

Quantifying the Impact of Unavailability in Cyber-Physical Environments

Anis Ben Aissa

Université de Tunis El
Manar
Tunis, Tunisia
anis.benaissa@enit.rnu.tn

Robert K. Abercrombie

Oak Ridge National
Laboratory
Oak Ridge, TN 37831 USA
abercrombie@ornl.gov

Frederick T. Sheldon

Department of Computer Science
University of Memphis
Memphis, TN 38152 USA
f.sheldon@memphis.edu

Ali Mili

College of Computing Sciences
New Jersey Inst. of Technology
Newark NJ 07102 USA
mili@cis.njit.edu

Abstract— The Supervisory Control and Data Acquisition (SCADA) system discussed in this work manages a distributed control network for the Tunisian Electric & Gas Utility. The network is dispersed over a large geographic area that monitors and controls the flow of electricity/gas from both remote and centralized locations. The availability of the SCADA system in this context is critical to ensuring the uninterrupted delivery of energy, including safety, security, continuity of operations and revenue. Such SCADA systems are the backbone of national critical cyber-physical infrastructures. Herein, we propose adapting the Mean Failure Cost (MFC) metric for quantifying the cost of unavailability. This new metric combines the classic availability formulation with MFC. The resulting metric, so-called Econometric Availability (EA), offers a computational basis to evaluate a system in terms of the gain/loss (\$/hour of operation) that affects each stakeholder due to unavailability.

Keywords— *Availability, Security measures, Dependability, Security requirements for control systems, Threats, Vulnerabilities and Risk*

I. INTRODUCTION

The typical architecture of a Supervisory Control and Data Acquisition (SCADA) system rely on an Internet that often uses wireless technologies. In such architectures SCADA systems are more vulnerable to the new security challenges including internal and external cyber-attacks. Four brief examples of SCADA security incidents include [1-4]:

- 2000: Disgruntled employee in Australia gained unauthorized access to a compromised SCADA causing millions of liters of raw sewage to spill into local parks and rivers. Pumps failed to start or stop when commanded, while at the same time alarms failed to be reported.
- 2006: An overload of network traffic caused failures in the reactor recirculation pumps in the Browns Ferry nuclear plant in Alabama, USA.
- 2009: Both Chinese and Russian spies penetrated the U.S. electric power grid, and have left disruptive software programs using network-mapping tools.
- 2010: The year Stuxnet worm was detected. The first

worm known to have successfully attacked SCADA systems physically isolated from the Internet, yet subsequently reported in the wild.

SCADA systems form the core of key critical infrastructures, which must be available nonstop. Continuous availability should be protected using strong measureable security processes and practices to prevent cyber-attacks and mitigate the impact of those risks.

A. 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) and present the mean failure cost (MFC) metric as a measure for security failure impact (Section III). Section IV improves on the general concept of MFC to the specific pursuit of measuring the impact of unavailability for SCADA systems. Section V describes a real example taken from a utility in

This manuscript has been authored by UT-Battelle, LLC, under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for U.S. Government purposes.

Tunis, Tunisia. To conclude, we discuss the proposed measure in comparison with more common formulations.

II. 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 process control using remote (and master) terminal units (RTUs). 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.

A. SCADA Architecture

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

1) Hardware SCADA Components

- Corporate network segment: operates in the same way as a general Information and Communications Technology (ICT) network performing operations such as e-mail and requiring an Internet connection.
- SCADA network segment: contains servers, workstations, Human Machine Interface (HMI) and data historian(s), among others.
- Field devices segment: containing three types of field devices namely programmable logic controllers (PLCs), remote terminal units (RTUs) and intelligent electronic devices (IEDs).

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,

TABLE I. IT/ICT VERSUS SCADA SECURITY REQUIREMENTS

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

Fieldbus, DNP3 and PROFIBUS.

- Operating systems: Current SCADA system servers commonly use both Windows and Linux OS variants.

3) SCADA communication components

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

- Physical connections, if linked to the Internet, through both guided and unguided transmission media.
- Logical connection: use standard logical network topologies, which transmit data through physical links.

