DE GRUYTER OPEN

JAISCR, 2015, Vol. 5, No. 3, pp.205 – 220
10.1515/jaiscr-2015-0029

RISK ASSESSMENT FOR INDUSTRIAL CONTROL SYSTEMS QUANTIFYING AVAILABILITY USING MEAN FAILURE COST (MFC)

Qian Chen[1], Robert K. Abercrombie[2], Frederick T. Sheldon[3]

[1]*Engineering Technology, Savannah State University, Savannah, GA 31404 USA*

[2]*Computational Science and Engineering, Oak Ridge National Laboratory, Oak Ridge, TN 37831 USA*
Department of Computer Science, University of Memphis, Memphis, TN 38152 USA

[3] *Department of Computer Science, University of Memphis, Memphis, TN 38152 USA*

Abstract

[1] Industrial Control Systems (ICS) are commonly used in industries such as oil and natural gas, transportation, electric, water and wastewater, chemical, pharmaceutical, pulp and paper, food and beverage, as well as discrete manufacturing (e.g., automotive, aerospace, and durable goods.) SCADA systems are generally used to control dispersed assets using centralized data acquisition and supervisory control.

Originally, ICS implementations were susceptible primarily to local threats because most of their components were located in physically secure areas (i.e., ICS components were not connected to IT networks or systems). The trend toward integrating ICS systems with IT networks (e.g., efficiency and the Internet of Things) provides significantly less isolation for ICS from the outside world thus creating greater risk due to external threats. Albeit, the availability of ICS/SCADA systems is critical to assuring safety, security and profitability. Such systems form the backbone of our national cyber-physical infrastructure.

Herein, we extend the concept of mean failure cost (MFC) to address quantifying availability to harmonize well with ICS security risk assessment. This new measure is based on the classic formulation of Availability combined with Mean Failure Cost (MFC). The metric offers a computational basis to estimate the availability of a system in terms of the loss that each stakeholder stands to sustain as a result of security violations or breakdowns (e.g., deliberate malicious failures).

1 Introduction

Consider the typical ICS architecture for a Supervisory Control and Data Acquisition (SCADA) system, which relies on an Internet that often uses wireless technologies. In such architectures these systems are more vulnerable to the new security challenges including internal and external cyber-

[1]This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy (DOE). The United States Government (USG) retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for USG purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan).

attacks. ICS security objectives typically follow the priority of availability and integrity, followed by confidentiality. Some of the possible incidents may include: i) Blocked or delayed flow of data through ICS networks disrupting ICS operation; ii) Unauthorized changes to instructions, commands, or alarm thresholds damaging, disabling or shutting down equipment causing environmental impacts and affecting safety; iii) Inaccurate "spoofed" information may be sent to operators to disguise unauthorized changes and/or cause operators to initiate inappropriate actions leading to various negative effects (e.g., unavailability); iv) Software or configuration settings may be modified by malware leading to similar negative effects. There are a myriad of disruptive scenarios that could negatively impact the operation and/or availability of equipment protection systems, endanger costly and difficult-to-replace equipment, as well as safety systems that would endanger human life. Four brief examples of SCADA security incidents include [1-4]:

– In 2000, a disgruntled employee, gained unauthorized access into a compromised management system in Australia. As a consequence, millions of liters of raw sewage spilled into local parks and rivers while both pumps and warning alarms failed.

– In 2006, an overload of network traffic caused a number of reactor recirculation pumps to fail in the Browns Ferry nuclear plant in Alabama, USA.

– In 2009, both Chinese and Russian spies penetrated the US electric power grid leaving behind disruptive malware using network-mapping tools.

– In 2010, the Stuxnet worm was detected. It was the first worm known to attack SCADA (supervisory control and data acquisition) systems.

Such key critical infrastructures, of which SCADA systems form the core, need to be available at all times. Continuous availability requires strong measureable security processes to protect against cyber-attacks.

1.1 Related Approaches to this Work

Organizations typically implement a focused risk management process to identify and mitigate risks and assure their organizational missions. Managing those risks requires an integrated approach to: identify, deter, detect, and prepare for threats and hazards to national critical infrastructure; reduce vulnerabilities of critical assets, systems, and networks; and mitigate the potential consequences to adverse events [5]. Presidential Policy Directive 21 *(PPD-21) on Critical Infrastructure Security and Resilience*, builds on the extensive work done to date to protect critical infrastructure, and identifies 16 critical infrastructure sectors.

The European Network and Information Security Agency (ENISA) has generated an inventory of risk management and risk assessment methods [6]. A total of 13 methods were considered. Each method in the inventory has been described through a template. The template used consists of 21 attributes describing characteristics of a method. The inventory also provides for the comparison of the risk management methods and also the risk management tools [7].

Boehm et al., [8] discuss the nature of information system dependability and highlight the variability of system dependability afforded to stakeholders; the dependency patterns of their model are subsequently analyzed in [9] to determine how and to what extent it addresses the issues raised by [8] in regards to the Stakeholder/Value definition of system dependability described in [10].

Herein we include an overview of SCADA systems (Section II). Section III introduces the risk assessment process to enhance the security of SCADA systems. We then present the mean failure cost (MFC) metric as a measure for security (Section IV). Section V illustrates a real example taken from a utility in Tunisia. Section VI focuses the generic concept of mean failure cost to the specific quest of measuring availability for SCADA systems (Section VII). We conclude by describing this proposed measure and discussing some differences with more common formulations.

2 SCADA Systems Background

The IEEE standard C37.1-2007 [11] defines SCADA as a system operating with coded signals over communication channels so as to provide control of remote terminal units (RTU) equipment. The supervisory system may be combined with a data acquisition system by adding the use of coded signals over communication channels to acquire information about the status of the RTU equipment for display or for recording functions.

2.1 SCADA Architecture

The SCADA system consists of several components that communicate with each other as illustrated in Fig. 1. Based on several studies such as those described by Igure [12] and Hentea [13] that have focused on SCADA architecture, we use the following classification:

2.1.1 Hardware SCADA Components

- Corporate network segment: operates in the same way as a general Information and Communications (ICT) network, thus, performs the same operations such as e-mail-communication, requiring an Internet connection.

- SCADA network segment: containing servers, workstations, Human Machine Interface (HMI) and data historian(s), among others.

