Quantifying availability in SCADA environments using the cyber security metric MFC

Anis Ben Aissa
Université de Tunis El Manar
Ecole Nationale d'Ingénieurs de Tunis
+216-98-692-415
anis.benaissa@enit.rnu.tn

Latifa Ben Arfa Rabai
Université de Tunis
Institut Supérieur de Gestion de Tunis
latifa.rabai@isg.rnu.tn

Robert K. Abercrombie
Oak Ridge National Laboratory
Oak Ridge, TN 37831 USA
+1 865-241-6537
abercrombier@ornl.gov

Frederick T. Sheldon
sheldon@ieee.org

Ali Mili
College of Computing Sciences
New Jersey Institute of Technology
Newark NJ 07102-1982 USA
+1 973-596-5215
mili@cis.njit.edu

ABSTRACT
Supervisory Control and Data Acquisition (SCADA) systems are distributed networks dispersed over large geographic areas that aim to monitor and control industrial processes from remote areas and/or a centralized location. They are used in the management of critical infrastructures such as electric power generation, transmission and distribution, water and sewage, manufacturing/industrial manufacturing as well as oil and gas production. The availability of SCADA systems is tantamount to assuring safety, security and profitability. SCADA systems are the backbone of the national cyber-physical critical infrastructure. Herein, we explore the definition and quantification of an econometric measure of availability, as it applies to SCADA systems; our metric is a specialization of the generic measure of mean failure cost.

General Terms
MFC, SCADA, Measurement, Economics, Reliability, Security.

Keywords
Availability, Security measures, Dependability, Security requirements, Threats.

1. INTRODUCTION
The typical architecture of a Supervisory Control and Data Acquisition (SCADA) system relies 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. Three brief examples of SCADA security incidents include [1]:

- In 2000, a disgruntled employee, gained unauthorized access into a compromised management system in Australia [1]. As a consequence, millions of liters of raw sewage have been spilled out into local parks and rivers, pumps failed to start or stop when specified, and alarms failed to be reported.
- In 2006, an overload of network traffic cause a failure of a number of reactor recirculation pumps in the Browns Ferry nuclear plant in Alabama, US.
- In 2009, both Chinese and Russian spies penetrated the U.S electric power grid, and left disruptive software programs using network-mapping tools.

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.

The remainder of this extended abstract includes a brief overview of SCADA systems (Section 2). We then present the mean failure cost metric as a measure for security (Section 3). Section 4 specializes the generic concept of mean failure cost to the specific question of measuring availability for SCADA systems. We conclude by describing this proposed measure and discussing some differences with more common formulations.

2. BACKGROUND ON SCADA SYSTEM
The IEEE standard C37.1-2007 defines SCADA as: "A system operating with coded signals over communication channels so as to provide control of 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. Based on several studies such as

 CISR '14, Apr 08-10 2014, Oak Ridge, TN, USA | ACM 978-1-4503-2812-8/14/04, http://dx.doi.org/10.1145/2602087.2602103

those described by Igure [2] and Hentea [3] that have focused on SCADA architecture, we propose 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.
- 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 [2, 3]:

- Protocols: some protocols are common and found in general ICT, which are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). While some protocols are unique to Critical Infrastructure Protection (CIP) Standards and found only within specific industrial settings such as ModBus, Fieldbus, Distributed Network Protocol (DNP3) and PROBIBUS.
- Operating systems: Current SCADA systems commonly use Windows NT software.

2.1.3 SCADA communication components

As discussed in [2, 3], communication links utilize:

- Physical connections: including optical fiber, radio, satellite, etc., and 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.

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. Based on an extensive literature analysis, the Information Assurance & Security (IAS) Octave has been developed and proposed as an extension of the CIA-triad [4]. The IAS Octave includes confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, 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.

3. THE MEAN FAILURE COST AS A MEASURE OF SECURITY

In [5-8], a value-based metric, Mean Failure Cost (MFC) was introduced that 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 Mean Failure Cost can be computed by means of the following formula:

$$\mathbf{MFC = ST \circ DP \circ IM \circ PT}$$

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 monetary terms and it represents loss incurred and/or premium placed on requirement. ST (Hi, Rj): Is the stake that stakeholders Hi has in meeting requirement Rj.
- 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 (Rj, Ck): The probability that the system fails to meet requirement Rj if component Ck is compromise.
- IM: The impact matrix (IM) 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 (Ck, Th): The probability that Component Ck is compromised if Threat Th has materialized.
- PT: The vector of threat characterizes the threat situation by assigning to each threat category the probability that this threat will materialize over a unitary period of operation time.

