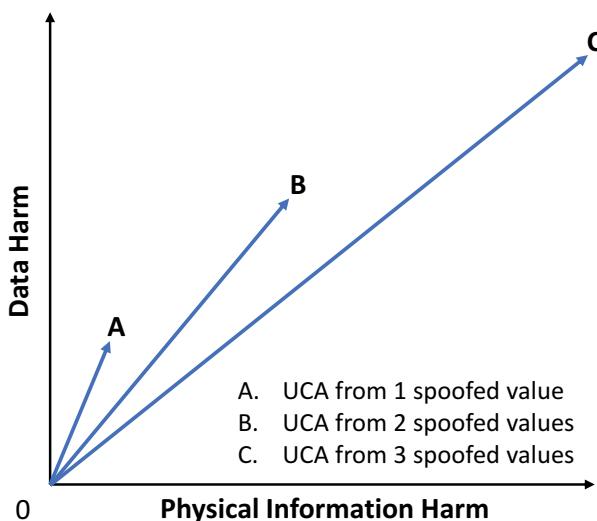


Fig. 8. Illustrative IHTs for UCA 3.C.2 from various levels of spoofing.

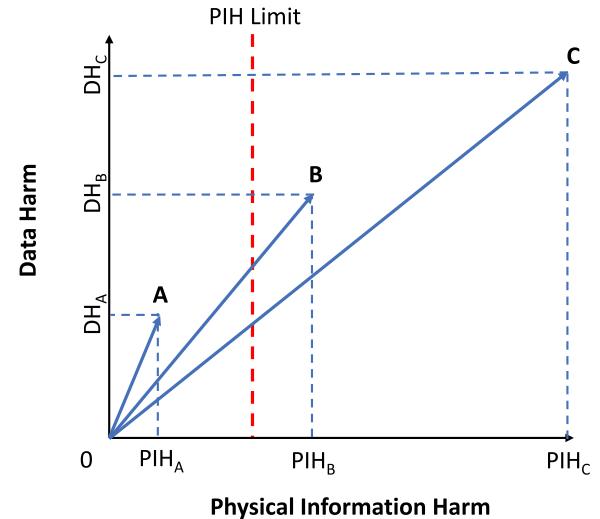


Fig. 9. Identification of data control requirements using PIH limits.

limit shown on the IHT in Fig. 9. This limit could be a separate system that provides automatic response to perform the required control action that is independent of the operator and the spoofed indications.

However, since this separate system may fail coupled with the potential for PIH_B and PIH_C to meet or exceed PIH_{reg} , data measures must be implemented to ensure that the adversary cannot cause enough DH to prolong UCA 3.C.2. DH_B is the minimum amount of DH required to meet PIH_{reg} ; therefore, effective data measures must ensure that the DH caused by the adversary is less than DH_B . Effective data controls against spoofing include those described in Sec. VII.A.3 (e.g., firewalls, anti-malware scanners, and cryptographic mechanisms). To achieve defense in depth, both data and physical information controls should also be implemented to directly ensure that PIH_{reg} is not met or exceeded.

VIII. CONCLUSION

The novel IHT approach aims to incorporate intuitive engineering concepts to simplify the development of defense-in-depth strategies for I&C systems at NPPs. The IHT postulates that all physical plant consequences are associated with PIH and are not associated with DH. The DH is either an initiating event or an event that inhibits or mitigates response of the operator (or autonomous systems) in taking the timely and corrective action.

The IHT further postulates that all physical plant consequences arise from UCAs and that STPA provides a method by which meanings are derived from

system information. These meanings are the UCAs and their descriptors. These meanings are then further extrapolated to plant consequences.

The basis of the IHT is that data are only of use to digital systems, which are the intermediaries or interpreters to humans or to autonomous applications that act on information encoded as data. Data and physical information do not interact with one another, meaning that data must be converted to physical information or physical information converted to data by a digital system acting as an intermediary. Once converted, the IHT representation preserves the separation of these components of information harm.