- Field devices segment: containing three types of fields, namely programmable logic controllers (PLCs), remote terminal units (RTUs) and intelligent electronic devices (IEDs).

2.1.2 Software SCADA Components

The software components combine [12, 13]:

- Protocols: some of these protocols are common and found in general ICT which are TCP and UDP, while some are unique and only found within specific industrial settings, such as CIP, Modbus, Fieldbus, DNP3 and PROFIBUS.

- Operating systems: current SCADA systems use commonly Windows and the older Windows NT software.

2.1.3 SCADA Communication Components

As discussed in [12, 13], communication links utilize:

- Physical connections: include optical fiber, radio, satellite, etc. SCADA are typically connected to the Internet through a gateway.

- Logical connection: SCADA typically use standard logical network topologies, which circulate data through physical links.

Table 1. Results of the simulations in static environment

Priority	Information Control Technology (IT/ICT)	SCADA
1.	Confidenitality	Availability
2.	Integrity	Integrity
3.	Availiability	Confidentiality

2.2 Security Issues on SCADA System

Availability, integrity and confidentiality (listed in priority order; usually referred to, in an IT context, as CIA reverse order) are the core requirements for cyber-physical security. Security professionals and students commonly refer to these three fundamental principles of security as the CIA triad. Based on an extensive literature analysis, the Information Assurance & Security (IAS) Octave has been developed and proposed as an extension of the CIA-triad [14]. The IAS Octave includes confidentiality, integrity, availability, privacy, authenticity & trustworthiness, nonrepudiation, accountability and auditability. The importance of security requirements depends on the nature/role of the system. The requirements in SCADA systems are different and focus on health, safety, environment factors and operational availability/reliability. As shown in Table 1, the availability and integrity of information in SCADA systems are ranked ordered as number one and two in this regard. SCADA systems impose deterministic hard real time response requirements with fixed constrained on maximum communication time making them more vulnerable to disruption [1].

Connecting SCADA systems to the Internet or corporate Networks (one step removed) with-

out taking appropriate security measures creates an easy target and introduces many security risks. This is especially true because designing-in security and authentication protocols into SCADA has been considered unnecessary up until the recent past. Such legacy deployments have relied on the obscurity/anonymity of specialized protocols and proprietary interfaces as well as physical isolation [15]. Readily available rootkits that can subvert/exploit, for example, Windows or other platform for that matter, have made obscurity untenable. Such tools have become very sophisticated (e.g., Stuxnet) while at the same time lowered the skill-level and time needed to launch an attack. Other problems such as increasing complexity and interdependence of critical infrastructures [16], include the risks from loss of service (e.g., electricity, traffic or process control), financial sector services, property and environment damage, and potential loss of life [17].

2.3 Cyber Vulnerabilities in SCADA Systems

SCADA systems have many security vulnerabilities as described in [12]. The increasing interconnectivity of SCADA networks has exposed them to a wide range of network security vulnerabilities including those related to hardware, software, communication links or user authorization:

- Hardware vulnerabilities: Different SCADA components (i.e., SCADA master, RTUs and IEDs) address these vulnerabilities in specific ways. For example, RTUs have low processing power as well as limited persistent and working memory [18].
- Software vulnerabilities: The most common SCADA software vulnerabilities deal with disruption, data traffic interception and modification. Software can be removed intentionally by an attacker to cause a potentially serious failure [19]. Other vulnerabilities are related to operating system/firewall security [20]. The problem occurs because many nodes on SCADA systems run real-time operating systems (RTOS). These systems are more susceptible to Denial of Service (DoS) attacks compared with regular operating systems because even minor disruptions in messaging can lead to a significant loss of system availability as a consequence of this type of deterministic hard real-time operations [21]. Additionally, there are problems related to the lack of authentication and nonrepudiation mechanisms in older protocols used in these systems (Modbus or e.g., Inter-Control Center Communications Protocol [ICCP]) [12] resulting in lower resiliency to disruptive attacks. Simpler protocols are often preferred over more complex mechanisms for improved reliability, maintainability and performance.
- Communication links vulnerabilities: Phone systems may be used as means of connection to the outside world. As noted in [22], problems occur since these types of gateways likely do not include requisite security features.
- Authorization vulnerabilities: A common theme in the industry is the fear that unauthorized access to equipment may deny legitimate access to a user or other resource demands, causing failure of these systems to become unavailable or to operate unreliably (less responsively) as it is supposed to [23, 24]. Unauthorized access can also alter control logics or upload a zero line control code to destroy the system [20].

These vulnerabilities provide the opportunity for attackers to easily SCADA systems via mechanisms such as:

- Hacker can intrude, modify, destroy or exfiltrate data thereby causing disruption to systems and networks [17, 22] and/or DoS.
- Malware (i.e., viruses, worms, Trojans and spyware) may act on behalf of hackers causing much the same effects albeit less intelligently but perhaps less invasively waiting for the right time to exfiltrate, disrupt or corrupt data and/or communications (installation via back doors or key loggers representing hidden functionality [17, 23] which may be delivered via firmware updates). Current research is ongoing toward ensuring that no hidden functionality is delivered in hardware scoured from “trusted” vendors.
- Human accidental errors can have the same impact as malicious attacks [13] whose effects may

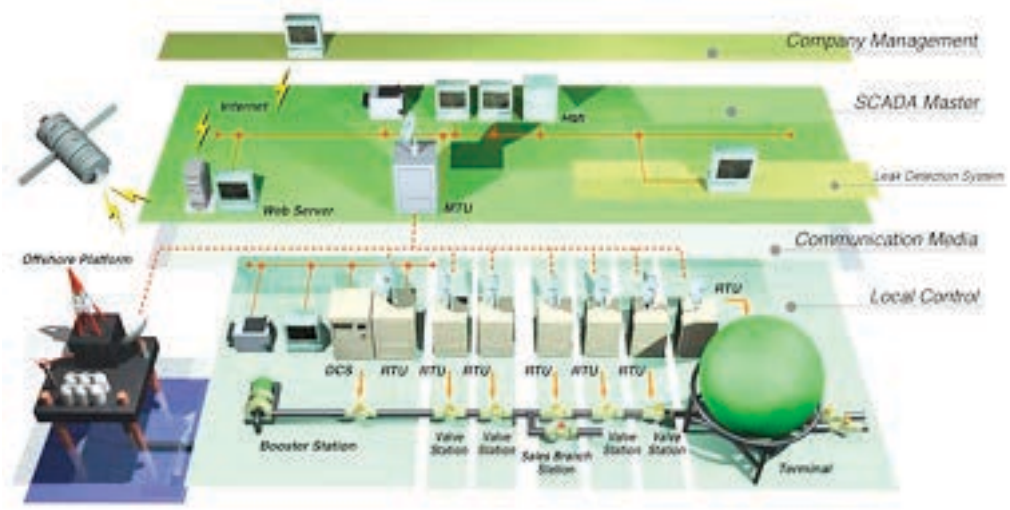

Figure 1. Example of Supervisory Control and Data Acquisition (SCADA) Architecture

in fact be mitigated by installing security type control measures for greater resiliency.

