Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 581

Graded Security Forensics Readiness of SCADA Systems

Jianghai Li[1], Edita Bajramovic[2], Yuan Gao[3], Mithil Parekh[3]

Abstract: Security event logs are major indicators for the timely discovery of cyberattacks and during security incident examinations. Collection of sufficient logs of events associated with security incident time is critical for effective investigation. SCADA systems logging capabilities are intended for identifying and detecting process disruptions, not security incidents, and are frequently not suitable for digital forensic investigation [Ta13]. Nevertheless, logs provide tremendous support during digital forensics investigations as they consist of vast amounts of information, e.g. step-by-step events that occurred in a system in question, including time stamping [AIJ12]. In addition, logging is a major element of forensic readiness. Numerous tools and methods contribute to log monitoring, e.g. evaluating log records and correlating them through various systems. This can assist in incident handling, identifying policy violations, auditing, and other efforts. Within the general context described above and the more specific graded security approach of IEC 62443-x-x, this paper will identify cybersecurity specific SCADA component requirements, preconditions for subsequent forensic investigations, collecting potential digital evidence, graded forensic-related security controls, and forensic readiness during SCADA lifecycle phases.

Keywords: cybersecurity, forensic readiness, logging, time stamping, asset management, digital forensics investigation.

1 Introduction

As indicated in [IEC613] [IEC615], the application or device of an industrial automation control system (IACS) should have the ability to produce audit records related to security for the access control, request errors, control system events including activity and transactions logs, backup and restore event, configuration changes, and audit log events. However, many controllers deployed in SCADA systems do not have any capability to log security events. Many challenges with digital forensics investigation for SCADA systems exist, e.g. the field devices frequently do not have essential ability for comprehensive logging. Additionally, most of devices are not able to gather a sufficient amount of data [Hs08]. The problem studied in the paper is how to develop security logging capacity in SCADA system as SCADA system and network device logs are

[1] Tsinghua University, Institute of Nuclear and New Energy Technology, Beijing, China, lijianghai@mail.tsinghua.edu.cn
[2] Friedrich-Alexander University Erlangen-Nuremberg, Informatics 1 Department, Erlangen, Germany, edita.bajramovic@gmail.com
[3] Otto-von-Guericke University Magdeburg, Group Multimedia and Security, Magdeburg, Germany, yuan.gao@ovgu.de
[4] Otto-von-Guericke University Magdeburg, Group Multimedia and Security, Magdeburg, Germany, mithil.parekh@ovgu.de

crucial to detect cyber-attacks and perform forensics investigation. In addition, log integrity and reliability are equally important during the investigation; hence, logs must be regularly saved on a different system and constantly backed up. Also, logs should be cryptographically hashed to permit proper discovery of log modifications [Hs16]. Operators are also part of forensics investigation challenge. Usually they do not have the knowledge and expertise to gather, investigate, or evaluate SCADA system's traffic [Hs09]. As a substitute, operators are dependent on vendors for support during incident response. As a result, security incident response and resolution becomes very slow.

Within the context described above and as a preparation towards gradual compliance with IEC 62443-x-x, this paper is divided in six sections. The current section introduces general information regarding logs. The second section addresses Component Requirements and how the combination of Component Requirements (CRs) and Requirement Enhancements (REs) determines the Target Security Level that a component is capable of. The third section identifies preconditions for subsequent forensic investigations. These include the identification of assets, asset management, tracking, and time stamping of logging information. Precise asset identification is needed to address the security of SCADA systems. The fourth section refers to collecting evidence from servers and mobile equipment and issues related to proper collection of electronic evidence from the respective devices. Some of these electronic evidence collection topics are SCADA specific, and may involve e.g. Physical Unidirectional Security Gateways for conduits connecting to the highest security zones according to IEC 626443. The fifth section outlines graded forensic-related security controls. Lastly, the sixth section presents forensic readiness during all SCADA lifecycle phases. This is in line with newest Industry 4.0 BMWi IT Security standard [Bm16].

2 Component Requirements

Each system requirement (SR) has a basic requirement and zero or additional requirement enhancements (REs) to improve security [IEC615].