The IHT could also be used to analyze nonmalicious DH and the PIH that may result from the corresponding UCA. The analysis techniques presented here for security applications are also valid for reliability applications because of the common necessity that a digital system must act as the intermediary between data and physical information. Future work will examine applications of the IHT for reliability challenges in ICSs.

The IHT as proposed is a construct to guide further research into how to quantify harm. The key challenges are (1) how to measure both types of harm with a single unit; (2) systematic methodology to derive meaning from information; (3) investigation of boundary cases such as fault injection via physical means or physical sabotage acts that harm data; (4) analysis of the effects of control methods on preventing, detecting, limiting, and protecting against DH and PIH; and (5) further analysis of the effects of timing and sequencing on combinations of UCAs.

Acknowledgments

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, SAND2022-9116J.

This paper describes objective technical results and analysis. This paper was assisted by the reviews of John A. Sladek, Canadian Nuclear Safety Commission, and Andrew Hahn, Sandia National Laboratories.

Disclosure Statement

The authors report there are no competing interests to declare.

ORCID

Michael T. Rowland  <http://orcid.org/0000-0002-3623-8710>

Lee T. Maccarone  <http://orcid.org/0000-0002-2023-0255>

References

1. J. A. FARBER et al., "Using Kernel Density Estimation to Detect Loss-of-Coolant Accidents in a Pressurized Water Reactor," *Nucl. Technol.*, **205**, 8, 1043 (2018); <https://doi.org/10.1080/00295450.2018.1534484>.
2. S. VINOD et al., "Symptom Based Diagnostic System for Nuclear Power Plant Operations Using Artificial Neural Networks," *Reliab. Eng. Syst. Saf.*, **82**, 1, 33 (2003); [https://doi.org/10.1016/S0951-8320\(03\)00120-0](https://doi.org/10.1016/S0951-8320(03)00120-0).
3. R. ALGULIYEV, Y. IMAMVERDIYEV, and L. SUKHOSTAT, "Cyber-Physical Systems and Their Security Issues," *Comput. Ind.*, **100**, 212 (2018); <https://doi.org/10.1016/j.compind.2018.04.017>.
4. N. G. LEVESON and J. P. THOMAS, "STPA Handbook" (2018); https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf (current as of Dec. 15, 2021).
5. "Cyber Security Plan for Nuclear Power Reactors," NEI 08-09, Rev. 6, Nuclear Energy Institute (2010); <https://www.nrc.gov/docs/ML1011/ML101180437.pdf> (current as of Dec. 15, 2021).
6. *Code of Federal Regulations*, Title 10, "Energy," Part 73, "Physical Protection of Plants and Materials," Sec. 73.54, "Protection of Digital Computer and Communication Systems and Networks," U.S. Nuclear Regulatory Commission (2015); <https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html> (accessed Dec. 4, 2021).
7. "Security and Privacy Controls for Information Systems and Organizations," Special Publication SP 800-53, National Institute of Standards and Technology (2020).
8. "Guide to Industrial Control Systems (ICS) Security," Special Publication SP 800-82, National Institute of Standards and Technology (2015).
9. "Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity Requirements," IEC 62645, International Electrotechnical Commission (2019).
10. "Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Security Controls," IEC 63096, International Electrotechnical Commission (2020).
11. "International Nuclear I&C and Electrical System Standards Tables with URLs," Report No. 2020/002, World Nuclear Association (2020).