– DoS is a difficult/resource intensive attack to defend. In SCADA, legitimate devices and services are prevented or refused access to needed resources that ultimately disrupt the proper functioning of network based control systems. These are discrete-time, linear dynamic systems where control and measurement packets are transmitted over a linked network. The packets may be jammed or compromised by a malicious adversary.

– Malicious cyber attacks to control systems can be classified as either deception or DoS attacks. In the context of control systems, integrity refers to the trustworthiness of sensor and control data packets. A lack of integrity results in deception: when a component receives false data and believes it to be true (e.g., an incorrect measurement, time stamp, or sender identity). On the other hand, availability of a control system refers to the ability of all components to being accessible [12, 25].

In the control and verification community there is a significant body of work on networked control, stochastic system verification, robust control, and fault-tolerant control [25] aimed at intrinsically (built-in) protecting or deferring malicious deception/DoS attacks. The more added-on type of security control measures includes typical ICT security measures (cryptographic techniques, passwords, firewalls, intrusion detection systems, virtual private network, antivirus, access control, etc.) [1, 12, 13, 21, 26]. Moreover, other SCADA measures have been proposed: first embodied in IEEE/ISO standards [11] and NIST Guidelines [27], and secondly enhancing SCADA protocols by placing at each end of the communication media encryption and decryption technologies, wrapping SCADA protocols without making changes to the protocols using external cryptographic and security protocols (SSL/TLS, IPSec) or modifying the protocols fundamentally [1, 25]. A significant challenge, however, is the decision about which of these measures is the appropriate mechanisms considering risk, impact and cost. Still, these techniques do not address quantifying the likelihood of success (and impact) of those diverse sets of security threats.

When quantifying risks to the organization let's not forget to include brand damage, loss of revenue, share price reduction and in severe cases within the context of cyber physical, loss of life [26]. The reality of the aforementioned threats (Section I, Items 1-4) has emerged over the past several decades [1-4]. While SCADA systems were originally designed to be closed systems, the number of systems driving physical infrastructure connected to the Internet and interlinked with other systems is increasing each year [28]. From these limits derive the need to develop pertinent threat and risk modeling approaches. A threat/risk model can help to assess the probability, the potential harm, the priority of

attacks, and thus help to minimize or eradicate the threats and needed to formalize the perceived risk [21, 29].

3 Risk Assessments

Decades ago, security of the first and second generations of SCADA systems were overlooked because of vendor-proprietary environments. Cyber attackers exploiting publicly known information security vulnerabilities breached those air-gapped SCADA systems when SCADA systems were first connected to the Internet. Most vulnerabilities, such as vulnerabilities of operating systems, off-the-shelf applications and communication protocols have been patched in IT systems. Therefore, the first step to enhance security of SCADA systems is to mitigate risks of known threats and vulnerabilities by producing and implementing recommendations of security controls and alternative solutions periodically [27, 30, 31].

Due to the limitation of resources, organizations need to compare the cost of implementing security controls and solutions with the losses of cyber attacks before they implement the recommended security controls. As shown in Formula (1), cyber security risk is a function of the probability of a given threat source exploiting known vulnerabilities and the resulting impact of a successful exploitation of the vulnerability [27]:

$$Risk = \frac{Vulnerability * Threat * Impact}{Probability} \qquad (1)$$

To manage risks of SCADA systems, an iterative and continuous risk management cycle including risk framing, risk assessment, risk responses, and risk monitoring can be structured [32].

- Risk Framing: this element describes environment in which recommended security controls and alternative solutions are made. In this step organizations make assumptions about threats, vulnerabilities, impacts, and the probability (likelihood) of occurrence. After that, organizations should identify their constraints and the level of acceptable risks. Trust relationships and trade-offs between different types of risks must be identified as well [33, 34].
- Risk Assessment: similar to the risk assessment for IT systems [32], this element is for SCADA systems to identify threats, vulnerabilities, impact and probability.
  - The first step of this element is to define the scoop of effort. In this step, the SCADA system boundaries are identified. System-related information such as hardware, software, system interfaces is collected. System functions and system/data criticality and sensitivity are identified as well.
  - The second step is to identify the potential threat-sources to successfully exercise vulnerabilities. The SCADA system's threat statement (the list of potential threat-sources) will be tailored to its environment.
  - The third step is to identify SCADA system vulnerabilities. In this step vulnerability sources associated with threats and security requirements checklists are generated. System security testing is a proactive method to identify the system vulnerabilities.
  - The fourth step is to analyze the security controls that have been implemented or are planned for implemented. Therefore, the overall probability (or likelihood) rating that a potential vulnerability would be exercised by threats can be derived in step five.
  - The sixth step is to determining the adverse impact (loss of availability, integrity, and confidentiality) resulting from the compromised system by potential threats. The magnitude of impact is determined by this step as well.
  - The seventh step is to assess the level of risk to the SCADA system using Formula (1). The output of this step is the risk level (i.e., high, medium, and low).
- Risk Response: this element provides risk responses to address SCADA system risks once that risk are assessed [33, 34]. Considering the effectiveness of recommended options, legislation and regulation, organizational policy, operational impact, and safety and reliability [32], the recommended security controls and alternative solutions could be evaluated. This element also recommends the organization to accept, avoid,

mitigate or transfer risks based on the results of risk assessment.