B. SCADA System Security Issues

Availability, integrity and confidentiality (listed in priority order; but usually referred to, in an IT context, as CIA) 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 our 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, environmental factors and operational availability/reliability. As shown in Table I, 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 constraints on maximum transmission time making them more vulnerable to disruption [1].

Connecting SCADA systems to the Internet or corporate Networks (one step removed) without taking appropriate security measures create an easy target and introduce many security risks. This is especially true because designing-in security and authentication protocols into SCADA has been considered unnecessary up until the more 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 any other platform for that matter have made security by 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 the increasing complexity and interdependence of critical

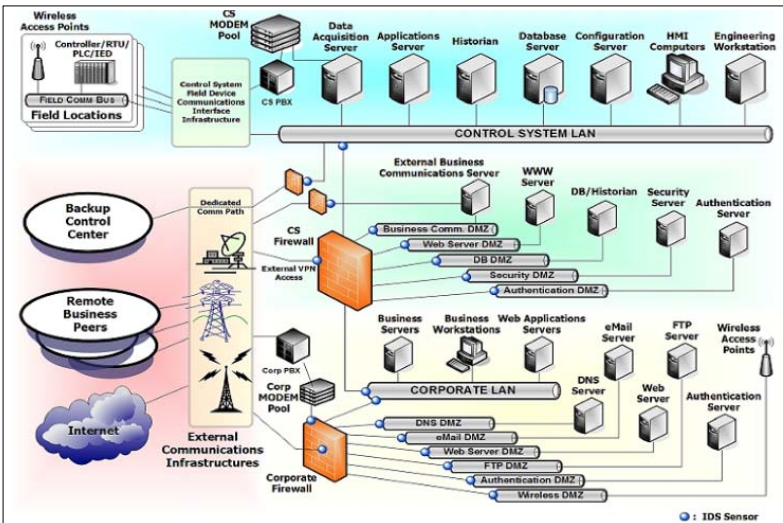


Fig. 1. Recommended SCADA Architecture post modernization with added security.

infrastructures [16], include the risks from loss of service (e.g., electricity, traffic or process control), financial sector services, property and environmental damage and potential loss of life [17].

C. 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 software, hardware, users or communication links:

Hardware vulnerabilities: Different SCADA components address these vulnerabilities in specific ways. For example, RTUs are difficult to protect because they 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 security. 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 [20]. 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 link vulnerabilities: Phone systems may be used as a means of connection to the outside world. As noted in [21], problems occur because 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) [22, 23].

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

- Hackers can intrude, modify, destroy or exfiltrate data thereby causing disruption to systems and networks [17, 21] 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, 22] which may be delivered via firmware updates). Current research

is ongoing toward ensuring that no hidden functionality is delivered in hardware sourced from “trusted” vendors.

- Human accidental errors can have the same impact as malicious attacks [13] whose effects may 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, 24].

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 [24] aimed at intrinsically (built-in) protecting or deferring malicious deception/DoS attacks. The more added-on type of security control measures include typical ICT security measures (cryptographic techniques, passwords, firewalls, intrusion detection systems, virtual private network, antivirus, access control, etc.) [1, 12, 13, 20, 25]. Moreover, other SCADA measures have been proposed: first embodied in IEEE/ISO standards [11] and NIST Guidelines [26], and secondly enhancing SCADA protocols by placing at each end of the communication media encryption/decryption technologies, wrapping SCADA protocols without making changers to the protocols using external cryptographic and security protocols (SSL/TLS, IPsec) or modifying the protocols fundamentally [1, 24]. 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 [25]. The reality of the aforementioned threats (Section I, Item 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 [27]. From these limits derives 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 needed to formalize the perceived risk [20, 28].

