2018

Detection techniques in operational technology infrastructure

Glenn Murray
Edith Cowan University, g.murray@ecu.edu.au

Matthew Peacock
Edith Cowan University, m.peacock@ecu.edu.au

Priya Rabadia
Edith Cowan University, p.rabadia@ecu.edu.au

Paresh Kerai
Edith Cowan University, p.kerai@ecu.edu.au

DOI: 10.25958/5c52780566692
Murray, G., Peacock, M., Rabadia, P., & Kerai, P. (2018). Detection techniques in operational technology infrastructure. In *proceedings of the 16th Australian Information Security Management Conference*(pp. 97-105). Perth, Australia: Edith Cowan University.

DETECTION TECHNIQUES IN OPERATIONAL TECHNOLOGY INFRASTRUCTURE

Glenn Murray, Matthew Peacock, Priya Rabadia, Paresh Kerai
School of Science, Edith Cowan University, Perth, Australia
{g.murray, m.peacock, p.rabadia, p.kerai}@ecu.edu.au

Abstract

In previous decades, cyber-attacks have not been considered a threat to critical infrastructure. However, as the Information Technology (IT) and Operational Technology (OT) domains converge, the vulnerability of OT infrastructure is being exploited. Nation-states, cyber criminals and hacktivists are moving to benefit from economic and political gains. The OT network, i.e. Industrial Control System (ICS) is referred to within OT infrastructure as Supervisory Control and Data Acquisition (SCADA). SCADA systems were introduced primarily to optimise the data transfer within OT network infrastructure. The introduction of SCADA can be traced back to the 1960's, a time where cyber-attacks were not considered. Hence SCADA networks and associated systems are highly vulnerable to cyber-attacks which can ultimately result in catastrophic events. Historically, when deployed, intrusion detection systems in converged IT/OT networks are deployed and monitor the IT side of the network. While academic research into OT specific intrusion detection is not a new direction, application to real systems are few and lack the contextual information required to make intrusion detection systems actionable. This paper provides an overview of cyber security in OT SCADA networks. Through evaluating the historical development of OT systems and protocols, a range of current issues caused by the IT/OT convergence is presented. A number of publicly disclosed SCADA vulnerabilities are outlined, in addition to approaches for detecting attacks in OT networks. The paper concludes with a discussion of what the future of interconnected OT systems should entail, and the potential risks of continuing with an insecure design philosophy.

Keywords

SCADA, Operational Technology, Critical Infrastructure, OT Protocols, Network Security

INTRODUCTION

The global cost of cybercrime has risen by 66% to an average cost of USD$11.7 million per organisation since 2015 (Ponemon Institute LLC, 2017). In Australia, an average per company attributed USD$5.41 million to cyber-attacks (Ponemon Institute LLC, 2017). This upward trending figure is potentially catastrophic to the political and economic state of a country such as Australia. Following the targeted use of ransomware on critical infrastructure such as the Kemuri Water Company (Kovacs, 2016), developing defences, which include detection techniques, against the offensive use of cyber weaponry is essential.

Supervisory Control and Data Acquisition (SCADA) systems were introduced to automate processes in industries such as oil and gas, water utilities, transportation, power generation and energy. SCADA systems allow operators to monitor and communicate with onsite systems remotely through a Human Machine Interface (HMI). This action of remotely controlled and monitoring the onsite systems has the advantage of a reduction in labour costs and minimise associated errors associated with measurements. Furthermore, inbuilt alarm systems can be monitored automatically rather than having humans checking with the risk of potentially miscalculating critical data.

However, increased connectivity has introduced significant vulnerabilities from IT environments that previously did not exist in OT environments. Cyber criminals have identified these vulnerabilities and have exploited for financial and/or political gain. This paper presents an overview of OT systems, describing historical design choices, system architecture, and vulnerabilities introduced from the convergence of IT and OT systems. Next, the paper describes intrusion detection methods for OT systems, concluding with a discussion on what is required to secure future OT systems from an increasing cyber threat.