– Risk Monitoring: this element monitors that security controls have been implemented. It also verifies that overall SCADA system risks have been reduced to an acceptable level by implementing recommended controls. Any changes that impact risk to the SCADA system are identified as well. In addition, proposed monitoring processes to assess the risk and its response are defined.

4 Mean Failure Cost (MFC) as a Measure of Security

In **[35]**, the concept of Mean Failure Cost (MFC) was first introduced. The concept was refined through a series of applications **[21, 36, 37]** and has been applied to several domains which include mission assurance **[38, 39]**, failure impact analysis in Advanced Metering Infrastructure (AMI) **[40, 41]**, risk assessment **[42, 43]**, game theoretic simulation **[40, 44]**, cybersecurity modeling in the cloud **[45]**, and SCADA environments **[46, 47]**. This value-based metric (MFC), when applied quantifies the security of a computing system by the statistical mean of the random variable that represents for each stakeholder, the amount of loss that results from security threats and system vulnerabilities. Unlike other dependability measures which are intrinsic to the system, MFC depends not only on the system but also on the stakeholder, and takes into account the variance of the stakes that a stakeholder has in meeting each security requirement. MFC can be extended beyond security to capture other aspects of dependability, such as reliability, availability, safety, since it makes no distinction about what causes the potential loss. Furthermore, whereas other dependability models distinguish between several levels of severity in security failures, we have no need for such a classification since the cost associated with each requirement violation provides a way to quantify potential loss over a continuum. The MFC can be computed by means of the following formula:

$$MFC = ST \circ DP \circ IM \circ PT \tag{2}$$

Where,

– ST: The stakes matrix filled by stakeholders according to the stakes they have in satisfying individual requirements. It is composed of the list of stakeholders and the list of security requirements. Each cell expressed in dollars (i.e., monetary terms) and it represents loss incurred and/or premium placed on the specific requirement.

  – ST (H_i,): Is the stake that stakeholders H_i has in meeting requirement R_j.

– DP: The dependency matrix is filled in by the system architect (i.e., cyber security operations and system administrators) according to how each component contributes to meet each requirement; each cell represents probability of failure with respect to a requirement given that a component has failed.

  – DP (R_j, C_k): The probability that the system fails to meet requirement R_j if component C_k is compromised.

– IM: The impact matrix is filled by analysts according to how each component is affected by each threat; each cell represents probability of compromising a component given that a threat has materialized, it depends on the target of each threat, likelihood of success of the threat.

  – IM (C_k, T_h): The probability that Component C_k is compromised if Threat T_h has materialized.

– PT: The vector of threats characterizes the threat situation by assigning to each threat category the probability that that threat will materialize over a unitary period of operation time.

  – P(Ti): The probability that threat Ti materialized within a unit of operation time.

5 Quantifying Security: The STEG Case Study

Herein we assessed a full-scale enterprise SCADA system within the domain of an electric power utility. We studied the case of the Tunisian Company of Electricity and Gas (STEG: Socit Tunisienne de l'Electricit et du Gaz) [47].

STEG's role is to develop and maintain the country's natural gas network, thus realizing the electrification and associated natural gas infrastructure. The case study analyzed service delivery and associated administrative controls for electric power flow during a one-year study period. All necessary data, including security requirements, stakeholders, components and the various threats (and actual attacks) were collected by interviewing STEG Managers/Subject Matter Experts. The information collected was used to parameterize the MFC model.

5.1 The Stakes Matrix (ST)

We populated the Stakes Matrix (Table 2) from data collected via interviewing the security team. Each cell is monetized in terms of dollars ($USD) and represents the loss and/or premium placed on a given requirement.

5.1.1 The stakeholders of SCADA

To simplify the analysis, we consolidated the stakeholders into 4 categories:

- Maintenance personnel and operational personnel responsible for the maintenance and the performance of all system operations.
- System administrators responsible for the administration of SCADA system.
- Technical staff responsible for installing software and ancillary materials on the system.
- Controllers of SCADA serving a vital role in maintaining the safe and efficient systems operation (e.g. quality assurance/control).

5.1.2 SCADA security requirements of the STEG Utility

We considered the security requirements concerns that are often cited in the SCADA systems:

- Integrity
- Availability
- Confidentiality
- Authenticity

Table 2 provides represented the populated Stakes Matrix with the Stakeholders and their respective security requirements.

5.2 The Dependency (DP) Matrix

The dependency (DP) matrix presented in Table 3 is populated by cyber security operations and system administrators according to how each component contributes to meet each requirement.

5.2.1 The components of system

To populate this matrix we used the values provided via interviews with STEG:

- Remote Terminal Unit (RTU)
- Programmable Logic Controller (PLC)
- Master Terminal Unit (MTU)
- Operating system (OS)
- I / O server (IOS)
- The database server (DBS)
- Communication (C)

5.3 The Impact Matrix (IM)

The impact matrix (IM) presented in Table 4 is populated, through an interview process using subject matter experts (SME). Each cell contains the estimated probability that a component becomes compromised given that a threat has materialized. Naturally, the likelihood of a successful compromise depends on the resiliency of a given target. Though this dependency is not denoted separately in mathematical terms, the *interview process* is designed to take into account the condition (resiliency) of the target. In other words, the likelihood determination process should elicit and account for the existence of known vulnerabilities and other architectural features and/or dependencies that may cause coincident failure at the target. A coincident failure is when the target component is affected indirectly by other failed components. The SME must decide during an interview, for example, what is the likelihood that a DoS attack would affect a given target component including any residual effects from a DoS attack on neighboring coincident target components. Those residual effects

Table 2. Stakes (ST) matrix for SCADA System

ST		Security Requirements			
		Integrity	**Availability**	**Confidentiality**	**Authenticity**
Stakeholders	**Mantainence personnel**	$7,000	$9,000	$0	$0
	System Adminstrators	$2,000	$2,000	$2,000	$2,000
	Technical Staff	$4,000	$4,000	$0	$0
	Controllers	$8,000	$8,000	$6,000	$4,000

Table 3. The dependency (DP) matrix for the SCADA System

DP		Components							
		RTU	**PLC**	**OS**	**MTU**	**IOS**	**DBS**	**C**	**No Failure**
Security Requirements	**Integrity**	0.043	0.043	0.043	0.11	0.16	0.043	0.16	0.398
	Availability	0.043	0.043	0.043	0.11	0.16	0.043	0.16	0.398
	Confidentiality	0	0	0.08	0.08	0.08	0.08	0	0.68
	Authenticity	0	0	0.07	0.07	0.08	0.07	0	0.71