III. THE MEAN FAILURE COST AS A MEASURE OF SECURITY

In [29], the concept of Mean Failure Cost (MFC) was first introduced. The concept was refined through a series of applications [20, 30, 31] and has been applied to several domains which include mission assurance [32, 33], failure impact analysis in Advanced Metering Infrastructure (AMI) [34, 35], risk assessment [36], game theoretic simulation [34, 37], cybersecurity modeling in the cloud [38] and SCADA environments [39]. 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 resulting 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 scheme because 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 multiplying (“ \circ ”) the matrices as follows:

$$MFC = ST \circ DP \circ IM \circ PT \quad (1)$$

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 is expressed in dollars (i.e., monetary terms) and represents the loss incurred and/or premium placed on the specific requirement.
 - ST (S_i, R_j): Is the stake that stakeholders S_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 an estimate of how much each component contributes to satisfying each security requirement; each cell represents the conditional probability of failure with respect to a requirement given 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 provides the probability of a component being compromised given that a threat has materialized, it depends on the target (component) of each threat and the likelihood that the threat will successfully compromise the target.

TABLE II. STAKES (ST) MATRIX FOR THE STEG SCADA SYSTEM

| ST | | Security Requirements | | | |
|--------------|-----------------------|-----------------------|--------------|-----------------|--------------|
| | | Integrity | Availability | Confidentiality | Authenticity |
| Stakeholders | Maintenance personnel | \$7,000 | \$9,000 | \$0 | \$0 |
| | System Admins | \$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 |

- 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 a probability each threat category.
 - P(T_i): The probability that threat T_i materialized within a unit of operation time.

IV. 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: Société Tunisienne de l'Electricité et du Gaz). 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.

A. The Stakes Matrix (ST)

We populated the Stakes Matrix (Table II) by 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.

1) The stakeholders of SCADA

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

- Maintenance personnel and operational personnel responsible for the maintenance and performance of all system operations,
- System administrators responsible for the SCADA system administration functions,
- Technical staff responsible for installing software and ancillary (non-admin type) materials/functions of the system,

TABLE III. DEPENDENCY (DP) MATRIX FOR THE STEG SCADA SYSTEM

| DP | | Components | | | | | | | |
|---------------|-----------------|------------|-------|-------|------|------|-------|------|------------|
| | | RTU | PLC | OS | MTU | IOS | DBS | C | No Failure |
| Security Reqs | Integrity | 0.042 | 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 |

- Controllers of SCADA serves a vital role in maintaining safe and efficient systems operation (e.g., quality assurance/control).

2) SCADA security requirements of the STEG

We considered the security requirements concerns that are typically cited for SCADA systems:

- Integrity
- Availability
- Confidentiality
- Authenticity

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

B. The Dependency (DP) Matrix

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

1) The components of system

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

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

C. The Impact Matrix (IM)

The Impact Matrix (IM) presented in Table IV has been 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 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).

TABLE IV. 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 | 0.9998 | 0.9 | 0.04 | 1 |

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

D. The Threat Vector (PT)

The vector of threat probabilities is presented in Table V 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.

E. The Mean Failure Cost of the STEG SCADA Enterprise

The mean failure cost for each stakeholder is initially calculated using the Stakes Matrix, Dependency Matrix; the Impact Matrix and the Probability Threat vector of STEG SCADA system per (1). The results of the initial MFC cost for each stakeholder are presented in Table VI (Column Initial MFC).

V. 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's consider average uptime availability. If the system is 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:

$$\overline{A(t)} = \frac{1}{t} \int_0^t A(u) du \quad (2)$$

where, the system functioned properly since the last repair at time u , $0 < u < t$ [40]. For systems that have periodical maintenance, availability may be zero at regular intervals. In this case, mean availability is a more meaningful measure than instantaneous availability. This definition of availability is commonly used in manufacturing and telecom systems as it considers both reliability (probability that the item will not fail) and maintainability (the probability that the function 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 has otherwise been restored). *This metric is availability*. Availability can be addressed as inherent (steady state when considering only the corrective downtime 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 including all experienced sources of downtime, such as administrative downtime, logistic downtime, etc.) [40]. Thus, availability is a performance criterion for repairable systems that inherently 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 operational taking into account all factors that affect downtime (both scheduled and unscheduled).

We adopt the following calculation as it satisfies a global perspective of the STEG SCADA system. $AVAIL_{Op}$ is the operational availability (3), the ratio of the system uptime and total time. Mathematically, it is given by:

$$AVAIL_{Op} = \frac{Uptime}{OperatingCycle} \quad (3)$$

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

TABLE V. THREAT VECTOR FOR THE STEG 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 |

- Independence with respect stakeholders.
- Independence of the components, which have failed to ensure availability.
- Independence of threats, which have caused the system/component to become unavailable.

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) of a security violation (or other such failure) of the system under study. Here, we extend 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 (4):

$$MFC = ST' \circ DP' \circ IM \circ PT \quad (4)$$

where, ST' is $n \times 1$; DP' is $1 \times h$; IM is $h \times p$; and PT is $p \times 1$. We consider a system A, where $S_1, S_2, S_3 \dots S_k$ are the stakeholders and $C_1, C_2, C_3 \dots C_k$ are the system components as above (Sec. 3) 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 II. ST' represents the stake of stakeholder S_i has in the 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 III.
 - DP' represents the set of probabilities for which a failed component, C_k 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 III.

TABLE VI. THE INITIAL MFC AND MFC ADJUSTED FOR UNAVAILABILITY OF THE STEG SCADA SYSTEM

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

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 (4). The results are presented in Table VI showing the MFC/stakeholder due to unavailability.

VI. APPLICATION OF MFC: EMPHASIS ON AVAILABILITY

Availability of a system is defined as the ratio of uptime over the total operating cycle as in (3) 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 $1 \leq i \leq 4$ (see Table VII column labeled "Gain") is provided as data from interviews made with the STEG SMEs.
- The loss, per unit of time, is 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.
- $AVAIL_{Op}$: The availability value defined in (3).

Using this concept of AVAIL and MFC, we define a value-oriented version of AVAIL namely, Econometric Availability (EA) presented by the following (5):

$$EA(S_i) = ((AVAIL \times G(S_i)) - ((1 - AVAIL) \times MFC(S_i))) \quad (5)$$

We applied the new formula (4) using STEG's SCADA system data. The data was collected from a year-long study that interviewed STEG stakeholders and SMEs by the Université de Tunis. The data was analyzed and the ST', DP', IM, and PT matrices were populated. The MFC was then calculated following formula (4) for the four primary stakeholders in Table VI and Table VII. 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 (3), the operational availability $AVAIL_{Op}$ is 98.38% (182.5 hours / (182.5 hours + 3 hours)).

This 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:

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

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 (5). Table VII 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 (2) 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.

VII. CONCLUSIONS

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 VII, we would expect 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 (5) assuming that MFC and the Gain are fixed by the characteristics of the system.

TABLE VII. STEG SCADA ECONOMETRIC AVAILABILITY (EA) CALCULATED USING MFC, GAIN, AND AVAIL

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

ACKNOWLEDGMENT

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.

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 Latracked 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] 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.
- [21] J. Caswell, "Survey of Industrial Control Systems Security," Washington University in St. Louis, St. Louis, Missouri 2011.
- [22] A. Hildick-Smith, "Security for Critical Infrastructure SCADA Systems," SANS GSEC Practical Assignment, Version 1.4c, Option 1, February 23, 2005.
- [23] "Vulnerability analysis of energy delivery control system," Idaho National Laboratory, Idaho Falls INL/EXT-10-18381, Sep 2011.
- [24] S. Amin, A. Cárdenas, 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.
- [25] 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.
- [26] 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.
- [27] I. Onyeji, M. Bazilian, and C. Bronk, "Cyber Security and Critical Energy Infrastructure," *The Electricity Journal*, vol. 27, pp. 52-60, 2014.
- [28] 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.
- [29] 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.
- [30] 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.
- [31] 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.
- [32] 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.
- [33] 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.
- [34] 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 Int. Conf. on System Sciences (HICSS)*, Big Island, HI, 2014, pp. 2015-2024.
- [35] 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.
- [36] 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 Int. Conf. on System Sciences (HICSS)*, Wailea, Maui, HI USA, 2013, pp. 1802-1811.
- [37] C. Vishik, F. 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.
- [38] 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.
- [39] 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.
- [40] "Introduction to Repairable Systems," in *System Analysis Reference, Reliability, Availability & Optimization*, ed Tucson: RealSoft Corporation, 2013, pp. 112-125.