SCADA SYSTEM EVOLUTION

As information/data architectures and technology has evolved, including the convergence of IT and OT technologies, the evolution of SCADA systems has also followed. SCADA systems started in the 1960's and are commonly separated into four generations:

- First Generation – Monolithic SCADA Systems;
- Second Generation – Distributed SCADA Systems;
- Third Generation – Networked SCADA Systems; and
- Fourth Generation – "Internet of Things" SCADA Systems (Kudłacik, Porwik, & Wesołowski, 2016).

As SCADA systems have evolved, they have adopted open network specifications for communications. The evolution of protocols began with proprietary protocols including SCADA vendor specific protocols, e.g. Modbus and Profibus, later the SCADA protocols were standardised through, IEC60870, IEC61850 and DNP3. These protocols naturally have advantages, disadvantages and commonalities. As with advances in technology, industry has increased the availability of control systems from remote locations. This has changed the behaviour that SCADA processes the communications data from a predominately standalone system to communicating through Wide Area Networks (WANs) and Local Area Networks (LANs) through TCP/IP protocols. Furthermore, the improvement of networking technology resulting in network speed increases has increased the uptake of TCP/IP protocols within OT systems. These improvements have hastened the move from EIA-232 and EIA-485 (serial) to Ethernet and wireless (DigitalBond, 2018) mediums. There has also been a shift in the technology and functionality associated with microprocessor devices or intelligent electronic devices (IEDs). This shift is to take advantage of the increased network speeds and different transmission mediums, allowing for more complex systems with finer timing requirements to be designed.

SCADA NETWORK ARCHITECTURE

SCADA systems operate on a node-to-node based topology that runs on the Data Link Layer (Layer Two) of the Open Systems Interconnection (OSI) model that had been designed as a closed system. SCADA systems are used to allow operators to monitor alerts and analyse real-time data collated from distributed processes such as gas pipelines, hydroelectric generating facilities and power stations. Traditional SCADA systems are comprised of five main components: Intelligent Electronic Device (IED) (Kolhar, Abd El-atty, & Rahmath, 2016), Programmable Logic Controller (PLC), Remote Telemetry Unit (RTU), Human Machine Interface (HMI) and Historian system. The IEDs are microcomputer sensors that monitor the physical SCADA machine and relay data to the PLC or RTU devices. PLCs and RTUs are devices that collect data from the IEDs then transmit the data to the HMI application. An HMI is an application installed on a SCADA workstation that interprets the information received from the PLC and RTU devices, allowing for a human operator to analyse and monitor the SCADA system. The Historian system collects and stores SCADA network data for audit purposes (Nicholson, Webber, Dyer, Patel, & Janicke, 2012).

Figure 1 illustrates a simple SCADA network architecture. Typically, a SCADA network architecture is a tree-like structure and was designed as a closed system. The convergence of IT and OT systems have changed the architecture of OT systems, with HMI workstations often connected to corporate intranets, with remote access provided through virtual private networks (VPNs) or other remote access technologies. With these added connections, OT infrastructure such as SCADA systems are exposed to vulnerabilities inherited from the IT environment, opening vectors for network attacks against the SCADA system. This has increased the importance of securing organisational networks which manage SCADA systems.

One defensive method is the use of network segregation (Sajid, Abbas, & Saleem, 2016). Network segregation is separating an organisational network into sub-networks to mitigate against adversarial activities propagating through the organisational network. This technique should be deployed in conjunction with active and passive cyber defences. A firewall is an active cyber defence tool, commonly located at the entrance of the segregated network (Gao et al., 2014). Firewall rules and policies should be implemented to monitor inbound and outbound SCADA network traffic. A correctly configured firewall located on a segregated SCADA network should be deployed along with an Intrusion Detection System (Sajid et al., 2016; SURF cert IDS, 2013). An IDS is a passive cyber defence tool that monitors network traffic for any anomalous behaviour that could be attributed to adversarial activities. An IDS should be placed within the SCADA network allowing for the detection of adversarial activities. Though it is important to note that firewalls and IDSs are only as effective as the rules and policies configured on these tools. With weaker rules and policies adversarial activities can go undetected on SCADA systems. Further, an IDS is only useful when the alerts which are generated are investigated. The use of

various defence tools and techniques is known as a defence in depth strategy and should be deployed to mitigate the vulnerabilities of OT systems such as SCADA.