Table 4. The Impact Matrix (IM) for the SCADA System

IM		Threats									
		UAV	**MV**	**DoS**	**OSV**	**AV**	**SV**	**HAV**	**HV**	**CV**	**No Threats**
Components	**RTU**	0	0	0.02	0.14	0	0.01	10^{-5}	0.02	0.02	0.3499
	PLC	0	0	0.02	0.14	0	0.01	10^{-5}	0.02	0.2	0.3499
	OS	0	0.01	0.02	0.1	10^{-3}	0.2	0	0	0	0.669
	MTU	0.3	0.3	0.02	0.1	10^{-3}	0.2	0	0.02	0.02	0.399
	IOS	0.3	0.02	0.02	0.02	10^{-3}	0.2	0	0.02	0.02	0.399
	DBS	0.3	0.02	0.02	0.02	10^{-3}	0.2	0	0.02	0.02	0.399
	C	0	0.01	0.02	0.01	0	0.01	0	0	0.5	0.45
	No Failure	0.1	0.64	0.86	0.07	0.996	0.17	0.99998	0.9	0.04	1

can vary greatly depending on the type of attack method (strategy and tactics) for example attacks sourced by an intelligent human agent versus a malware agent (or some combination).

A SCADA system can be attacked by a large number of threats. For the STEG SCADA systems that were evaluated, the following categories of threats were considered:

- Unauthorized access (UAV)
- Malware (MV)
- Denial of service (DoS)
- Operating System vulnerability (OSV)
- Authentication (AV)
- Software vulnerability (SV)
- Human attacks (HAV)
- Hardware vulnerability (HV)
- Communications vulnerability (CV)

5.4 The Threat Vector (PT)

The vector of threat probabilities is presented in Table 5 and was established empirically over the study period. Each cell gives the probability a given threat will emerge and are generally mapped to requirements based on the various encountered threats. This probability does not distinguish between successful/unsuccessful compromise attempts, only emergence probability. $P(T_i)$ is the probability that threat T_i materialized within a unit of operation time (hour) and is accounted for within the various empirical perpetrator models designed to account for both observed and unobserved emergences. Factors such as known/unknown vulnerabilities and countermeasures are factored into the IM, not the PT.

Each cell represents the probability of realization of each threat, which depends on perpetrator models, empirical data, known vulnerabilities, and known counter-measures. $P(T_i)$: The probability that threat T_i materialized within a unit of operation time (in this case, one hour of operation).

5.5 The Mean Failure Cost of the STEG SCADA Enterprise

The vector of mean failure costs is calculated using the stake matrix, dependency matrix; the impact matrix and the threat vector each stakeholder of STEG SCADA system using the formula explained in Section IV formula (2). The results of the mean failure cost for each stakeholder are presented in Table 6 (Column: Initial MFC).

6 MFC AS A MEASURE OF AVAILABILITY

The classification of availability is somewhat flexible and is largely based on the type of downtime used in the computation and on the relationship with time (i.e. the span of time to which the availability refers). A wide range of availability classifications and definitions exist:

- Instantaneous (or Point) Availability
- Average Uptime Availability (or Mean Availability)
- Steady State Availability
- Inherent Availability
- Achieved Availability
- Operational Availability

One popular class is instantaneous (or point) availability, which is the probability that a system (or component) will be operational (up and running) at a specific time, t. However, let us consider average uptime availability. If the system if functioning properly from time *0* to t (i.e. it never failed by time t), then the probability of this happening is $R(t)$, the instantaneous reliability at time t.

The mean availability is the proportion of time during a mission or time period that the system is available for use. It represents the mean value of the instantaneous availability function over the period (0, T) and is given by:

$$\bar{A(t)} = \frac{1}{t}\int_0^t A(u)du \qquad (3)$$

Table 5. The Threat Vector for the SCADA System

Threats	probability/hour
Unauthorized access (UAV)	0.0042
Malware (MV)	0.004
Denial of service(DoS)	0.0025
Operating System vulnerability(OSV)	0.003
Authentication(AV)	0.007
Software vulnerabilities(SV)	0.004
Human attacks (HAV)	10 E-5
Hardware vulnerabilities(HV)	0.0007
Communications vulnerabilities(CV)	0.003
No Threats	0.97159

where, the system functioned properly since the last repair at time u, $0 < u < t$ [48]. For systems that have periodical maintenance, availability may be zero at regular periodical intervals. In this case, mean availability is a more meaningful measure than instantaneous availability. This definition of availability is commonly used in manufacturing and telecommunication systems as it considers both reliability (probability that the item will not fail) and maintainability (the probability that the item is successfully restored after failure).

Still, an additional metric is needed to know the probability that the component/system is operational at a given time, (i.e., has not failed or it has been restored after failure). *This metric is availability*. Availability can be addressed as inherent (steady state when considering only the corrective downtown of the system), achieved (similar to inherent availability with the exception that preventive maintenance downtimes are included), or operational (a measure of the average availability over a period of time and it includes all experienced sources of downtime, such as administrative downtime, logistic downtime, etc.) [48]. Thus, availability is a performance criterion for repairable systems that accounts for both the reliability and maintainability properties of a component or system. To summarize, availability measures the amount of time a system or component performs its specified function. Availability is related to reliability, but different. Reliability measures how frequently the system fails; availability measures the percentage of time the system is in its operational state taking into account all factors that affect downtime (both scheduled and non-scheduled).