4. QUANTIFYING 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.

In order to apply the MFC approach to the calculation of mean failure cost stemming from loss of availability in a SCADA system, we need to collect the following information:

- The list of relevant availability requirements as they apply to SCADA systems.
- The list of relevant stakeholders in a typical generic SCADA system.
- A standard reference architecture of SCADA systems, detailing the main components and their role in the operation of the system.
- The list of typical threats that SCADA systems are exposed to, by virtue of their vulnerabilities, and of typical perpetrator models.

We review these items in turn, below.

4.1 Availability Requirements

It is common to consider availability as a monolithic security requirement; but on closer inspection we can identify a structure therein. Indeed, a SCADA system delivers a broad range of services, and it is quite possible that due to cyber-attacks or to system failures, some of these services may be more available (i.e. available a higher percentage of the time) than others. Among the services that we see a SCADA system providing, we cite:

- Process Control.
- Resource management, resource allocation.
- Routing, load distribution, service delivery.
- Infrastructure monitoring, maintenance.
- Billing, accounting, planning.
- Data collection, statistical analysis, bookkeeping.

From our standpoint, these services are distinguishable for several reasons:

- They can be targeted (by perpetrators) separately,
- They carry different stakes for different stakeholders,
- They depend on different parts of the SCADA system for their secure operation.

4.2 Stakeholders

SCADA systems span a broad range of application, each with a specific set of relevant stakeholders. For a general discussion, we adopt a broad list of stakeholders, with the qualification that any particular stakeholder may have a subset of these. We consider the following set:

- The engineering department/ utility company.
- The financial department/ utility company.
- The management department/ utility company.
- The Government as regulatory agency.
- The Government as custodian of national infrastructure.
- The Government as service provider.
- The SCADA operator.
- Relevant/ concerned civic organizations (e.g. relevant environmental concerns).
- End users.
- End user organizations.

4.3 SCADA Architecture

We adopt the reference architecture proposed by Berg and Stamp [9], which cites the following generic components:

- The Infrastructure, which includes sensors, actuators, and field I/O.
- The Field Equipment, which includes RTU's (Remote Terminal Units, or Remote Telemetry Units), PLC's (Programmable Logic Controllers), and IED's (Intelligent Electronic Devices).
- The System and Plant Control Center, which includes modules for data collection, data archiving, data analysis.
- Automation Oversight, which includes such functions as ISO's (Independent System Operators), RTO's (Regional Transmission Operators) and PX's (Power Exchanges).

To these four system components, we add a fifth component, which may offer a conduit for channeling attacks into a SCADA system, namely the human component; indeed some of the attacks that we cite in the next section can be carried out through emails to system users.

4.4 SCADA Threats

Following the survey conducted by Alcaraz and Zeadally [10], we adopt the following classification of relevant cybersecurity threats to SCADA systems:

- PLC attacks,
- VPN attacks,
- Spear-phishing,
- Attacks via the TCP/IP protocol,
- Attacks via the wireless protocol,
- Confidentiality attacks via installed software tools,
- Route falsification,
- Sybil attacks.

4.5 Availability Estimation, and Applications

In order to estimate the availability of a particular SCADA system, we must compute all the relevant matrices; this involves, in general, a detailed analysis of the stakes that each stakeholder has in the availability of each service, as well as the probabilities of requirement violation contingent upon the failure of each component, the probabilities of component failures contingent upon the advent of each security threat, and the probability of each security threat within a unit of time. Because we are talking about SCADA systems in general rather than one such

system in particular, we use generic data rather that stems from empirical SCADA studies.

As per the assumptions of the MFC model, we assume that no more than one threat materializes within a unit of time; that whenever a threat materializes it causes the failure of no more than one component; and that when a component fails it causes no more than one requirement to be violated. The Stakes matrix represents, for a stakeholder and a requirement, the amount of loss (in $K) the selected stakeholder stands to incur if the selected requirement is violated. The dependability and impact matrices are stochastic matrices (where the sum of each column is 1) without dimension. The threat vector has a probability distribution (that adds up to 1) and represents the probability that each threat has to materialize during a unitary duration of time (as well as an entry for the event that no threat materializes). This vector introduces a denominator in the form of a unit of time, so that the product of all four matrices produces a vector whose dimension is dollars per unit of time; this vector contains the mean failure cost of each stakeholder of the system.