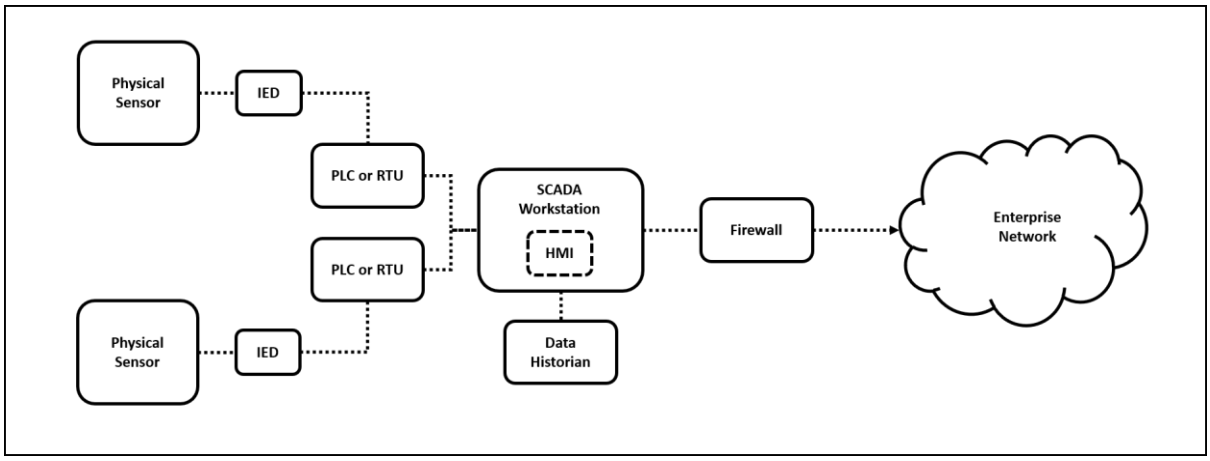

Figure 1: A simple SCADA network topology

Companies by nature aim to increase a return to their shareholders, therefore there is a requirement to optimise their respective plants to achieve an increase in production and in turn revenue. This translates to optimised performance and reduced overhead costs. To achieve this, access to the OT environment from the IT enterprise domain was required to conduct analysis. This forced the convergence of IT to OT. The devices within the OT environment were not designed to defend against cyber-attacks like those seen within the IT environment. Hence this has left OT devices highly exposed (Murray, Johnstone, & Valli, 2017). Therefore it is acknowledged that the increasing complexity of OT networks caused by IT connections requires tailored OT defence measures, such as intrusion detection and intrusion prevention systems which counter vulnerabilities in both OT devices and network protocols (Horkan, 2015).

SCADA SYSTEM VULNERABILITIES

SCADA systems started as standalone systems, with a defined gap between the IT systems and the OT systems, with no access to the outside world, not alone the Internet. The early associated SCADA protocols were propriety and the connections were through an RS-232 low speed serial cable (Shahzad et al., 2016). The original design of SCADA systems was to ensure an optimised transfer of data, i.e. no data loss. There wasn't any thought to the SCADA design to include cybersecurity requirements.

To capture the vulnerability of SCADA systems, it is important to understand how an attack on a traditional IT system has different priorities than an attack on an OT system. Traditionally in IT security where the concerns are associated with financial integrity, denial of service or loss of information, properties can be grouped into confidentiality, integrity and availability or CIA. This is also in the order of importance within an IT system. Within an OT system, the order of importance is reversed to availability, integrity and then confidentiality. This change of importance is due to the difference in conditions between IT and OT. In IT, data is paramount where all processes are within the virtual environment. In OT, production is the number one requirement. There is a crossover from the virtual environment to the physical environment, e.g. process control. Therefore in the OT environment, there is a requirement for effective operation of the onsite plant and to ensure data is presented in case of an emergency (Murray et al., 2017).