12. "Safety Classification for I&C Systems in Nuclear Power Plants – Current Status & Difficulties," Report No. 2015/008, World Nuclear Association (2015).
13. "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities," INF/CIRC/225/Revision 5, IAEA Nuclear Security Series No. 13, International Atomic Energy Agency (2011).
14. "Computer Security Techniques for Nuclear Facilities," IAEA Nuclear Security Series No. 17-T, International Atomic Energy Agency (2021).
15. "Computer Security of Instrumentation and Control Systems at Nuclear Facilities," IAEA Nuclear Security Series No. 33-T, International Atomic Energy Agency (2018).
16. "Design of Instrumentation and Control Systems for Nuclear Power Plants," Specific Safety Guide No. SSG-39, International Atomic Energy Agency (2016).
17. "Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants," IAEA Nuclear Energy Series No. NR-T-3.30, International Atomic Energy Agency (2020).
18. "Computer Security for Nuclear Security," IAEA Nuclear Security Series No. 42-G, International Atomic Energy Agency (2021).
19. "Security of Nuclear Information," IAEA Nuclear Security Series No. 23-G, International Atomic Energy Agency (2015).
20. "Committee on National Security Systems (CNSS) Glossary," CNSSI No. 4009, Committee on National Security Systems (2015).
21. R. MOREHOUSE, *Beginning Interpretive Inquiry*, 1st ed., Routledge, London, United Kingdom (2011).
22. "Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model," ITU-T X.200, International Telecommunications Union (1994).
23. "OSI Model: Layer Architecture," Wikipedia; https://en.wikipedia.org/wiki/OSI_model#Layer_architecture (accessed Mar. 6, 2021).
24. J. P. ANDERSON, "Computer Security Technology Planning Study," Vol. II, Appendix I, "Security Threats and Penetration Techniques," ESD-TR-73-51, U.S. Air Force (1972).
25. "HAZCADS: Hazards and Consequences Analysis for Digital Systems," Electric Power Research Institute (2018).
26. C. E. SHANNON, "A Mathematical Theory of Communication," *Bell Syst. Tech. J.*, **27**, 3, 379 (1948); <https://doi.org/10.1002/j.1538-7305.1948.tb01338.x>.
27. D. J. C. MACKAY, *Information Theory, Inference, and Learning Algorithms*, Vol. 7.2, Cambridge University Press, Cambridge (2003).
28. A. KOLMOGOROV, "Three Approaches to the Quantitative Definition of Information," *Int. J. Computer Math.*, **2**, 1–4, 157 (1968).
29. G. J. CHAITIN, "On the Simplicity and Speed of Programs for Computing Infinite Sets of Natural Numbers," *J. ACM*, **16**, 3, 407 (1969); <https://doi.org/10.1145/321526.321530>.
30. N. KRISLOCK and H. WOLKOWICZ, "Euclidean Distance Matrices and Applications," *Handbook on Semidefinite, Conic and Polynomial Optimization*, pp. 879–914, M. F. ANJOS and J. B. LASSERRE, Eds., Springer US, Boston, Massachusetts (2012); https://doi.org/10.1007/978-1-4614-0769-0_30.
31. M. T. ROWLAND and A. J. CLARK, "Application of the Information Harm Triangle to Inform Defensive Strategies for the Protection of NPP I&C Systems," *Proc. 12th Int. Topl. Mtg. Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021)*, Virtual Conference, June 14–17, 2021, American Nuclear Society (2021).
32. *Westinghouse Technology Systems Manual*, Sec. 10.2, "Pressurizer Pressure Control System," Rev. 1208, U.S. Nuclear Regulatory Commission; <https://www.nrc.gov/docs/ML1122/ML11223A287.pdf> (accessed Dec. 8, 2021).
33. J. THOMAS, F. L. DE LEMOS, and N. LEVESON, "Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants," NRC-HQ -11-6-04-0060, U.S. Nuclear Regulatory Commission (2012).
34. *Westinghouse Technology Systems Manual*, Sec. 7.1, "Main and Auxiliary Steam Systems," Rev. 0101, U.S. Nuclear Regulatory Commission; <https://www.nrc.gov/docs/ML1122/ML11223A244.pdf> (accessed Dec. 8, 2021).
35. *Westinghouse Technology Advanced Manual*, Sec. 4.6, "Steam Generator Tube Rupture," Rev. 0809, U.S. Nuclear Regulatory Commission; <https://www.nrc.gov/docs/ML1121/ML11216A088.pdf> (accessed Dec. 8, 2021).