The control system should have ability to centrally maintain audit events and collect audit records from numerous devices through the control system into a one system (logical or physical). In addition, time-correlated audit track should be provided. Furthermore, the control system should have the ability to export these audit records in industry standard formats for enabling analysis by standard commercial log analysis tools, for example, security information and event management (SIEM) [IEC615].

Fig. 1 indicates how Component Requirements (CR) are derived from Foundational Requirements (FR) and System Requirements (SR) while taking into consideration a grading according to four Security Levels [IEC613] [WD14]. Standard format is important for higher security levels, lower probability of false negatives, and better basis for testing (different depth of testing of forensic readiness).

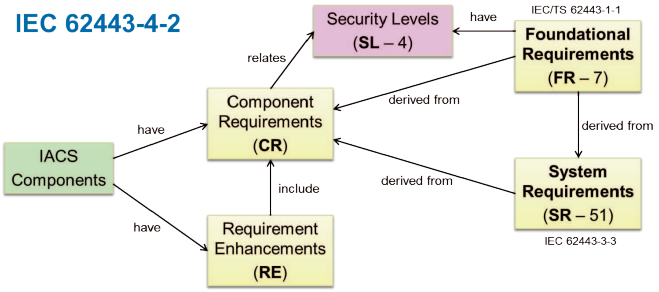

Fig. 1: Component Requirements for Security Graded SCADA Systems

3 Preconditions for Subsequent Forensic Investigations

Numerous international standards provide details regarding digital forensics investigation procedures and response to security incidents [EGI13] [EGI14] [ISIE11a] [ISIE14b] [ISI12b] [ISIE14c] [ISIE15c] [ISIE15d] [ISIE15e] [ISIE15f] [ISIE16a] [ISIE16b]. Nevertheless, many preconditions should be fulfilled for subsequent forensic investigation. The Asset Management addresses the systematic definition and maintenance of an up-to-date Asset Portfolio [ISO514a]. A first step towards an asset management is the asset identification [Wa16]. Asset identification is needed to address the security of SCADA systems [ISO514a] [ISO514b] [ISIE12a] [ISIE15a] [ISIE15b]. Automatic asset identification can increase the efficiency of security controls for communication networks, IT equipment and software assets. Non automatic asset identification could be implemented for some applications, e.g. safety-critical process automation, secure development environments, tamper indicating devices or legacy systems [Wa16]. The most critical assets are located in higher security zones.

3.1 Identification of Assets and Asset management

Understanding and monitoring SCADA system networks and asset management are essential elements in discovering cyberattacks and performing subsequent forensic analyses [LL15]. Asset identification serves numerous purposes inside a SCADA system. Four basic methods exist that support the identification of assets, as indicated in Fig. 2 [Le15].

Fig. 2: Asset Identification Basic Methods [Le15]

Additionally, many other methodologies in identifying assets exist; however, the risk that some assets will not be identified is present, e.g. certain legacy systems just do not use network for communication or they do rarely [NERC09a]. So in this case, physical identification of assets is needed [Le15]. Physical identification should be conducted occasionally to verify outcomes. Evaluation of configuration files on hardware, e.g. switches, discloses already identified and registered hardware. In addition, when hardware, e.g. a switch, is part of managed infrastructure, capturing network traffic necessary for passive scanning is possible. Evaluating data can be performed using open source tools, e.g. Wireshark, to accurately detect assets and communication patterns [Le15]. Passive scanning is good method for fast and competent identification of assets. On the other hand, active scanning on SCADA networks should not be always conducted as interrelating with sensitive hardware using unanticipated methods can cause interruption of normal operations or asset failure. Moreover, network hardware, e.g. proxies and firewalls often logically block involuntary communications [Le15]. As a result, partial network design records by active scanning are returned. Furthermore, sending communications through the network can alter the communication topologies causing difficulties for precise discovery and baseline.