The purpose of an adversary can range from an individual who is trying to see if they can defeat the defences of a plant. Conversely, it could be a nation state for the purposes of industrial espionage. As seen through the Triton attack on a middle eastern oil and gas plant where the intent was to cause a high impact attack (Johnson et al., 2017). Since Stuxnet, publicly reported cyber-attacks against OT systems have increased, a selection of which are presented in Table 1.

Table 1: Selected disclosed OT cyber-attacks, expanded from (Murray et al., 2017)

Year	Cyber Attack	Details	Outcome
2010	Stuxnet worm	A sophisticated malware was installed via a third-party contractor using a USB drive to an Iran nuclear facility. The malware infected the SCADA system controlling the Nuclear centrifuges and changed the values and mechanics to behave abnormal (Schneier, 2010).	Nuclear Centrifuges and valves were sabotaged/destroyed
2011	Steel plant infected with Conficker worm	Network and Computer systems infected with the Conficker worm, which spread across the corporate and OT network systems. Communications between the PLCs and field devices were flooded, causing most control system devices in become unresponsive (RISI, 2015).	The malware spread throughout the network and impact the communication of SCADA systems and field devices, which resulted to latency and partial outage on the SCADA network.
2012	Computer Virus targets Saudi Arabian Oil Company	Nation state hackers attacked Saudi Aramco with the Shamoon virus which infected 30,000 computers across the network, wiping hard drives (Bronk & Tikk-Ringas, 2013).	30,000 corporate computers systems wiped clean. The corporate network was down for several days.
2012	Shamoon virus affects computers at Qatari gas firm RasGas	Qatari gas firm RasGas became infected with the Shamoon virus. The attack was believed to be state sponsored (Mills, 2012).	The website and corporate network of the organisation was impacted for several days.
2012	Canadian Software Manufacturing Company Firewall Breach	Adversaries compromised the firewall system of Telvent Canada Ltd, stealing critical project SCADA files that were related to the OASyS SCADA project (Krebs, 2012)	Theft of critical and sensitive project files related to SCADA systems.
2012	US Power Plant Infected with Malware	The malware was identified on a USB drive used for control system configuration backups in a US nuclear powerplant (Sanger, 2013).	Compromised ICS system with an undisclosed impact to the operation.
2014	US Public utility compromise	Adversaries compromised a security system at a US public utility through a brute-force password attack (Kirk, 2014).	The system was not directly connected to other OT equipment due to maintenance.
2014	Dragonfly Group Energy Industry reconnaissance campaign	Reported that adversary group called Dragonfly have been targeting the energy sector in the US and Europe. Using IT based vectors, such as phishing emails to pivot into OT networks (Braga, 2017).	Undisclosed, expected loss of critical assets information and business operations process
2014	German Steel Mill attack	A German Steel Mill was breached using social engineering vectors to enter the company network and further compromise the control system network. The compromise resulted in preventing a blast furnace from shutting down when required (Robert M Lee, Asante, & Conway, 2014).	Catastrophic damage to the steel mill.
2015	Blackenergy3 Ukraine power grid cyber-attack	A suspected nation state adversary group attacked a regional Ukraine power company, compromising the ICS network causing a 3 hour power outage (Robert M. Lee, Assante, & Conway, 2016).	225,000 customers lost power, deleted files from the master boot records and shut down communications.
2015	Kemuri Water Plant	Adversary compromised a water utility online billing system, pivoting into the SCADA network servers and holding the utility company ransom (Leyden, 2016).	Modified chlorine and chemical levels on the water used at the treatment plants. 2.5 million customer details stolen.
2017	Triton	An oil and gas plant in Saudi Arabia was compromised through remote access to an engineer workstation. The adversary reprogrammed controller units, causing fail safes to occur shutting down the plant (Johnson et al., 2017).	Failsafe systems worked correctly

APPROACHES TO DETECTING NETWORK ATTACKS IN OT

For detection of system-level events on specific devices operating in OT, operating system logs, and host-based intrusion detection systems can be used. Host-Based intrusion detection systems (HIDS) monitor for system changes in the device which the system monitors. HIDS however, utilise resources on the device it is monitoring and thus are not commonly used in OT devices due to device resource constraints. System logs detail events which occur on a device at an operating system-level and network-level. System logs are generated automatically by IT devices but are not generated by default in OT devices. Typically, system logs from both device types when available are sent to a server device for correlation and analysis. A downside of system logs in general is the potential for tampering by an adversary. Given the data provided to the log server is provided by a potentially untrustworthy source, i.e the adversary-controlled device, system logs may provide less meaningful data for sophisticated, targeted attacks undertaken by organised adversaries, such as the BlackEnergy malware kit (MITRE ATT&CK, 2018).