We have discussed in [6] how the mean failure cost can be used to estimate the return on investment of a given security defense, for individual stakeholder and for the overall stakeholder community. This can be applied to estimate the ROI of common SCADA defenses, such as [10, 11]:

- Firewalls,
- IDS's (Intrusion Detection).
- IPS's (Intrusion Prevention).
- DMZ's (Demilitarized Zones).
- ACL's (Access Control Lists).
- EAP-TLS (Extensible Authentication Protocol for the Transport Layer Security).
- RADIUS (Remote Authentication Dial In User Service).
- CBC-MAC (Cipher Block Chaining/ Message Authentication Code).

5. CONCLUSION

In this paper we have specialized the generic MFC model in two ways: First by considering the requirement of availability; and second, by focusing specifically on SCADA systems, with their specific pattern of stakeholders, reference architecture, typical threats, and common defense mechanisms. Using empirical or analytical data, the MFC model can estimate the mean failure cost of each stakeholder, as well as determine the worthiness of any defense mechanism for individual stakeholders as well as for the broad stakeholder community. Our metric estimates availability in econometric terms, there by supporting rational decision making.

6. REFERENCES

[1] Miller, B. and Rowe, D. 2012. A survey SCADA of and critical infrastructure incidents. In *Proceedings of the Proceedings of the 1st Annual Conference on Research in Information Technology (RITI'12)* (Calgary, Alberta, Canada, October 11-13, 2012). ACM, New York, NY, 51-56. DOI=http://dx.doi.org/10.1145/2380790.2380805.

[2] Igure, V. M., Laughter, S. A. and Williams, R. D. 2006. Security issues in SCADA networks. *Computers & Security*, 25, 7 (October 2006), 498-506.

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

[4] Cherdantseva, Y. and Hilton, J. A Reference Model of Information Assurance & Security. In *Proceedings of the Proceedings of the 2013 International Conference on Availability, Reliability and Security (ARES)* (Regensburg, Sept. 2-6, 2013). IEEE Computer Society, Wash., D.C., 546-555. DOI=http://dx.doi.org/10.1109/ares.2013.72.

[5] Sheldon, F. T., Abercrombie, R. K. and Mili, A. 2008. Evaluating security controls based on key performance indicators and stakeholder mission. In *Proceedings of the Proceedings of the 4th annual workshop on Cyber security and information intelligence research (CSIIRW'08)* (Oak Ridge, Tennessee, 2008). ACM, New York, NY, 11 pp. DOI=http://doi.acm.org/10.1145/1413140.1413188.

[6] Aissa, A. B., Abercrombie, R. K., Sheldon, F. T. and Mili, A. 2010. Quantifying Security Threats and Their Potential Impacts: A Case Study. *Innovations in Systems and Software Engineering*, 6, 4 (December 2010), 269-281.

[7] Jouini, M., Aissa, A. B., Rabai, L. B. A. and Mili, A. 2012. Towards Quantitative Measures of Information Security: A Cloud Computing Case Study. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, Vol. 1, Issue 3 (2012), 248-262.

[8] Rabai, L. B. A., Jouini, M., Aissa, A. B. and Mili, A. 2013. A cybersecurity model in cloud computing environments. *Journal of King Saud University - Computer and Information Sciences*, 25, 1 (January 2013), 63-75.

[9] Berg, M. and Stamp, J. *2005. A Reference Model for Control and Automation Systems in Electric Power*. Report SAND2005-1000C, Sandia National Laboratories, Albuquerque, NM.

[10] Alcaraz, C. and Zeadally, S. 2013. Critical Control System Protection in the 21st Century. *Computer*, 46, 10 (October 2013), 74-83.

[11] Cárdenas, A. A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y. and Sastry, S. 2011. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (Hong Kong, China, March 22-24, 2011). ACM, New York, NY, 355-366. DOI=http://dx.doi.org/10.1145/1966913.1966959.