We adopt the following calculation as it satisfies a global perspective of the STEG SCADA system. AVAIL_{Op} is the operational availability (4) is the ratio of the system uptime and total time. Mathematically, it is given by:

$$AVAIL_{Op} = \frac{Uptime}{OperatingCycle} \tag{4}$$

where, the operating cycle is the overall time period of operation being investigated and uptime is the total time the system was functioning during the operating cycle. The assumptions for determining availability have weaknesses:

- Independence with respect stakeholders
- Independence of the components, which have failed to ensure availability
- Independence of threats, which have caused the unavailability

Given these weaknesses, we propose to derive a new measure of availability through the MFC. We compare the advantages of this new formulation to the original MFC formula. MFC is a formulation generally used to determine the cost (to affected stakeholders) or a security violation (or other such failure) of the system under study. Here, we extended MFC to describe *a single attribute of dependability*, namely the mean failure cost of availability. First, we suppose that availability is decomposable and we consider that the MFC has the same definition and is presented by the following formula (5):

$$MFC = ST' \circ DP' \circ IM \circ PT \quad (5)$$

where, ST' is nxl; DP' is lxh; IM is hxp; and PT is px1. We consider a system A, where $S_1, S_2, S_3 \ldots S_k$ are the stakeholders and C_1, C_2, $C_3 \ldots C_k$ are the system components as above (Section IV) with *operational availability* $AVAIL_{Op}$ as the sole criteria.

- ST' is an extension of the Stakes Matrix defined for MFC, where we consider the availability requirement as the only column vector in Table 2. ST' represents the stake of stakeholder Si for availability attribute.
- DP' is an extension of the Dependency Matrix, in which we consider the availability as a row vector (i.e., the availability row from Table 3).
  - DP' represents the set of probabilities for which a failed component, Ck will cause a violation of the availability requirement. The last column represents the case when no failure occurs (i.e., probability System A will be availability) as shown in the Availability row from Table 3.

The resulting vector of mean failure costs is now calculated using the updated Stakes Matrix (ST'), updated Dependency Matrix (DP'), the original Impact Matrix (IM) and the original Probability Threat (PT) vector for each STEG SCADA system stakeholder category using formula (5). The results are presented in Table 6 showing the MFC/stakeholder due to unavailability.

7 Application of MFC with emphasis on Availability

Availability of a system is defined as the ratio of up overt the total operating cycle as in (4) that the system is operational. If we want to redefine availability in value-oriented terms, we must consider three factors:

- The gain, per unit of time, is realized by stakeholder S from the system being operational; we denote this by G(S). If we consider the STEG enterprise (i.e., the utility) and let *S* be the utility, then G(*S*) represents the average revenue stream per unit of operational time.
  - The $G(S_i)$ for $1 \leq i \leq 4$ $G(S_i)$ (see Table 7 column labeled "Gain") is provided as data from interviews made with the STEG SMEs.
- The loss, per unit of time, incurred by stakeholder S_i from the system being down; we denote this by $MFC(S_i)$. If we consider the STEG enterprise and let S be the utility company, then $MFC(S_i)$ represents lost business, productivity and customer loyalty caused by downtime.
- AVAILop: The availability value defined in (4).

Using this concept of AVAIL and MFC, we define a value-oriented version of AVAIL namely, Econometric Availability (EA) presented by the following formula (6):

$$EA(S_i) = ((AVAILG(S_i)) - ((1 - VAIL)MFC(S_i)) \quad (6)$$

We applied the new formula (5) using the STEG's SCADA system. The data was collected from a year-long study that interviewed STEG stakeholders and SME's by the Universit de Tunis. The data was analyzed and the ST', DP', IM, and PT matrices were populated. The MFC was then calculated following formula (5) for the four primary stakeholders in Table VI and Table 7. The mean time between failures (MTBF) was 182.5 hours. From historical records during the one-year period, the maintenance teams required, on average, 3 hours to repair the system (MTTR) including both administrative and logistic downtime. Applying the classic formula (4), the operational availability $AVAIL_{Op}$ is 98.38% (182.5 hours/(182.5 hours + 3 hours)).

The classical formula of availability is inadequate to determine whether the system is profitable or not. Let us recall that the ratio $AVAIL_{Op}$, operational availability, has a value in [0, 1]. Therefore, if:

- AVAIL=1: the percentage of availability of the system is 100% (high level of availability).
- AVAIL=0: The system is unavailable (unacceptable)
- 0<AVAIL<1: the system is not guaranteed to be available.

Table 6. The initial MFC and MFC Adjusted for Unavailability of the STEG SCADA System

Stakeholder	Initial MFC ($/hour)	MFC Adjusted for Unavailability
Maintenance Personnel	$ 6,437	$5,220
System Administrators	$3,735	$1,153
Technical Staff	$3,218	$2,316
Controller	$11,739	$4,632

Table 7. STEG SCADA Econometric Availability (EA) Calculated Using AVAIL, GAIN, and MFC

Stakeholder	MFC Adjusted ($/hour)	Gain ($/hour)	EA ($/hour) =98.4%	EA ($/hour) =93%	EA ($/hour) =90%	EA ($/hour) =75%
Maintenance Personnel	$5,220	$340	$250	-$49	-$216	-$1,048
System Administrators	$1,153	$197	$175	$103	$62	-$140
Technical Staff	$2,316	$170	$130	-$4	-$79	-$451
Controller	$4,632	$620	$535	$252	$95	-$693

In all three of these cases the value of AVAIL does not provide us with a definitive understanding about system profitability. To make the availability more useful in value- oriented terms, we have used the EA formulation (6). Table 7 shows the MFC, Gain and EA for the selected stakeholders with the actual AVAIL of 98.4% and hypothetical values of 93%, 90%, and 75% respectively. These actual and synthetic values illustrate where: (1) the system is available and profitable (i.e., positive dollar values; all stakeholders at values of 98.4% availability, and only for system admins and controllers at values of 93% and 90% availability), and (3) the system is available and not profitable (i.e., negative dollar values for maintenance personnel and technical staff at values of 93% and 90% availability, and all stakeholders at value of 75% availability).

The new formula Econometric Availability (EA) can be used to evaluate the availability of a system in terms of the gain/loss ($/hour of operation) that each stakeholder stands to sustain as a result of availability breakdowns. If:

- $EA(S_i) = G(S_i)$: System is available with an average of 100% gain per unit of time.
- $EA(S_i) = -MFC(S_i)$: System is unavailable and the MFC(S) is the average loss per unit of time.
- $(1-AVAIL)\times MFC(S_i) < EA(S_i) < 0$: System is available but not profitable.
- $AVAIL\times G(S_i) > EA(S_i) > 0$: System is available and profitable.

8 Conclusion

In the STEG SCADA system, all selected stakeholders are profitable. However, this may not always be true. In the current set of data, if we had chosen other stakeholders, whose MFC and Gain parameters were marginal, and AVAIL was approximately $\geq 15\%$ less resulting in the values 93%, 90% or 75% as shown in Table 7, we see a situation where those stakeholders incurring such a failure causing unavailability becoming unprofitable.

SCADA systems used in critical infrastructures are characterized by interdependencies (physical, cyber, geographic and logical) and complexity (collections of interacting components). The critical nature and the high cost of failures causing unavailability make EA an important metric to ascertain. The classical formula based on time between failure and time to recovery does not adequately convey the stakes (profitability). In the future, we plan to experiment with the AVAIL parameter to investigate the sensitivity of the EA formula (6) assuming that MFC and the Gains are fixed by the characteristics of the system.

9 Acknowledgement

The views expressed in this paper are those of the authors and do not reflect the official policy or position of our respective academic institutions, the Department of Energy, or the U.S. Government.

This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy (DOE). The United States Government (USG) retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for USG purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan

(http://energy.gov/downloads/doe-public-access-plan).

References

[1] B. Miller and D. Rowe, "A survey SCADA of and critical infrastructure incidents," in Proceedings of the 1st Annual Conference on Research in Information Technology (RITI'12), Calgary, Alberta, Canada, October 11-13, 2012, pp. 51-56.

[2] T. M. Chen, "Stuxnet, the real start of cyber warfare? [Editor's note]," Network, IEEE, vol. 24, pp. 2-3, 2010.

[3] D. Kushner, "The Real Story of Stuxnet: How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program," IEEE Spectrum, 2013.

[4] D. P. Fidler, "Was Stuxnet an Act of War? Decoding a Cyberattack," IEEE Security & Privacy, vol. 9, pp. 56-59, 2011.

[5] "Sector Risk Snapshot," DHS Office of Cyber and Infrastructure Analysis (OCIA) ed. Washington, DC, 2014, p. 52.

[6] "Inventory of Risk Management/Risk Assessment Methods," in Risk Management/Risk Assessment Methods and Tools, ENISA European Network and Information Security Agency ed. Heraklion, Greece, 2014.

[7] "Comparison of Risk Management Methods and Tools," in Risk Management/Risk Assessment Methods and Tools, ENISA European Network and Information Security Agency ed. Heraklion, Greece, 2014.

[8] B. Boehm, L. G. Huang, A. Jain, and R. Madachy, "The nature of system dependability: A stakeholder/value approach," University of Southern California USC-CSSE-2004-520, 2004.

[9] D. Wu, Q. Li, M. He, B. Boehm, Y. Yang, and S. Koolmanojwong, "Analysis of stakeholder/value dependency patterns and process implications: A controlled experiment," in 43rd Hawaii Int. Conf. on System Sciences (HICSS), 2010.

[10] A. B. Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Defining and computing a value based cyber-security measure," Information Systems and e-Business Management, vol. 10, pp. 433-453, 2012.

[11] IEEE, "IEEE C37.1-2007, IEEE Standard for SCADA and Automation Systems," ed, 2008, p. 143.

[12] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," Computers & Security, vol. 25, pp. 498-506, October 2006.

[13] M. Hentea, "Improving Security for SCADA Control Systems," Interdisciplinary Journal of Information, Knowledge, and Management, vol. 3, pp. 73-86, 2008.

[14] Y. Cherdantseva and J. Hilton, "A reference model of information assurance & security," in 2013 Int. Conf. on Availability, Reliability and Security (ARES), Regensburg, 2013, pp. 546-555.

[15] A. Daneels and W. Salter, "What is SCADA?," in Int. Conf. on Accelerator and Large Experimental Physics Control Systems, 1999, pp. 339-343.

[16] D. H. Ryu, H. Kim, and K. Um, "Reducing security vulnerabilities for critical infrastructure," Journal of Loss Prevention in the Process Industries, vol. 22, pp. 1020-1024, 2009.

[17] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," ISA Transactions, vol. 46, pp. 583-594, 2007.

[18] R. Dawson, C. Boyd, E. Dawson, and J. M. G. Nieto, "SKMA: A Key Management Architecture for SCADA systems," in Proceedings of the 2006 Australasian Workshops on Grid computing and e-Research - Volume 54, Hobart, Tasmania, Australia, 2006, pp. 183-192.

[19] C. Ning, W. Jidong, and Y. Xinghuo, "SCADA system security: Complexity, history and new developments," in Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on, Daejeon, Korea, 2008, pp. 569-574.

[20] W. Yang and Q. Zhao, "Cyber security issues of critical components for industrial control system," in 2014 IEEE Chinese on Guidance, Navigation and Control Conference (CGNCC), Yantai, 2014, pp. 2698-2703.

[21] A. B. Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Quantifying Security Threats and Their Potential Impacts: A Case Study," Innovations in Systems and Software Engineering, vol. 6, pp. 269-281, December 2010.

[22] J. Caswell, "Survey of Industrial Control Systems Security," Washington University in St. Louis, St. Loius, Missouri 2011.

[23] A. Hildick-Smith, "Security for Critical Infrastructure SCADA Systems," SANS GSEC Practical Assignment, Version 1.4c, Option 1, February 23, 2005.

[24] "Vulnerability analysis of energy delivery control system," Idaho National Laboratory, Idaho Falls INL/EXT-10-18381, September 2011.

[25] S. Amin, A. Crdenas, and S. S. Sastry, "Safe and secure networked control systems under Denial-of-Service attacks," in Hybrid Systems: Computation and Control. vol. 5469, R. Majumdar and P. Tabuada, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 31-45.

[26] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of Cyber-Warfare," Computers & Security, vol. 31, pp. 418-436, 2012.

[27] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology (NIST), Gaithersburg, MD Special Publication 800-82, June 2011.

[28] I. Onyeji, M. Bazilian, and C. Bronk, "Cyber Security and Critical Energy Infrastructure," The Electricity Journal, vol. 27, pp. 52-60, 2014.

[29] F. T. Sheldon, R. K. Abercrombie, and A. Mili, "Evaluating security controls based on key performance indicators and stakeholder mission," in 4th Workshop on Cyber security and information intelligence research (CSIIRW'08), Oak Ridge, Tennessee, 2008, pp. 1-11.

[30] Q. Chen and S. Abdelwahed, "Towards realizing self-protecting SCADA systems," in Proceedings of the 9th Annual Cyber and Information Security Research Conference, Oak Ridge, Tennessee, USA, 2014, pp. 105-108.