Network capture is used as part of Network Intrusion Detection Systems (NIDS). Network captures record network traffic occurring over a network, often using a standalone device and either at a flow-level or packet-level. Network flows describe a series of network packets over a defined time duration, keeping high-level information such as source, destination, protocol and packet length (J. Quittek, 2004). Packet level captures record all information for each individual packet traversing a network. Due to finite storage requirements, network flows are often used given the reduced storage requirement, however, the lack of semantic knowledge of the underlying processes provided by network flows restricts their applicability to actionable detection measures (Hofstede et al., 2014). Conversely, deep packet inspection provides all the semantic data regarding each network transaction, with the added cost of increased storage. Drawing meaning from this wealth of knowledge however, is challenging, as detection systems can be overwhelmed with noise. Filtering the noise is required to identify appropriate indicators for detection. Indicators can be derived from expert knowledge of the individual system, learnt automatically using machine learning approaches, or a combination of automated learning and expert acceptance.

For intrusion detection systems, there are two core designations, misuse (signature) based, and anomaly based. Misuse based approaches are highly accurate at detecting known malicious events, given a rule is developed/exists and is used. However, they cannot detect unknown attacks (Yuksel, den Hartog, & Etalle, 2016). Signatures exist for a range of OT protocols, including ModBus, S7 and DNP3 (Bro, 2018; DigitalBond, 2018; Open Information Security Foundation, 2018b) , through a range of open source signature IDS systems, such as Bro, Snort, Suricata and Yara (Amann et al., 2018; CISCO, 2018; Open Information Security Foundation, 2018a; VirusTotal, 2018). Alternatively, anomaly-based approaches use a learned model of normal transactions to identify anomalies in data, based on either protocol semantics, process data, network transaction probabilities or physical process models. A range of anomaly approaches based on the use of machine learning exist in literature such as (Carcano et al., 2011; Caselli, Zambon, & Kargl, 2015; Yuksel et al., 2016), however, commercial machine learning anomaly detection approaches are typically closed source. The difficulty with anomaly detection is understanding what detected anomalies mean in the context of the system. For this reason, systems which automatically act on anomalies are detrimental in OT networks, given the potential effect and risk to system availability if a false positive is acted upon (NIST, 2007). While OT systems are more static than IT systems, if the behaviour is not learnt during the training process, it will be classified as an anomalous action, even if it is a low interaction normal device. Further, if adversary actions are already taking place in the network, the malicious behaviour may be baselined (NIST, 2007). A means of online learning is required to increase the usability of many anomaly detection approaches for OT systems.

DISCUSSION

The convergence of IT and OT systems has left OT devices exposed, as outlined by attack vectors used in OT cyber-attacks. As noted by (Gregory-Brown, 2107) the devices that are perceived to be at the highest risk are IT devices such as servers and workstations. These devices provide the entry vectors into OT systems and networks through IT based vulnerabilities and then pivot into the internal OT network (Knapp & Langill, 2015). A summary of attack vectors for 39 reported attacks collated from the RISI database between 2010 and 2014 are outlined in Table 2. While the majority are undisclosed from this database, initial attack vectors are not complex, with unauthorised access in these cases achieved through default credentials, or insider attackers, while USB based entry vectors traverse network defences. Domain awareness of OT cyber threats is increasing with (Schwab Wolfgang & Mathieu, 2018) reporting 77% of respondents identifying ICS cybersecurity as a major priority in 2018. A major challenge is the slow pace of OT system lifecycles when compared to IT systems.