3.2 Tracking for Correctly Associating to Sources

Asset tracking through SCADA system components provides benefits for the implementation of some security controls, but it also introduces the possibility of misuse. Locating assets is essential for safety and security reasons [NIST11]. For example, it should be possible to track the smart sensor that generated a specific event, even if the e.g. analog signal values provided by the sensor are received via intermediate (e.g. signal conditioning and preprocessing) automation equipment. Active log management functionalities may even identify cyberattack or security event in progress and provide information regarding place and traces leading to better response to the incident [NIST11]. Additionally, continuous tracking and monitoring of audit traces on critical zones of a SCADA system leads to discovery of malicious activities and thus permit the essential remedial actions. [Ba16b].

3.3 Time Stamping of Logging Information

During digital forensics investigation, proper time stamping and recording of events is achieved only if a high precision reference clock is available [NERC09b]. For example, timestamps might incorrectly specify that event A occurred 35 seconds before event B, when event A in reality occurred two minutes after event B [NIST06]. Thus, it is essential that reference system clock indicates accurate time. Inaccurate time leads to difficult log analysis. Furthermore, time stamps as outlined in IEC 62443 series, are required for successful audits and also for legal purposes. However, real-time clock may not be available in highest security zone or may not be supported by the embedded hardware or may deliver only a part of the time stamp (e.g. subdivision within one

second).

Nowadays, global positioning system (GPS) clocks are used to make sure universal time through the domain. However, network latency can cause substantial time dissimilarities between devices [NERC09b]. As a result, Network Time Protocol (NTP) can be utilized to approximate and calculate this latency. On the other hand, NTP can allow network spoofing attacks, initiating wrong time stamping [NERC09b]. Fig. 3 indicates real-time collection of the data and time stamping in a subsequent device (e.g. in a gateway). In a typical IT environment, time stamping is performed at the source, e.g. by the server or workstation, but a time stamp source may not be available for all SCADA components.

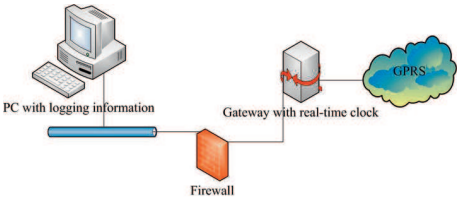

Fig. 3: Real-time Collection of the Data with Time Stamping in a Gateway

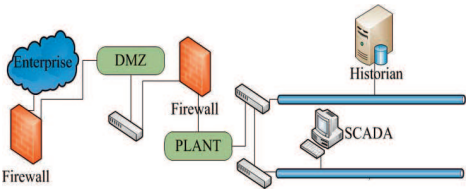

Fig. 4: Network Segmentation by Firewalls

4 Collecting Potential Digital Evidence

Collection of efficient and reliable data needed for forensic analysis cannot be fully extracted from numerous traditional device and control systems technologies due the nature of the technologies in question [Hs08] [Ed15]. Collecting evidence from servers and mobile equipment e.g. maintenance laptop, is not an issue as logging capability is available. But, collecting evidence from embedded devices is challenging as logging is not available and any transfer of evidence must be properly secured.

4.1 Regular Collection of Logging Information

Many challenges with regular collecting of logging information exist, e.g. restricted access to high security zones. Providing additional access, just to read the logging data brings in security risks. To overcome this issue additional firewalls can be implemented. Fig. 4 indicates an Industrial network that has been separated from an Enterprise network using Firewalls [Sc15].

Fig. 4 indicates Data Diode (DD) from High Security Zone to Low Security Zone, e.g. no manipulated command can be sent to SCADA system. Fig. 6 shows DD for transfer from an outside location of the utility e.g. intranet towards a Low Security Zone and no sensitive information will be stolen through Internet. Lower security zone, e.g. containing monitoring systems, needs connection only for time stamping.

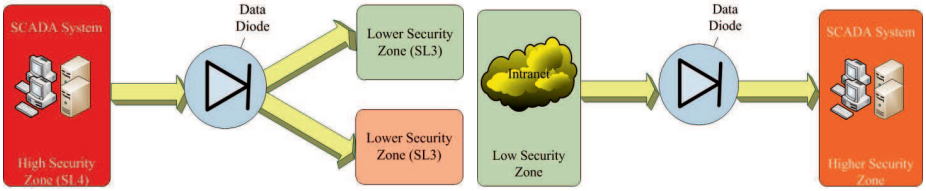

Fig. 4: Data Diode (High Sec. to Low Sec. Zone) Fig. 6: Data Diode (Low Sec. to Higher Sec.)