[31] Q. Chen and S. Abdelwahed, "A Model-based Approach to Self-Protection in SCADA Systems," in 9th International Workshop on Feedback Computing (Feedback Computing '14), Philadelphia, 2014.

[32] "DOE Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline (DOE/OE-003)," Department of Energy, Washington, D.C., 2012.

[33] G. Stoneburner, A. Y. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems," NIST Special Publication 800-30, Germantown, MD United States, 2002.

[34] "Guide for Conducting Risk Assessments," NIST Special Publication 800-30, Revision 1, Germantown, MD United States, September 2012.

[35] A. Mili and F. T. Sheldon, "Challenging the Mean Time to Failure: Measuring Dependability as a Mean Failure Cost," in 42nd Hawaii International Conference on System Sciences (HICSS), 2009, pp. 1-10.

[36] F. T. Sheldon, R. K. Abercrombie, and A. Mili, "Methodology for evaluating security controls based on key performance indicators and stakeholder mission," in 2009 42nd Hawaii International Conference on System Sciences (HICSS), 2009, pp. 1-10.

[37] R. K. Abercrombie, E. M. Ferragut, F. T. Sheldon, and M. R. Grimaila, "Addressing the need for independence in the CSE model," in 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2011, pp. 68-75.

[38] R. K. Abercrombie, F. T. Sheldon, and M. R. Grimaila, "A systematic comprehensive computational model for stake estimation in mission assurance," in 2010 IEEE SocialCom, Minneapolis, MN, 2010, pp. 1153-1158.

[39] R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Synopsis of evaluating security controls based on key performance indicators and stakeholder mission value," in High Assurance Systems Engineering Symposium, 2008. HASE 2008. 11th IEEE, 2008, pp. 479-482.

[40] R. K. Abercrombie, B. G. Schlicher, and F. T. Sheldon, "Security analysis of selected AMI failure scenarios using agent based game theoretic simulation," in 47th Hawaii International Conference on System Sciences (HICSS), Big Island, HI, 2014, pp. 2015-2024.

[41] R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantz, and A. Mili, "Failure impact analysis of key management in AMI using cybernomic situational assessment (CSA)," in Eighth Cyber Security and Information Intelligence Research Workshop, 2013.

[42] R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantz, and A. Mili, "Risk assessment methodology based on the NISTIR 7628 guidelines," in 46th Hawaii International Conference on System Sciences (HICSS), Wailea, Maui, HI USA, 2013, pp. 1802-1811.

[43] R. K. Abercrombie, "Cryptographic Key Management and Critical Risk Assessment," Oak Ridge National Laboratory, Oak Ridge, TN ORNL/TM-2014/131, 2014.

[44] C. Vishik, F. T. Sheldon, and D. Ott, "Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment," in ISSE 2013 Securing Electronic Business Processes, ed: Springer, 2013, pp. 133-147.

[45] M. Jouini, A. B. Aissa, L. B. A. Rabai, and A. Mili, "Towards Quantitative Measures of Information Security: A Cloud Computing Case Study," International Journal of Cyber-Security and Digital Forensics, vol. 1, pp. 248-262, 2012.

[46] A. B. Aissa, L. B. A. Rabai, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Quantifying availability in SCADA environments using the cyber security metric MFC," in Proceedings of 2014 9th Cyber and Information Security Research Conference, Oak Ridge, TN, 2014, pp. 81-84.

[47] A. B. Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Quantifying the impact of unavailability in cyber-physical environments," in 2014 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2014, pp. 1-8.

[48] "Introduction to Repairable Systems," in System Analysis Reference, Reliability, Availability & Optimization, ed Tucson: RealiSoft Corporation, 2013, pp. 112-125.

Qian Chen is currently an Assistant Professor in the Engineering Technology Department: Computer Science Technology Program, Savannah State University. She received the B.E. degree in Automation from Nanjing University of Technology, China, in 2009. In 2014, she received her Ph.D. degree in Electrical and Computer Engineering from Mississippi State University. Her main research interests include autonomic computing, self-protection techniques, cyber security, and industrial control system security.

Dr. **Abercrombie** is a joint faculty member in the Graduate School and Department of Computer Science, The University of Memphis. He is the Co-Director, Computational Intelligence Behavior Modeling Laboratory, Modeling & Simulation Group, Oak Ridge National Laboratory (ORNL) and also a Science & Technology Program Manager/Principal Investigator at ORNL with extensive experience in all phases of program and project life cycle management from requirements definition through retirement and system closeout. He was awarded a B.S. in Biology from The College of William & Mary in 1973, a M.S. degree in Computer Science from The University of Missouri, Columbia in 1979, a Ph.D. degree in Physiology for The University of Tennessee, Knoxville in 1978, and held a NIH/NLM Post-Doctoral Fellowship at The University of Missouri, Columbia during 1978-79. Dr. Abercrombie has over 200 publications, including 18 patents (issued or pending), 9 proceedings editors/book chapters, 71 conference papers and 106 technical reports. His most research efforts deal with developing breakthrough approaches for analytic capabilities that work across heterogeneous data sets addressing the necessary computational intelligence techniques to accomplish threat mitigation in resilient, scalable cyber state awareness of Industrial Control System (ICS) networks within the energy delivery sector.retic self-organizing maps and information maximization methods for supervised learning.

Frederick Sheldon is Professor and Chair of the Department of Computer Science at the University of Idaho. Currently, he is focused on cyber-physical and information security and has over 30+ years of experience in the fields of software engineering and computer science. He has served as a software requirements/design/test engineer, principal investigator, program/capture manager, business developer, and conference chair. He held a Sr. Research Scientist at Oak Ridge National Laboratory for 11 years and R&D positions at 3 Fortune 100 companies and an NRC postdoc/visiting scholarship at NASA LaRC and ARC/Stanford.
Dr. Sheldon has published 130+ articles and edited six proceedings books concerned with developing and validating models, applications, and methods for developing safe, secure, and dependable systems. He has facilitated and participated in national R&D thrusts including as an invited speaker, panelist, and moderator. A co-inventor and IEEE Senior Member, he has received Sigma Xi research and UT-Battelle key contributor and significant event awards. He received his PhD from the University of Texas at Arlington in 1996.