Table 2: OT entry vectors collated from RISI (2015)

Entry Vector	**Total Reported (%)**
Undisclosed	22 (56.4%)
Unauthorised Access	9 (23.1%)
USB	6 (15.4%)
Social Engineering	1 (2.6%)
Phishing	1 (2.6%)

OT environments such as SCADA systems were designed as closed systems, however the IT and OT convergence has resulted in SCADA systems being connected to other networks including enterprise networks and the Internet for productivity increases. Additionally, the order of security concerns within an IT environment is different to those of the OT environment. Confidentiality of data is considered to be of utmost importance within the IT environment, while the availability of data and services is of utmost importance within the OT environment (Rezai, Keshavarzi, & Moravej, 2017; Zhu, Joseph, & Sastry, 2011). Given the differences in both environments, IT based detection techniques are not adequate to detect OT threats (Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, & Hahn, 2015). The focus of current research is on OT specific detection techniques and method (Cherdantseva et al., 2016; Gao et al., 2014)

Detection in OT systems should leverage the wealth of knowledge provided by IT systems. Correlating system, network and threat intelligence alerts between IT and OT systems can provide a whole system view for security analysts who draw meaning from these complex interconnected systems. Given that the entry vector for OT cyber-attacks are typically IT based due to system convergence, drawing inferences between actions in the whole system will provide efficient, actionable remediations.

A key to having secure and controlled OT network and environments is hardening OT networks and systems with a security focus. A deep understanding of both OT network architectures and IT network systems is required to harden the environment. A defence in depth approach is key to hardening OT networks, including network segmentation, firewalls and intrusion detection systems. However, securing OT systems requires more than technical solutions. Policy, both internal and industry compliance, staff training and testable incident response plans are also required (NIST, 2015).

Current anomaly detection approaches for OT systems rely on identifying variations in features of interest to identify anomalies. These features are typically frequency based, such as an increase in connections from a host, when compared to historical learnt behaviours. These features can be learnt from network data, process-based semantics such as device or protocol definitions, and behaviours defined by system experts. The end result of current anomaly detection alarms is an indicator that a value has deviated from normal. Additional semantic meaning is required to evaluate if this is an indication of a cyber-attack or an infrequent normal action. Advanced adversarial threats can overcome existing anomaly detection approaches when conforming to normal learnt action. However, combining categorical data, such as command type or function code, with frequency based and time-based features into compound features provides both additional semantic meaning to alerts, in addition to richer classification approaches. For example, using a write function may be defined as a normal action between two devices, but added contextual behaviour, such as the value being written, and the time of transaction may indicate a network attack when compared to normal operations. Future anomaly detection approaches for OT systems should incorporate both process level semantics, and contextual behaviour to improve the rigour of anomaly detection.

Ultimately, improved security of OT systems requires a fundamental change in the development mindset of OT systems. From the hardware-level to high-level network protections, future OT networks will need to be designed to be robust and secure, while maintaining the safety and availability requirements as convergence between IT and OT systems manifests into the Industrial Internet of Things (IIoT). Further, the protocols which are currently used in OT systems require updating to modern secure design standards. Existing protocols are insecure by design and attempts to secure these protocols are met with resistance, or not integrated due to the optionality requirements of the security functions for backwards compatibility with existing systems. Schneider Electric has recently undertaken this process with the creation of Secure Modbus TCP, which uses Transport Layer Security (TLS), digital certificates and role-based access control (Desruisseaux, 2018). While rebuilding protocols to embed security from design can be costly, this approach to improving the security of OT protocols will provide the robust security requirements of future connected OT systems.

CONCLUSION

This paper sought to highlight current detection techniques in OT systems, and identify existing known challenges and goals for the next generation of OT system, the Industrial Internet of Things (IIoT). OT systems such as SCADA systems were originally designed as closed systems. However, the evolution of information/data architectures and the convergence of IT and OT environments has driven the evolution of SCADA systems to adopt an open network specification for communications. With the inclusion of added connections due to the adaptation of an open network, OT infrastructure such as SCADA systems are exposed to vulnerabilities inherited from the IT environment, opening vectors for network attacks against the SCADA system. In recent years cyber-attacks have been launched exploiting vulnerabilities against OT systems.