4.2 Identification of Users and Mapping to Roles

Identification of users is mandatory. No group logging should be allowed. However, multiple users may be assigned to the same role e.g. that allows them to change set-points of a SCADA component. This assures that they can perform their day-to-day work, assuming the respective work permits are issued (where appropriate), while a personal tracking of user activities related to the SCADA equipment is possible. When staff from multiple shifts is working with the same equipment, they need to login/logout. Therefore, efficient means for switching between users is needed.

4.3 Forensic Readiness for Maintenance Equipment

An essential aspect in preparing maintenance equipment for regular use during outages or for emergency situations is the incorporation of forensic readiness. The main idea is to assure that it was not manipulated, e.g. somebody replaces the software to be locally loaded. In this case, firewalls or a Physically Unidirectional Security Gateways [ISIE14a] are not applicable. Further, additional scanning before loading the new software to embedded devices is needed so that malicious software can be rejected or at least the loading behavior and authorized user will be recorded for forensic investigations.

4.4 Tamper Proof Logging

The following Building Technology and Data Diode example demonstrate how tamper proof logging is implemented and the purpose of a Physically Unidirectional Security Gateway (Data Diode).

4.4.1 Building Technology Example

Traditionally Building Technology (BT), often also called (Industrial) Facility Management, contained some security controls that still meet current cybersecurity recommendations [LW15]. For example, the commonly deployed logging of access of persons to different plant areas on a paper roll is definitely tamper-proof and can be used when addressing non-repudiation, as in Fig. 5, Current BT equipment, like heavy doors

or gates, includes automation equipment, usually with an electronics cabinet and a pneumatic cabinet per heavy gate. As an example, Fig. 5 also indicates how the networks connected to these gates have to be designed, in order to assure that an additional, completely independent monitoring and logging is in place [IEC611]. Tamper-proof logging on paper rolls is still in place. However, new cybersecurity technologies like Security Information and Event Management (SIEM) complement these [Ba16a].

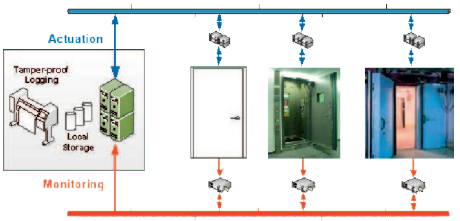

Fig. 5: Building Technology Example

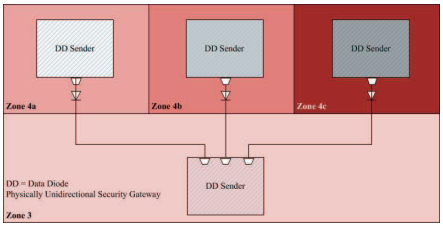

Fig. 8: Data Diode Example

They have to be considered in the Criticality Analysis with regard to correlating logging information of I&C and Electrical Systems (ES) with monitoring information provided by BT [WLZ15]. This logging information is also important with regard to Emergency Preparedness [Hs15] and protecting Critical Digital Assets from tampering [MT15].

4.4.2 Data Diode Example

According to the industrial facility specific security zone model, monitoring of systems through secure zone boundaries (security conduits) is required, in line with IEC 62443-3-3. Therefore, zone perimeter security policies must allow the transfer of security logs and events produced by monitoring devices to a central management system [WLZ15].

Data diodes can support the implementation of solutions that meet requirements of high security levels, as shown by the example in Fig. 8 [KL14]. As physical separations, they assure that the information flow is in one direction—away from the zones with higher security levels and in the direction of the central management system [Ba16a]. Additionally, data diodes make sure there is no capability for malicious traffic to penetrate the secure zone from the logging facility [KL14].

5 Graded Forensic-related Security Controls

For graded forensic-related security controls, a graded level of review stringency and testing depth is needed. Forensic-related security controls should be implemented, reviewed and tested according to security level presented in Fig. 6. Therefore, auditing on workstations, servers, and network devices must be permitted; audit records should be stored on centralized log servers. Critical applications should be configured towards auditing, including recording authentication attempts. Because logs manipulated, preparations, e.g. through their policies, guidelines, and procedures, should be done to

demonstrate the trustworthiness and integrity of such logs. Proactive approach should be considered in collecting valuable data. Configuring auditing on SCADA system, employing centralized logging, and implementing and using security monitoring controls in different security can all produce sources of data for further forensic efforts. In addition, Automated Asset Identification should be implemented.

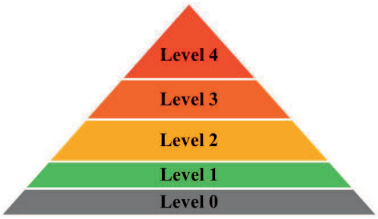

Fig. 6: Security Levels

Security levels are a concept that describes the degrees of security protection needed by different SCADA systems. Each level requires different sets of forensic-related security controls implemented in each security level satisfy the security requirements of that level [IEC614]. Multiple schemes and numbers of security levels or security grades are deployed by different industrial domains, e.g. four security levels according to IEC 62443 and as indicated in Fig. 6.

5.1 Automated Asset Identification

As mentioned in previous sections, Asset Management System needs to be implemented in order to assure an initial identification of assets at the right level of detail and for subsequent enforcement of identification updates after ongoing modifications. This can be supported by Asset Management Tools, including software modules for automatic asset identification. Automated asset identification may not be applicable for higher security zones either because it introduces an additional risk or because the SCADA components do not support automatic asset identification functionalities.

6 Forensic Readiness during all SCADA Lifecycle Phases

Incorporating forensic readiness into the SCADA system lifecycle phases, e.g. during development, leads to more successful control of security incidents. Examples include configuration management, change management, and validation and verification.

6.1 Configuration Management Processes and Assessment

Configuration management process is essential for the security of the SCADA hardware and software configurations. Each system alteration could have severe consequences on

its security [Pa13]. Therefore, system alteration must be properly assessed. Any modification could bring vulnerabilities that weaken security. Configuration management starts with properly tested and acknowledged security baselines for SCADA systems [Pa13]. Strong performance assessments are required in order to get successful forensic readiness during all SCADA lifecycle phases. Regular vulnerability assessment and automated auditing of the network and systems are essential part of the configuration management process [Pa13]. During development, it must be assured what is logged for changes of source code. In addition, reliance is on a configuration management system with logging enabled (assumptions, e.g. like ClearCase, that code is deleted, but all operations, including deletion, are recorded).

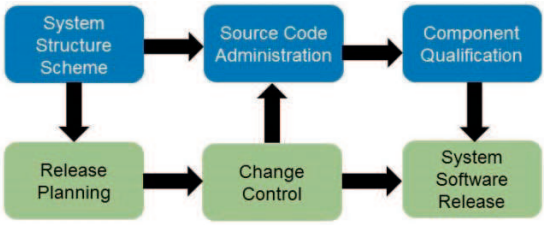

Fig. 7: Configuration Control

Configuration controls as outlined in Fig. 7 is also important against the insider threat as it ensure that I&C software employed by the customer is not maliciously manipulated during the software development lifecycle and during the software employment.

Each software component is uniquely identified according to a scheme of structured configuration IDs. Thus, e.g. a function block library (which may be mandatory for a high Safety Integrity Level and accordingly for e.g. SL3 or SL4 according to IEC 62443) is identified as one component and additionally each included function block is identified as an individual configuration management entity.

6.2 Change management

The purpose of change management is to manage the consequences of alterations in SCADA system configurations. In addition, it also prevents modifications that could have harmful impact to the security posture of a system. Therefore, modifications to an asset are only performed in a controlled manner. The process of managing changes reduces the risk of any changes made to a system, e.g. as insertions, installations, deletions and modifications that result in a compromise to system or data. To minimize risks of possible unfavorable consequences, the change management procedure requires verification of changes prior to implementation. In addition, risk assessment is conducted on all changes to the SCADA network that could have an impact on security, including configuration changes, the addition of network components, and installation of software [NIST11]. The current SCADA network configuration must always be well-known and documented [NIST11].

6.3 Verification and Validation (V&V)

V&V processes are associated to the analysis, evaluation, review, inspection, assessment, and testing of systems, software, hardware, and their interfaces in different lifecycle phases [ISII13]. These processes ensure that the final product meets the design anticipations. V&V is done using a graded approach according to IEC 62443.

7 Conclusion

Modern SCADA systems are dependent on information technology to operate efficiently. Understanding and monitoring SCADA networks and asset management are essential elements in discovering cyberattacks and performing subsequent forensic analyses [LL15]. During digital forensics investigation, proper time stamping and recording of events is required but it is achieved only if a high precision reference clock is available. In addition, many challenges with regular collecting of logging information exist, e.g. restricted access to high security zones. Providing additional access, just to read the logging data brings in security risks. Furthermore, an essential aspect in preparing maintenance equipment for regular use during outages or for emergency situations is the incorporation of forensic readiness. The main idea is to assure that it was not manipulated, e.g. somebody replaces the software to be locally loaded. In this case, firewalls or a Physically Unidirectional Security Gateways [ISIE14a] are not applicable. Further, additional scanning before loading the new software to embedded devices is needed. Forensic-related security controls should be also implemented, reviewed and tested according to security level. Auditing on workstations, servers, and network devices must be permitted; audit records should be stored on centralized log servers. Incorporating forensic readiness into the SCADA system lifecycle phases, e.g. during development, leads to more successful control of security incidents. Examples include configuration management processes and assessment, change management, and V&V.

References

[AIJ12] Al-Nemrat, A.; Ibrahim, N.; Jahankhan, H.: Sufficiency of Windows event log as evidence in digital forensics. University of East London, London, 2012.

[Ba16a] Bajramovic, E. et.al.: Cybersecurity Aspects in the I&C Design of Nuclear Power Plants. 3rd INPPS, Istanbul, 03.2016.

[Ba16b] Bajramovic, E. et.al.: Forensic Readiness of Smart Buildings: Preconditions for Subsequent Cybersecurity Tests, Trento, 09.2016 (unpublished yet).

[Bm16] Studie i.A. des BMWi IT-Sicherheit für die Industrie 4.0 Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten, 2016.

[Ed15] Eden, P. et.al.: A Forensic Taxonomy of SCADA Systems and Approach to Incident Response. 3rd International Symp. for ICS & SCADA Cyber Sec. Research, 2015.

[EGI13] ETSI GS ISI 002: Information Security Indicators (ISI) — Event Model — A security event classification model and taxonomy, 2013.

[EGI14] ETSI GS ISI 003: Information Security Indicators (ISI) — Key Performance Security Indicators (KPSI) to evaluate the maturity of sec. event detection, 2014.

[Hs08] Recommended Practice: Creating Cyber Forensics Plans for Control Systems. Homeland Security, 08.2008.

[Hs09] Recommended Practice: Developing an ICS CSIR Capability, 10.2009.

[Hs16] Preparing for Cyber Incident Analysis. The National Cybersecurity and Communications Integration Center, Homeland Security, 2016.

[HS15] Hollern, J.; Stringfellow, P.: Considerations for Integrating CS Reqs into the Nuclear Facility Emergency Preparedness Plan, 9th NPIC, Charlotte, 2015.

[IEC611] IEC 61513: NPPs — I&C Sys. Important to Safety — General Req. for Systems, 2011.

[IEC613] IEC 62443-3-3: Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels, 2013.

[IEC614] IEC 62645: NPPs – I&C–Req. for sec. programmes for computer-based systems, 2014.

[IEC615] IEC 62443-4-2: Security for IACS – Part 4-2: Technical security requirements for IACS components, 2015.

[ISO514a] ISO 55001: Asset management — Overview, principles and terminology, 2014.

[ISO514b] ISO 55001: Asset management — Management systems — Requirements, 2014.

[ISIE11a] ISO/IEC 27035: IT — Security techniques —Inf. security incident management, 2011.

[ISIE12a] ISO/IEC 19770-1: Software Asset Management — Processes and tiered assessment of conformance, 2012.

[ISIE12b] ISO/IEC 27037: IT — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence, 2012.

[ISIE14a] ISO/IEC 27033-4: IT — Security techniques — Network security — Part 4: Securing communications between networks using security gateways, 2014.

[ISIE14b] ISO/IEC 27036-2: IT — Security techniques — Information security for supplier relationships — Part 2: Requirements, 2014.

[ISIE14c] ISO/IEC 27038: IT — Sec. techniques — Specification for dig. redaction, 2014.

[ISIE15a] ISO/IEC 19770-2: SW Asset Management — Software Identification Tag, 2015.

[ISIE15b] ISO/IEC 19770-5: IT Asset Management — Overview and Vocabulary, 2015.

[ISIE15c] ISO/IEC 27040: IT — Security techniques — Storage security, 2015.

[ISIE15d] ISO/IEC 27041: IT — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method, 2015.

[ISIE15e] ISO/IEC 27042: IT — Security techniques — Guidelines for the analysis and interpretation of digital evidence, 2015.

[ISIE15f] ISO/IEC 27043: IT — Security techniques — Incident investigation principles and processes, 2015.

[ISIE16a] ISO/IEC DIS 27050-1[Draft]: IT — Security techniques — Electronic discovery — Part 1: Overview and concepts, 2016.

[ISIE16b] ISO/IEC WD 27050-2 [Draft]: IT — Sec. techniques — Electronic discovery — Part 2: Guidance for governance and management of electronic discovery, 2016.

[ISII13] ISO/IEC/IEEE 29119-1: Software and systems engineering — Software testing — Part 1: Concepts and definitions, 2013.

[KL14] Knapp, E.; Langill, J.: Security Monitoring of Industrial Control Systems. In Industrial Network Security. 2nd Edition. Syngress Publishing, 29.12.2014.

[Le15] Lee, R.: Active cyber defense cycle: Asset identification and network security monitoring. Control Engineering, 03.06.2015.

[LL15] Lee, R.; Luallen, M.: Making digital forensics a critical part of your cyber security defenses, Control Engineering, 15.01.2015.

[LW15] Lillo, E.; Waedt, K.: Challenges in Considering National and International CS Requirements and Performing a Criticality Analysis, IAEA Conf., Vienna, 06. 2015.

[MT15] Martyak, P.; Thow, M.: Enhancing Defense-in-Depth and Monitoring Programs to Protect CDAs from Tampering, NPIC & HMIT Charlotte, 2015.

[NERC09a] Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets. NERC, 17.10.2009.

[NERC09b] Security Guideline for the Electricity Sector: Time Stamping of Operational Data Logs. NERC, 2009.

[NIST11] NIST SP 800-82: Guide to Industrial Control Systems Security, 06.2011.

[NIST06] NIST SP 800-92: Guide to Computer Security Log Management, 09.2006.

[Pa13] Paganini, P.: Improving SCADA System Security. INFOSEC Institute. 06.12.2013.

[Sc15] Scott, A.: Tactical Data Diodes in IACS. SANS Institute, 18.05.2015.

[Ta13] Taveras, P.: SCADA Live Forensics: Real Time Data Acquisition Process to Detect, Prevent or Evaluate Critical Situations. 1st Internat. Conf., Azores, 24.04.2013.

[Wa16] Waedt, K. et.al.: Automatic Assets Identification for Smart Cities: Prerequisites for Cybersecurity Risk Assessments, Trento, 09.2016 (unpublished yet).

[WD14] Waedt, K.; Ding, Y.: IT Security / Interoperability. 1st Sino-German Intelligent Manufacturing/Industry 4.0. Standardization Summit Forum, Shanghai, 16.12.2015.

[WLZ15] Waedt, K.; Lillo, E.: Zavarsky, P.: Identification of the Critical Components of an ICS and Options to Protect Them, WINS. Workshop on Effective Integration of Physical Protection and Cyber Security, Vienna, 02. 2015.