Mitigation strategies such as a defence in depth security approach to hardening OT networks could be implemented. In addition to gathering threat intelligence alerts from both IT and OT environments as well as incorporating process level semantics and contextual behaviour for an anomaly based detection approach. As the latest evolution of OT systems are IIoT based, rebuilding OT protocols with security embedded in the design is costly but will provide the robust security requirements of future connected OT systems.

REFERENCES

Amann, Azoff, Fleury, Grigorescu, Hall, Paxson, . . . Vallentin. (2018). Bro Network Security Monitor. Retrieved from https://www.bro.org/

Braga, M. (2017). Russia-linted hackers infiltrated US and European energy companies, security firm finds. *CBC News*. Retrieved from https://www.cbc.ca/news/technology/russia-dragonfly-energetic-bear-hacking-energy-us-symantec-1.4276999

Bro. (2018). Bro Protocol Analysers. Retrieved from https://www.bro.org/sphinx/script-reference/proto-analyzers.html

Bronk, C., & Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. *Survival, 55*(2), 81-96. doi:10.1080/00396338.2013.784468

Carcano, A., Coletta, A., Guglielmi, M., Masera, M., Fovino, I. N., & Trombetta, A. (2011). A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems. *Industrial Informatics, IEEE Transactions on, 7*(2), 179-186.

Caselli, M., Zambon, E., & Kargl, F. (2015). *Sequence-aware Intrusion Detection in Industrial Control Systems.* Paper presented at the Proceedings of the 1st ACM Workshop on Cyber-Physical System Security.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security, 56*, 1-27. doi:https://doi.org/10.1016/j.cose.2015.09.009

CISCO. (2018). Snort. Retrieved from https://www.snort.org/

Desruisseaux. (2018). Modbus Security - New Protocol to Improve Control System Security. Retrieved from https://blog.schneider-electric.com/machine-and-process-management/2018/08/30/modbus-security-new-protocol-to-improve-control-system-security/

DigitalBond. (2018). Digital Bond's IDS/IPS rules for ICS and ICS protocols. . Retrieved from https://github.com/digitalbond/Quickdraw-Snort

Gao, J., Liu, J., Rajan, B., Nori, R., Fu, B., Xiao, Y., . . . Chen, C. L. P. (2014). SCADA communication and security issues. *Security and Communication Networks, 7*(1), 175-194. doi:10.1002/sec.698

Gregory-Brown, B. (2107). *Securing Industrial Control Systems - A SANS Survey*. Retrieved from https://www.belden.com/hubfs/resources/knowledge/white-papers/sans-survey-report-ics-security.pdf?hsLang=en&t=1531332510474

Hofstede, R., Čeleda, P., Trammell, B., Drago, I., Sadre, R., Sperotto, A., & Pras, A. (2014). Flow Monitoring Explained: From Packet Capture to Data Analysis With NetFlow and IPFIX. *IEEE Communications Surveys & Tutorials, 16*(4), 2037-2064. doi:10.1109/COMST.2014.2321898

Horkan, M. (2015). *Challenges for IDS/IPS Development in Industrial Control Systesms*. Retrieved from https://www.sans.org/reading-room/whitepapers/ICS/challenges-ids-ips-deployment-industrial-control-systems-36127

J. Quittek, T. Z., B. Claise and S. Zander. (2004). *RFC3917: Requirements for IP Flow Information Export (IPFIX)* (RFC3917). Retrieved from Online:

Johnson, B., Caban, D., Krotofil, M., Scali, D., Brubaker, N., & Glyer, C. (2017). Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. Retrieved from https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Kirk, J. (2014). Public utility compromised after brute-force attack, DHS says. *Computer World*. Retrieved from https://www.computerworld.com.au/article/545681/public_utility_compromised_after_brute-force_attack_dhs_says/

Knapp, E. D., & Langill, J. T. (2015). Chapter 3 - Industrial Cyber Security History and Trends. In E. D. Knapp & J. T. Langill (Eds.), *Industrial Network Security (Second Edition)* (pp. 41-57). Boston: Syngress.

Kolhar, M., Abd El-atty, S. M., & Rahmath, M. (2016). Storage allocation scheme for virtual instances of cloud computing. *Neural Computing and Applications*. doi:10.1007/s00521-015-2173-8

Kovacs, E. (2016). Attackers Alter Water Treatment Systems in Utility Hack: Report. Retrieved from https://www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report

Krebs, B. (2012). Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent. Retrieved from https://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/

Kudłacik, P., Porwik, P., & Wesołowski, T. (2016). Fuzzy approach for intrusion detection based on user's commands. *Soft Computing, 20*(7), 2705-2719. doi:10.1007/s00500-015-1669-6

Lee, R. M., Asante, M. J., & Conway, T. (2014). German Steel Mill Cyber Attack.

Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid

Leyden, J. (2016). Water treatment plant hacked, chemical mix changed for tap supplies. *The Register*. Retrieved from https://www.theregister.co.uk/2016/03/24/water_utility_hacked/

Mills, E. (2012). Virus knocks out computers at Qatari gas firm RasGas. *CNET*. Retrieved from https://www.cnet.com/news/virus-knocks-out-computers-at-qatari-gas-firm-rasgas/

MITRE ATT&CK. (2018). Indicator Removal on Host. Retrieved from https://attack.mitre.org/techniques/T1070/

Murray, G., Johnstone, M. N., & Valli, C. (2017). *Thee convergence of IT and OT in critical infrastructure*. Paper presented at the The Proceedings of 15th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia.

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security, 31*(4), 418-436. doi:https://doi.org/10.1016/j.cose.2012.02.009

NIST. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS) NIST.

NIST. (2015). Guide to Industrial Control Systems (ICS) Security: US Department of Commerce.

Open Information Security Foundation. (2018a). Suricata Open Source IDS / IPS / NSM engine Retrieved from https://suricata-ids.org/

Open Information Security Foundation. (2018b). suricata/rules/modbus-events.rules. Retrieved from https://github.com/OISF/suricata/blob/master/rules/modbus-events.rules

Ponemon Institute LLC. (2017). *Cost Of Cyber Crime Study - Insights On The Security Investments That Make A Difference* Retrieved from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Rezai, A., Keshavarzi, P., & Moravej, Z. (2017). Key management issue in SCADA networks: A review. *Engineering Science and Technology, an International Journal, 20*(1), 354-363. doi:https://doi.org/10.1016/j.jestch.2016.08.011

RISI. (2015). RISI Online Incident Database. https://www.risidata.com/Database

Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. *IEEE Access, 4*, 1375-1384. doi:10.1109/ACCESS.2016.2549047

Sanger, D. E. (2013). US plants hit by USB stick malware attack. *BBC*. Retrieved from https://www.bbc.com/news/technology-21042378

Schneier, B. (2010). The Story Behind teh Stuxnet Virus. *Forbes*. Retrieved from https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html - 4352814851e8

Schwab Wolfgang, & Mathieu, P. (2018). *The State of Industrial Cybersecurity 2018*. Retrieved from https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf

Shahzad, A., Lee, M., Xiong, N., Jeong, G., Lee, Y.-K., Choi, J.-Y., . . . Ahmad, I. (2016). A Secure, Intelligent, and Smart-Sensing Approach for Industrial System Automation and Transmission over Unsecured Wireless Networks. *Sensors, 16*(3), 322.

SURF cert IDS. (2013). SURF cert IDS. Retrieved from http://ids.surfnet.nl/wiki/doku.php

VirusTotal. (2018). YARA. Retrieved from https://yara.readthedocs.io/en/v3.7.0/

Yuksel, O., den Hartog, J., & Etalle, S. (2016). *Reading Between the Fields: Practical, Effective Intrusion Detection for Industrial Control Systems.* Paper presented at the Proceedings of the 31st Annual ACM Symposium on Applied Computing.

Zhu, B., Joseph, A., & Sastry, S. (2011). *A Taxonomy of Cyber Attacks on SCADA Systems*. Paper presented at the Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing.