Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Assessing and augmenting SCADA cyber security: A survey of techniques

Sajid Nazir [a,b,*], Shushma Patel [a], Dilip Patel [a]

[a] School of Engineering, London South Bank University, London SE1 0AA, UK
[b] Firstco Ltd., London W2 6EU, UK

ARTICLE INFO

Article history:
Received 30 October 2016
Received in revised form 17 May 2017
Accepted 26 June 2017
Available online 5 July 2017

Keywords:
Cyber defence
Anomaly detection
Attack tools
Vulnerability
Simulation
Modelling
SCADA

ABSTRACT

SCADA systems monitor and control critical infrastructures of national importance such as power generation and distribution, water supply, transportation networks, and manufacturing facilities. The pervasiveness, miniaturisations and declining costs of Internet connectivity have transformed these systems from strictly isolated to highly interconnected networks. The connectivity provides immense benefits such as reliability, scalability and remote connectivity, but at the same time exposes an otherwise isolated and secure system, to global cyber security threats. This inevitable transformation to highly connected systems thus necessitates effective security safeguards to be in place as any compromise or downtime of SCADA systems can have severe economic, safety and security ramifications. One way to ensure vital asset protection is to adopt a viewpoint similar to an attacker to determine weaknesses and loopholes in defences. Such mind sets help to identify and fix potential breaches before their exploitation. This paper surveys tools and techniques to uncover SCADA system vulnerabilities. A comprehensive review of the selected approaches is provided along with their applicability.

1. Introduction

Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control critical national infrastructures such as smart grids, oil and gas, power generation and transmission, manufacturing, and transportation networks. They are also used to manage public utilities like buildings control, water, sewage, and traffic lights. The downtime or compromise of these systems can have disastrous consequences for the economy, public health and national security.

SCADA systems (Fig. 1) are cyber physical systems with communications networks (wired and wireless) interfacing the monitoring and control system with the hardware and providing a large attack surface (Dong et al., 2015). The architecture can be envisaged as four layers as shown in Fig. 1. At the lowest level, field or slave devices (sensors, pumps, motors) provide an interface for control and monitoring of the physical process. At the next higher level, Remote Terminal Unit (RTU) and Programmable Logic Controllers (PLC) aggregate control (acting as master) for many field devices by passing commands and responses through the communications network to the SCADA server. PLC is a computer system running Ladder Logic for decision making to control the field devices. The operator monitors the process state through Human-machine Interface (HMI) and controls the process by activating commands as required (Protecting Industrial Control Systems, 2011). A typical SCADA system could have multiple supervisory systems, PLCs, RTUs,

[*] Corresponding author.
E-mail address: sajid.nazir@firstco.uk.com (S. Nazir).

http://dx.doi.org/10.1016/j.cose.2017.06.010
0167-4048/© 2017 Published by Elsevier Ltd.

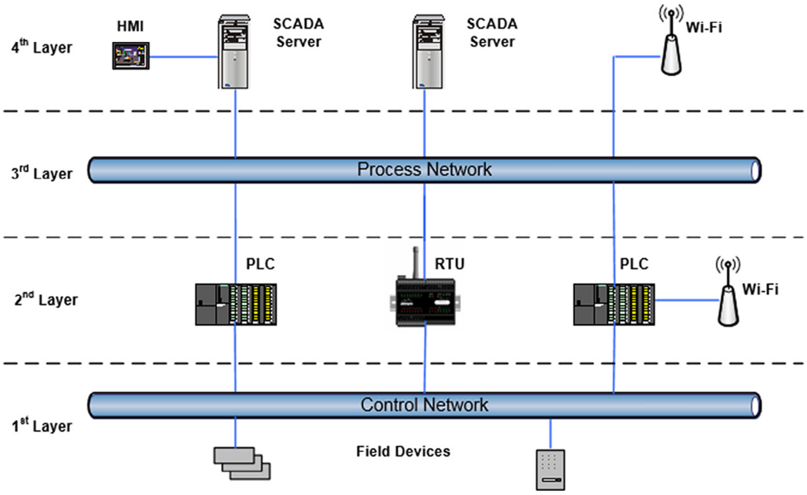

Fig. 1 – A simplified layered architecture for typical SCADA system.

HMIs, process and control instrumentation, sensors and actuator devices over a large geographical area, interconnected through a communications network.

The use and applications of SCADA systems has increased as a result of rising levels of industrial process automation, reduced cost of operation and growth in global economies. Growth is expected to increase in the use of SCADA systems and the investment is expected to reach up to $13.43 billion by 2022 (SCADA). With the proliferation of the Internet of Things (IoT), SCADA sensor and actuator devices which are Internet connected SCADA systems are being transformed from a traditional on-site, stand-alone system to an Internet-connected remotely accessible system. An overview of challenges and security requirements for IoT is provided in Li et al. (2016). A significant obstacle in IoT adoption is security aspect as it would be an attractive target for hackers (Li et al., 2016; Mallouhi et al., 2011).

There are many benefits of Internet access including scalability, better communications protocols, efficiency, cost effectiveness, interoperability between components (Genge et al., 2012) and remote access, but SCADA systems were never designed with network connectivity and security (Erol-Kantarci and Mouftah, 2013; Mallouhi et al., 2011) in mind. The focus had always been on reliability rather than security, and protection had been ensured through isolation and obscurity (Mahoney and Gandhi, 2011; Zhu et al., 2011) by using proprietary standards. Since the 1990s the control systems are being integrated with computer networks (Kesler, 2011) and also more and more Commercial-off-the-shelf (COTS) products are being used in SCADA systems (Almalawi et al., 2014). SCADA server and user interfaces are now accessible over the Internet and cellular networks, providing many entry points for an attacker (Backhaus et al.; Zhu et al., 2011). Most SCADA communications protocols are just plain-text (Pidikiti et al., 2013; Yang et al., 2013) with no message authentication (Jain and Tripathi, 2013) making it easier for a man-in-the-middle (MITM) attack. TCP/IP protocols have their own vulnerabilities that can be exploited (Mallouhi et al., 2011). PLCs would treat code as legitimate as long as it has the correct syntax (Langner, 2011). The threat landscape for SCADA systems has been broadened (Zhu et al., 2011) by Internet and cellular network connectivity, bringing along open standards such as web technologies, which have known security loopholes making it very easy for an attacker to gain an in-depth knowledge of SCADA networks (Igure et al., 2006; White paper). The modern SCADA communications use a variety of communication media, such as WiFi, cellular, and Bluetooth. Vulnerabilities in the communications protocols have been the main focus and target of cyber attacks. Failure to protect the SCADA infrastructure against the evolving threats of the changed connectivity landscape can have disastrous consequences. In the prevailing cyber security global environment, it is not a matter of if an attack of catastrophic proportion would happen, but rather when.

A Denial-of-Service (DoS) attack on a website can render a service unavailable, but similar attacks on SCADA systems can have potentially disastrous consequences (Disso et al., 2013) because of the fallout of the controlled process getting out of control. Stuxnet (Langner, 2011), June 2010, was the first malware designed to attack control systems and was the first attack of its kind that brought SCADA security vulnerabilities to prominence (Disso et al., 2013). Prior to that, although vulnerable, SCADA systems were not considered to be actively targeted. Malware, such as Flame (2012) that copied data, recorded Voice over Internet Protocol (VoIP) audio and intercepted network traffic (Disso et al., 2013). Stuxnet (2010) and Duqu (2011) used USB devices to spread and attacked the PLCs by changing the Ladder Logic code (Disso et al., 2013). Havex (2014) can reportedly infect the software downloads from the SCADA manufacturers' web sites (Constantin, 2014). An active group of attackers, Dragonfly (Symantec Security Response, 2014), mainly target energy sectors through malware tools and infect targeted organisations using spam emails. These malware attacks highlight security weaknesses in SCADA system design (Genge and Siaterlis, 2014). Other attacks like Slammer at Davis-Besse nuclear plant (Kesler, 2011) negate the illusion of security. The cyber attacks on SCADA systems have seen a 100% increase (Dell Security Annual Threat Report, 2016). General technology awareness, widespread availability of free

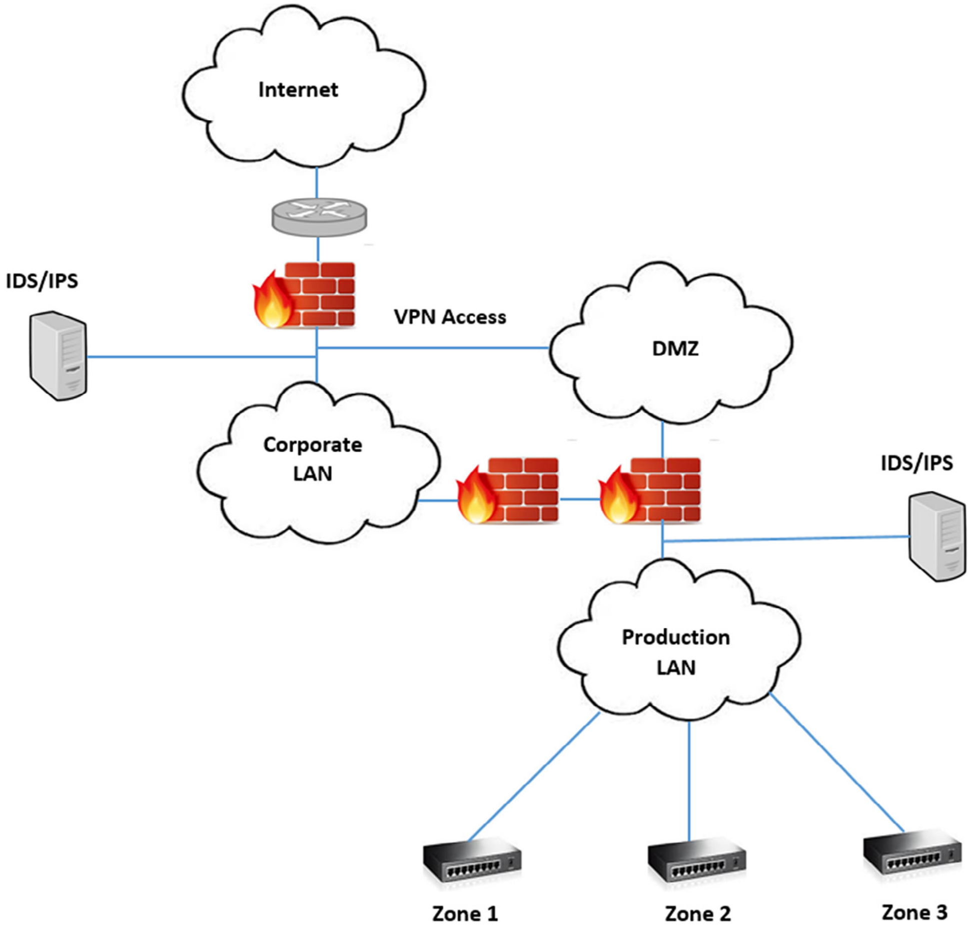

Fig. 2 – DMZ with separation of trust zones.

information, and the current global security situation of state and non-state elements with malicious intent, all combine to make launching such attacks easier and probable.

Countering the cyber attack is an emergent need to provide adequate safeguards against the cyber attacks by strengthening the defence. The general cyber security safeguards such as restricted physical access, cryptography, patch management, separation of corporate and production systems (through Demilitarized Zones (DMZ), Firewalls and Access Control Lists (ACLs)), and activity logging are all applicable (Fig. 2) but need to be viewed in conjunction with typical SCADA systems characteristics. Nonetheless these security measures are important as the corporate network could be the entry point for launching an attack on the SCADA network. Most of these security measures are not capable of defending SCADA systems from attacks against SCADA protocols (Fovino et al., 2009). For instance, SCADA characteristics make it difficult to apply existing cryptographic techniques due to limited computational capability, low data rate, and the need for real-time response (Igure et al., 2006). The confidentiality, integrity and availability (CIA) triad (Information Security Management (ISMS), 2013) applies to SCADA systems but with a changed order of priority as availability, integrity and confidentiality (AIC), with availability being the most important. Agencies such as the National Institute of Standards and Technology (NIST), USA, and European Network and Information Security Agency (ENISA) provide best practice documents for cyber security for SCADA systems in particular. Protection for telework devices is described in Scarfone and Souppaya (2007), and Cyber security of SCADA systems in Guide to industrial control systems (ICS, 2015). Guidelines for Patch management are provided in Pauna and Moulinos (2013). Protecting Industrial Control Systems (ICS) (Protecting Industrial Control Systems, 2011) has recommendations for Europe and member states, which identifies security challenges and recommends a common test bed for security testing. North American Electric Reliability Corporation (NERC) has released Critical Infrastructure Protection (CIP) documents. The industry regulations have started mandating the cyber security safeguards and this trend is likely to increase in the future.

Investigating the effect of an attack on an actual system is neither recommended due to the unintended consequences, nor feasible on a replicated system due to the cost and effort involved. Analysis methods and tools are very important to secure such systems (Urias et al., 2012). Therefore SCADA cyber security researchers mostly rely on developments of simulation software and hardware to model SCADA attacks to analyse the system security. SCADA system security can be assessed by using vulnerability analysis through actively attacking a system which not only uncovers the vulnerabilities but can also be used to determine the system failure response, which helps to understand the system and provide necessary safeguards by fixing the vulnerabilities. Techniques such as penetration testing and vulnerability analysis can be considered inclusive in vulnerability assessment (Ten et al., 2008).

Generic Simulators for SCADA systems are described in Mathioudakis et al. (2013) but the focus is not on cyber security. Smart Grid simulators (Mets et al., 2014) provide a useful reference for simulation tools but do not address SCADA or cyber security. Vulnerability assessment and analysis comprises a spectrum of techniques from the simplest ones doing port scanning to those involving exploitation of vulnerabilities, as in an actual attack (Guide to industrial control systems (ICS), 2015).

This paper provides a comprehensive survey of simulation, modelling and related techniques helpful for assessing the cyber-attack vulnerabilities of SCADA systems. In this paper we aim to cover the array of techniques for assessing SCADA vulnerabilities under simulation, modelling, tools and techniques as these are often employed by researchers for SCADA cyber security. This categorisation is purely with a view to better organise the research literature rather than a taxonomy. We also highlight recent technology innovations which can aid in minimising the effect of cyber security risks.

The rest of the paper is organised into the following sections. Section 2 provides SCADA systems' characteristics and vulnerabilities. Section 3 covers the simulation and modelling techniques for identifying security weaknesses. Section 4 describes other tools and techniques for evaluating defence. Section 5 provides conclusions, and Section 6 discusses future research directions.

2. SCADA system characteristics and vulnerabilities

SCADA system (Fig. 1) differs in characteristics from a conventional information technology (IT) system (Guide to industrial control systems (ICS), 2015; Zhu et al., 2011). SCADA systems have tighter constraints on reliability, latency and uptime that preclude some IT security measures (Jain and Tripathi, 2013). SCADA are cyber physical systems, that is, cyber system (control and communications) and physical system (sensors, actuators) comprising a system of systems that interact as a cohesive and unified whole. The software commands manifest actions to modify physical processes. It is important to consider these differences when devising the protection strategies.

2.1. *Generic OS*

SCADA systems run over conventional operating systems (OS), thus inheriting vulnerabilities which can compromise the SCADA system (Kesler, 2011). The vulnerabilities of the operating systems are periodically announced by the vendors (Microsoft Security Bulletins). The patches are normally issued after vulnerabilities are discovered, but there could be a substantial time lag to release patches or the patches may not be applied in time. The patch for the vulnerability exploited by Stuxnet in 2010 became available in 2012 (Pauna and Moulinos, 2013). There is generally a time lag for patch application, for instance, Slammer infections occurred six months after the patch to fix the vulnerability had been released (Kesler, 2011). Similarly lack of user incentives (August et al., 2014) to apply patching enabled Code Red, a malware to infect 360,000 servers, although a security patch had been released earlier. In some cases, an attack comes before vulnerability is discovered and is termed as a Zero day attack.

2.2. *Legacy systems with long operational life*

The installation of SCADA systems is costly and time-consuming and most systems remain in operation from eight to fifteen years (Kesler, 2011). A system may have devices from many different manufacturers using various standards or proprietary communications protocols (Oman and Phillips, 2008). This is sometimes well past the expected supported lifespan of the software and also hardware. Thus at times a system would comprise of legacy components and their associated vulnerabilities (Urias et al., 2012).

2.3. *Multiple points of entry and failure*

A SCADA system is geographically spread over a large area starting at the sensors, in the field, to the user and control interface. Although SCADA servers may themselves be well protected against cyber attacks, however, similar guarantees do not exist for field devices. The communications network, comprising of wireless Internet, cellular and Bluetooth, provides multiple remote entry points which can be exploited by attackers. Wireless networks are especially vulnerable using freely available tools like Aircrack-NG that can sniff, test and even decrypt packets (Aircrack-NG).

2.4. *Communications protocols*

The low-level networking protocols used for industrial systems use simple plain-text messages based on a master–slave communications model. These lack security and encryption, as these were designed for isolated systems (Pidikiti et al., 2013).

For example, Modbus protocol can be attacked as reported in Huitsing et al. (2008) and Zhu et al. (2011) with varying consequences (Huitsing et al., 2008). Other recent protocols, such as Distributed Network Protocol 3.0 (DNP3), also have their vulnerabilities (DNP-3 Protocol, 2005; Jin et al., 2011; Mallouhi et al., 2011) and packets can also be analysed (Aircrack-NG) through network sniffing tools to gain information and cause damage. Widely used protocols IEC 60870-5-101 and IEC 60870-5-104 lack application and data link layer security and have vulnerabilities that can be exploited (Pidikiti et al., 2013). With an understanding of the process and the protocol, an attacker can maliciously alter the process control by injecting valid control commands and responses with malicious intent (Genge and Siaterlis, 2014; Pidikiti et al., 2013). Attacks on protocol implementation (Huitsing et al., 2008) can cause failures resulting in possible exploits (Zhu et al., 2011).

2.5. *Real-time and complex interactions*

SCADA systems monitor real-world processes under very tight timing and operational constraints. Time is critical for decision making, affecting a control system and vital process deviations, which must be accurately reflected and effectively managed. The stringent operational constraints (such as timing) of a SCADA system mean that it is more prone to fail in response to small deviations caused by an attacker. "Aurora Generator Test" (Dong et al., 2015; Kesler, 2011) in March 2007 simulated a remote cyber-attack resulting in destruction of a $1 million dollar diesel-electric generator (Srivastava et al., 2013). A patch application (Information Security Management (ISMS), 2013) or loss of time synchronisation (Dong et al., 2015) may have unintended consequences detrimental to the prescribed operation. Application of a software update resulted in automatic shutdown of a nuclear plant (Kesler, 2011). Analysing and exploiting vulnerabilities may be complicated but unintelligent computer viruses and mere malfunctions in small devices can result in enormous unintended effects (Kesler, 2011).

2.6. *Conflicting priorities*

SCADA control and monitoring projects remain in continuous operation (Kirsch et al., 2014) for many decades after commissioning. This creates a dilemma for the administrators between ensuring adequate protection and sustained system operation. Application of software upgrades and patches may get postponed due to the desire to keep the system running without change to the execution environment (Pauna and Moulinos, 2013). Anti-virus and patches may result in undesirable consequences (Kesler, 2011) or may also tend to slow down the communication and may interfere with normal functioning of the system.

The operational nature of these systems precludes post commissioning cyber security testing due to associated risks of jeopardising the controlled system.

2.7. *Social engineering and insider attacks*

Social engineering attacks purporting to be from a known person or organisation can be used to infiltrate a system. Often the cyber security is focused on an outsider's attack, which makes sense, but equally probable and dangerous is an attack originating from within the trusted network, through a deliberate or unintentional omission, or sabotage.

The attack in 2000 on a sewage control system in Queensland, Australia (Kesler, 2011; Slay and Miller, 2008), causing flooding with a million litres of sewage, was an act of a disgruntled employee. Stuxnet infiltrated the network (Kesler, 2011; Langner, 2011) mainly through USB sticks.

2.8. *Backdoors*

The Stuxnet (Vijayan, 2010) worm exploited system vulnerabilities to attack a PLC in Iran's uranium enrichment programme in 2010. It exploited an administrative backdoor, which can be used to access a system remotely, and generally their availability on a system is known to system maker only. Such coded backdoor passwords which can be used to exploit a system remotely are not uncommon (Disso et al., 2013; Roberts, 2010). Such malpractice could also take place without the knowledge of a SCADA vendor, as increasingly the product is assembled from components manufactured from facilities across the globe (Disso et al., 2013).

2.9. *Integral protection*

With cyber security awareness coming into prominence, SCADA manufacturers also provide and emphasise security in products. These features provide encryption and security features such as Kerberos and multiplexing proxy. Activating these in a project can make an intruder's task difficult. SCADA systems also provide other built-in mechanisms such as User Groups, Historian, Encryption and Redundant Servers.

3. Simulation and modelling

SCADA systems are not only complex but have many system interdependencies which makes it difficult for them to be tested for cyber defence. The production systems are required to provide a continuous and reliable service, and depending on the monitored process, even small delays are intolerable. As such the systems cannot be taken out of service for vulnerability checks, and also these are very costly and hard to duplicate.

Simulation and modelling techniques are useful to model and test complex systems. Development of realistic models help to create scenarios that do not yet exist or would be very costly to build. A model also makes it easier to quickly change parameters to suit another scenario or configuration.

Simulation and modelling techniques are used advantageously to evaluate and probe the defence of SCADA systems. A summary is provided in Tables 1 and 2.

3.1. *Simulation frameworks*

Simulation frameworks are needed to model all aspects of the SCADA system using simulators and emulators. Generally a network simulator such as OMNeT++ is used for network modelling and Simulink/MATLAB is used to simulate the process control. A framework in general also provides the facility to integrate the various simulators to realistically represent the system as a whole.

3.1.1. *High level architecture (HLA)*

HLA is a simulation integration platform designed by the Department of Defence (DoD) (IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) Framework and Rules, 2010) that can be used to integrate simulators. This concept was chosen as no single simulation can meet all the requirements. An individual or a set of simulations can be applied across different uses, under the HLA federation concept. Federation means a set of interacting simulations, with each simulation termed as a federate. The federates must allow exchange of data through the Runtime Infrastructure (RTI).

HLA which is a co-simulation environment has been used by researchers to design simulations using OMNeT++ and MATLAB, for example.

Chabuksawar et al. (2010) used Command and Control (C2) WindTunnel as a simulation framework (based on HLA) (Hemingway et al., 2012) to simulate a plant, its controller and

Table 1 – Simulation frameworks, test beds, and risk assessment techniques with their focus of investigation, tools used, and application.

Category	Sub-category	Focus	Tools used	Application	Citations
Simulation framework	SCADASiM	Regulatory monitoring	ADACS	Water supply system	Mahoney and Gandhi (2011)
	SCADAsim	DDoS, spoofing attacks	OMNeT++	Smart meters, wind power plant	Queiroz et al. (2011)
	MAlsim	Malware simulation for security evaluation	MAlsim based on JADE	Power plant	Leszczyna et al. (2008)
	Co-simulation	Custom smart grid component analysis	CIM, GridLab-D, AKKA, EclipseSCADA	Power system	Bytschkow et al. (2015)
	Framework	Integration of simulations and SCADA	EngSB	Software prototype	Novak et al. (2014)
	Framework	Malware experimentation	MATLAB, Emulab	Stuxnet on a power plant, Tennessee-Eastman	Genge et al. (2012)
Test bed	Simulation	DoS	TrueTime (MATLAB/Simulink)	American Gas Association Report No. 12	Farooqui et al. (2014)
	Hybrid (simulation, emulation, hardware)	Anomaly based detection for HMI attack, DoS	OPNET, PowerWorld, ASPS	Biosphere 2 Power Grid at the University of Arizona	Mallouhi et al. (2011)
	Pedagogy	Modbus, HMI	Hardware, software, Snort	Various industrial applications	Morris et al. (2011)
	Intrusion and Defence	Communication protocols, networks	Software, hardware, anomaly detection	PowerCyber testbed	Hahn et al. (2010)
	Statistical data gathering	DoS, Data logging	Data statistics	Power Control Systems – Resilience Testing Laboratory of CESI-RICERCA	Dondossola et al. (2009)
	Attack	DoS, integrity, phishing	Simulation	Single simulation-based instantiation	Giani et al. (2008)
	Communications network	DDoS, Network	Simulink/Stateflow, HLA, NS2, OPNET, OMNeT++	Tennessee Eastman chemical process	Davies et al.
	Attack	DDoS	SCADA 2, Modbus simulator, GNS3	Generic implementation	Boldea (2011)
	Virtual machine	Modbus TCP/IP, DDoS, False data injection	Common Open Research Emulator, Python, Pymodbus, Ettercap	Water tank system	Tesfahun and Bhaskari (2016)
	Intrusion detection, event monitoring	RTUs	Snort, Perl, XML	Electric substation	Oman and Phillips (2008)
Risk assessment	Probabilistic	Risk estimation	HMM, IIM, RFRM	Generic system	Ralston et al. (2007)
	Modeling	Control systems	NSRM	Oil pipeline pump station	Henry and Haimes (2009)
	Network vulnerability	Graph	Attack graph	Simplified example	Phillips and Swiler (1998)
	Attack graphs	Bayesian network	MTTC, CVSS	IEEE RTS79	Zhang et al. (2015)
	Attack trees	Vulnerability assessment	Vulnerability index	Control centre	Ten et al. (2007)

the interconnecting network. The objective was to simulate network security attacks using this framework that requires domain-specific modelling language for defining integration models. The SCADA system was a simplified version of the Tennessee Eastman Control challenge problem (Downs and Vogel, 1993). DDoS attacks were simulated on the routers concluding a proof of concept implementation.

3.1.2. SCADASiM

An integrated framework for control system simulation, SCADASiM, is presented by Mahoney and Gandhi (2011). It can be modelled and simulated at different levels of abstractions commensurate with the problem at hand. The modelling notation is through Autonomous Component Architectures (ACA) that allows components to be modelled at simulation runtime. The authors proposed a new language Autonomous Component based policy Description Language for Anomaly monitoring in Control Systems) (ADACS) that was used for monitoring regulatory compliance.

3.1.3. SCADASim

Queiroz et al. (2011) present a framework for building SCADA system simulations. Additionally it can be used to create malicious attacks against SCADA systems. The framework can be extended by SCADASim users to add their own protocols; otherwise there are too many protocols. The framework is built on top of OMNeT++. Details of DoS and spoofing attack simulation are provided in the paper.

Table 2 – Simulation and modelling techniques with their main focus, tools used, and application.

Category	Sub-category	Focus	Tools used	Application	Citations
Simulation	Attack trees	Intrusion	Colored Petri Net	SCADA case study	Bouchti and Haqiq (2012)
	False sequential logic attack	Intrusion	MATLAB/Simulink	Three tank system	Li et al. (2016)
	Malware attacks	Modbus	MAlsim	Power plant testbed	Fovino et al. (2009)
	Test bed	Modbus TCP	OSSIM, Snort, Sebekd, OpenVAS	Simulated PLC	Mahboob and Zubairi (2013)
	MITM	IEC 60870-5-104	Snort, Qtester, Kali Linux, WinPP104	Software simulated laboratory, testbed	Maynard et al. (2014)
	Graph	Modbus	"C" Language	Tennessee Eastman chemical process	Genge and Siaterlis (2014)
	Monitoring	Malicious commands	Real-time and simulation monitor	Water treatment plant	Li et al. (2009)
	Attack	DDoS	OPNET	Hydropower	Markovic-Petrovic and Stojanovic (2013)
	Attack	Malware injection, DoS, MITM	Netlogo	Electrical grid connected to corporate network, NS2	Ciancamerla et al. (2013)
Modelling	Mathematical	DoS, deception attacks	Linear dynamical models	Water tank	Ćardenas et al. (2008)
	Mathematical	Model-driven testing	Modelica, Eclipse	Tank with valves and pumps	Süß et al. (2008)
	Game Theory	Interactions between cyber intruder and operator	Semi network-form game (SNFG)	Distribution feeder line	Backhaus et al.
	Bayesian Networks	System survivability	SCADASim	MITM	Queiroz et al. (2012)
	FNN	Defence	Factor neural network	Generic	Yang et al. (2012)
	Framework, attack trees	Modbus, DoS	RAIM	power system control network	Ten et al. (2010)
Attack	Attack trees	Modbus/tcp	Attack trees	Generic system	Byres et al. (2004)
	Replay attack	Sensors	Analytical, simulation	Tenessee Eastman problem	Mo et al. (2014)
	False data injection	AC state estimation	Analytics	IEEE 57 bus system	Hug and Giampapa (2012)

3.1.4. *Co-simulation framework*

A co-simulation framework is proposed by Bytschkow et al. (2015) using Common information model (CIM) as an intermediate model. It uses the approach of federation enabling both simulation and deriving possible impacts. The co-simulation framework is constructed using SCADA, CIM, GRIDLAB-D and AKKA.

3.1.5. *Emulation framework*

A framework for emulation based security analysis using Emulab and Simulink is proposed by Genge et al. (2012) that can be used to measure impact of attacks against both physical and cyber parts of systems. The authors' proposed framework extends Emulab to incorporate additional features required for cyber physical security analysis. The architecture comprises a cyber layer, physical layer, and a cyber physical link layer. The authors provide a feature based, cost based and an experimental scenario-based in comparison to other frameworks reported in the literature and contend their approach to be better. The authors provide two case studies from the electrical and chemical domains. The first studies the effect of Stuxnet on a Boiling Water power plant showing that the proposed framework can be used to recreate a scenario with complex malware. The second studies the effect of network parameters on a cyber attack targeting a chemical process, showing that in cyber attacks where the attacker communicates with PLCs, the communications delays and packet losses have little effect.

3.1.6. *Integration framework*

An integration framework has been proposed by Novak et al. (2014) that advocates semantic and technical integration of simulation models into SCADA systems. The authors contend that simulations cannot be developed without access to online and historical data and thus propose a platform for integration of simulations and SCADA. It reduces design-time errors (for simulation) and improves re-configurability and reuse. Two case studies are provided for design of simulation models for passive houses, and an application allowing the management and execution of simulations.

3.1.7. *Real-time monitoring, anomaly detection, impact analysis, and mitigation strategies (RAIM)*

The security SCADA framework proposed by Ten et al. (2010) comprises real-time monitoring, anomaly detection, impact analysis, and mitigation strategies (RAIM). Real-time monitoring can utilise the data for real-time control functions. Anomaly detection and impact analysis can be done through monitoring and correlating the system logs. The output is ranked as varying degrees of risks, based on which mitigation actions can be taken.

3.2. *Test beds*

Test bed is a platform used to test systems or technologies where the actual system cannot be endangered by testing, due to unintended consequences, for example, checking the effects of patch application and response to malware. A test bed must capture the essence of the system under test for it to be useful. The facility can also be shared to save cost or share knowledge. Test bed creation is also recommended in Protecting Industrial Control Systems (2011). Although some test beds have been developed by large organisations, generally the access is restricted to affiliated researchers only (Zhang et al., 2015). Unlike a simulation environment being fully contained in software, a test bed uses hardware, simulated and emulated devices. A survey of test beds in software and hardware is provided in Zhang et al. (2015).

Test beds could be realised (Giani et al., 2008) as simple simulation based (TrueTime), federated simulation (several dedicated simulation federates for plant, network etc. such as HLA) or emulation/implementation based (real hardware or emulator such as EmuLab).

3.2.1. *National SCADA test bed (NSTB)*

The Department of Energy, US, have established a National SCADA test bed (National SCADA Test Bed) that aims to provide testing, research and training facilities to help improve the security of control systems. However free access to academia and industry is not available. Thus, many researchers have developed test beds to investigate some element of security.

3.2.2. *TRUST*

An experimental simulation test bed TRUST-SCADA (Davies et al.) was aimed to assess and address vulnerabilities, and to provide an open-source design for a flexible test bed. DoD/HLA was chosen as the integration platform, for the plant model (Simulink/Stateflow), Network model using (OMNeT++, NS2, OPNET) and controller (Simulink/Stateflow).

Giani et al. (2008) have also proposed a test bed for SCADA vulnerabilities and validating security. The specific scenarios analysed were DoS attack on sensors, integrity attacks, and phishing attacks.

3.2.3. *Live virtual and constructive (LVC) test bed*

Urias et al. (2012) describe a hybrid test bed that can be used to perform cyber-physical security analysis. It was developed at Sandia National Laboratories to identify system level vulnerabilities, results of their exploitation, and approaches to eliminate it. Simulated network devices were represented using OPNET, enabling passing of simulated traffic to real devices. Virtual machines were used as hosts, servers and Cisco routers' emulation, and physical devices to which the simulated network traffic could be addressed. The experimental setup simulated the enterprise and control system network and provides analysis of cyber attacks against the business and control system network. The experiments investigated the effects of attacks on SCADA protocols (DNP and Modbus TCP) and how to mitigate such attacks using network security.

3.2.4. *TrueTime*

A simple test bed (Farooqui et al., 2014) has been proposed by Farooqui et al. using TrueTime (MATLAB/Simulink based simulator developed by Lund University) to simulate DoS attacks and its effects. The SCADA network is designed to control four different DC servo motors through a reference signal. The DoS attack scenarios covered attack on a PID controller and a specified actuator.

3.2.5. *Research and pedagogy*

A test bed for SCADA cyber security research and pedagogy has been developed by Morris et al. (2011). It provides the facility to discover vulnerabilities, implications and classification of vulnerabilities by type, mitigations and validations. Developed at Mississippi State University, it models various industrial applications such as smart grid and gas pipeline, through hardware and software.

3.2.6. *TASSCS*

The OPNET test bed by Mallouhi et al. (2011) is used to simulate networks, PowerWorld simulation system to simulate the functioning of power grid, and Autonomic Software Protection System (ASPS) for detection and protection against SCADA cyber security attacks. The attack detection is based on an anomaly based approach. It provides details of DNP, Modbus, and TCP/IP attacks through a training and detection phase.

3.2.7. *Power station simulation*

The test bed proposed by Hahn et al. (2010) consists of power station simulation, substation automation and SCADA system, and uses scenarios based on anomaly detection. It is based on real-time monitoring, anomaly detection, impact analysis, and mitigation strategies (RAIM). The test bed uses ICCP, DNP 3.0 over TCP/IP, and OPC communications protocols.

3.2.8. *Power control system*

A test bed for a simulated power control systems is reported by Dondossola et al. (2009) for collection of data through controlled experiments on a power system test bed, and activities for using the collected data for analysis and risk assessment frameworks. Cyber threats such as DoS and false injection attacks were investigated. The authors also gathered statistics based on message delays, number of lost messages, and time to failure to UDP flooding attacks.

3.2.9. *Common open research emulator (CORE)*

Tesfahun and Bhaskari (2016) propose a scalable and reconfigurable virtual SCADA security test bed for developing and evaluating security solutions. The authors provide a labelled dataset for other researchers. It is based on Common Open Research Emulator (CORE) for simulating SCADA networks. It is possible to launch multiple attacks simultaneously and benchmark datasets can also be generated. CORE can be connected to real world networks, with the Python module to customise network emulation. The researchers represented SCADA devices by a virtual node in CORE. DDoS and False Data Injection attack were simulated.

3.2.10. *Software defined networking (SDN)*

SDN makes it possible to dynamically reconfigure an IP network. Dong et al. (2015) explore the use of SDN techniques for enhancing the protection against cyber attacks. The authors propose a co-simulation test bed comprising Mininet (to emulate smart grid communications) and PowerWorld (to simulate physical aspects of power systems). The test bed has Bro-based IDS to analyse the DNP3 traces and provide results for SDN countermeasures. Three use cases were considered to demonstrate the SDN potential for strengthening the resilience.

3.2.11. SCADA virtual test environment

A test environment is proposed by Boldea (2011) to assess the security of SCADA systems, and the use of virtual systems to emulate the real systems, and used GNS3 for network components and Virtual Box for software virtualisation. The SCADA test bed used the free SCADA 2 software with a Designer and Runtime tool to simulate DDoS attacks.

3.3. Simulating SCADA attacks

Simulating SCADA attacks makes it possible to explore the cyber defence of the system under investigation. The results can then be used to strengthen the defence.

3.3.1. Malware attacks

Malware or malicious software poses a serious threat to SCADA systems. The vulnerabilities present in the IT and communications systems can be exploited by viruses and malware, hence making SCADA systems vulnerable to such attacks as reported by Fovino et al. (2009).

A malware attack simulator for testing SCADA system under controlled environments, Mobile Agent Malware Simulator MAlSim has been proposed by Leszczyna et al. (2008). The toolkit provides the facility to implement various types of malware. The aim was to provide security assessment based on simulated attacks. It can be used to simulate well-known malware such as Code Red, SQL Slammer. A malware template is comprised of a MAlsim agent with its behavioural and migration patterns.

MAlsim was used by Fovino et al. (2009) to investigate malware attacks on a SCADA system on a power plant test bed comprising of a process network, field network, intranet, data exchange network, external network and observer network. The code for Code Red, Nimda, Slammer and Scalper was obtained and injected into the process network to activate these malwares. The malwares infected the machines but did not lead to system failures. The authors also provide results for a Modbus DoS and network attack.

Ciancamerla et al. (2013) provide results for a malware injection on an electric grid.

3.3.2. Network attacks

Chabuksawar et al. (2010) used a simulator that uses C2WindTunnel. The paper emphasises co-simulation of controller and plant dynamics in Simulink/MATLAB and network architecture and behaviour in a network simulator like OMNeT++ (Fovino et al., 2009).

NETA is a framework for the simulation of communications network attacks. Network Attacks (NETA) (NETA) is based on OMNeT++ and provides a framework for simulating attacks in heterogeneous networks.

3.3.3. Communication protocol attacks

There are hundreds of communications protocols in use for SCADA communications. Jin et al. (2011) provide modelling of buffer flooding attack on DNP3 protocol. A simple flooding attack fills the event buffer in the data aggregator so that the critical alerts from legitimate devices cannot be buffered which impacts the control station's situational awareness. The behaviour is analysed through a simulation model (Jin et al., 2011). Moya et al. (2009) describe a Grey Hole attack against a SCADA substation using DNP3.0.

Fovino et al. (2012) provided a filtering system based on state analysis for securing SCADA protocols, Modbus and DNP3. The aim of the study was to detect attacks where a set of licit commands on execution can disrupt a SCADA system while in particular states. A firewall does not guarantee complete protection to SCADA systems, as it operates on a signature-based approach. Thus a firewall needs the system state and the set of unwanted states. In order to check whether the system is proceeding to a critical state from which the distance from critical states can be calculated. The proposed method was validated on a prototype system.

A "C" language graph based implementation by Genge and Siaterlis (2014) for network segmentation separates control hardware regulating input flows from output flows of the industrial process for SCADA resilience. The human expert is needed to construct a directed graph where vertices are process units and edges are product flows, the segmentation is performed through a heuristic algorithm. The methodology was applied on the Tennessee-Eastman chemical process using two attack scenarios on PLCs using Modbus protocol and the results show that it can be used for defence against Stuxnet like attacks.

A graph theory analysis for IEEE 118 bus system is presented by Srivastava et al. (2013).

3.3.4. Denial-of-service/MITM

This has been the most well studied type of attack as it is easy to implement and launch. A malicious agent can flood a specific device through protocol exploitation, resulting in bandwidth saturation that renders the service unavailable as described by Ciancamerla et al. (2013). SCADA system vulnerability analysis through DDoS attack is presented by Markovic-Petrovic and Stojanovic (2013). The simulation considers a corporate and SCADA network. A DoS attack on an actual SCADA system of a medium voltage electrical grid is provided in Ciancamerla et al. (2013). Malware attack results for DoS for Modbus protocol are provided in Fovino et al. (2009).

The wireless packets are easy to exploit because the intruder does not have to be physically connected to the network (as in wired) to access the network traffic. Xie et al. (2014) have proposed a simulation platform based on radio modem for analysing radio modem security. Radio modems are typically used for long range communications to connect PLC, RTU etc. but often the data are sent in plain text that can be exploited. The paper explored four types of attacks, that is, communication jam, data eavesdropping data tamper and eavesdropping, and DoS attack.

MITM attacks on IEC 60870-5-104 SCADA networks are described by Maynard et al. (2014). Details of the protocol packet payload are provided. MITM attacks will follow the stages of detection (to identify targets), capture (data collection), and finally attack. The experiments cover relay and MITM attacks and, attackers with varying degrees of experience can compromise the system by hiding fault condition from a SCADA server.

3.3.5. *False data injection (FDI)*

In false data injection attack the stored or transmitted data from RTUs, control centre or communications infrastructure is modified with a malicious intent (Hug and Giampapa, 2012).

Hug and Giampapa (2012) considered the FDI attack on a SCADA system for a power grid for ac state estimation. Through simulation using IEEE 57 bus system, details are provided for a number of measurements that the attacker needs to alter, to stay hidden. If the attacker has knowledge of the system data then the attack will not be noticed through the ac state estimation. FDI were also investigated in Dondossola et al. (2009).

3.3.6. *False sequential logic attacks*

Li et al. (2016) proposed a false sequential logic attack on a SCADA system. An informed attacker can alter the sequential logic of control to disrupt the physical process before the intrusion is detected. The sequential logic of the physical process is modelled as finite state machine (FSM). Traditional IDS will not be able to detect an intrusion as it is based on licit commands, demonstrated for a three tank system. To detect the proposed attack there is a need for sequential logic feature-based IDS to continuously monitor the control sequence.

3.3.7. *Integrity attacks*

An attacker can gain access to the sensors and/or actuators and modify the software to launch a coordinated attack as reported by Mo et al. (2014). Data integrity attacks wherein the sensor or control signals are manipulated can have severe consequences as the operator could be misled into taking wrong actions. These attacks are more difficult to overcome as their onset is not as obvious as DoS attacks. In Mo et al. (2014) the authors focused on techniques for integrity attack detection and describe an analytic approach verified through simulation for detecting replay attacks on sensors. It assumes that the attacker has capability to read sensor inputs and capability to inject input.

Such an attack however would require knowledge of the system as described by Sridhar and Manimaran (2010). In Sridhar and Manimaran (2010) an integrity attack is simulated on an Automatic Gain Control (AGC) loop that keeps both tie-line flow and frequency deviation values correct. Simulation is performed on a two-area system, and verifies that the system can be led to an unhealthy state by an attacker manipulating values intelligently.

Unsupervised anomaly detection for integrity attacks on SCADA systems is described in Almalawi et al. (2014).

3.3.8. *Real-time and simulation monitor*

A methodology to ensure SCADA availability through a real-time monitor and a simulation monitor is proposed by Li et al. (2009). The real-time monitor monitors states and events and, based on that, estimates if there are faults or risks. The simulation monitor simulates control commands, monitors and predicts the results of those commands and estimates whether the commands are dangerous or not. The methodology is then tested on a simulated water treatment system.

3.4. *Mathematical modelling*

Modelling techniques provide a reliable and formal mechanism for validating a system under attack. Linear dynamical models (Ten et al., 2008) are used to model the behaviour of control systems. A model for a web robot network (botnet) is proposed by Brand et al. (2011), which can be used to attack the system in different ways. Botnets can bring down a server through a DDoS attack from many compromised machines as investigated by Baecher et al. (2006).

Backhaus et al. describe a game theory model to outline a scenario where the attacker, after gaining access to the system will interact through its control system with the system operator, and the outcome of these machine–machine interactions will be governed by the design of the physical and control systems. Considering a simple model, the interactions of the attacker and defender are explored and the outcome is estimated. Extensions to real world complex problems would increase the computational requirements exponentially.

Yang et al. (2012) proposed Factor Neural Network (FNN) to study the security problem in SCADA through developing a FNN-based security defence architecture model. The attack and defence of SCADA is taken as online digital intelligent antagonising process and all reasoning, judgement and thinking is abstracted into corresponding network attacks and defence knowledge system. The proposed model needs further research into SCADA network attack simulation.

Ćardenas et al. (2008) use a mathematical formulation to detect and survive attacks in specific research problems. The physical system is modelled as a linear dynamical system.

Testing complex SCADA systems is challenging; Süß et al. (2008) propose the use of Modelica and Eclipse Modeling framework. Modelica is a mathematical modelling language for complex physical systems and offers Ecore, the meta-language of the Eclipse framework. The focus is on an integrated unified model driven development environment.

3.5. *Probabilistic modelling*

Queiroz et al. (2012) propose a survivability model based on Bayesian networks, taking into account the type of protocol communication. The focus is on system survivability despite attacks. The simulated system consisted of fibre networks modelled using SCADASim (Boldea, 2011) to simulate and test the model. Such techniques are very useful as the complex interaction between system components can be easily validated. A Bayesian attack graph model is proposed by Zhang et al. (2015).

3.6. *Risk modelling and assessment*

A review of risk assessment techniques is provided by Cherdantseva et al. (2016). Risk management reduces the likelihood of cyber attacks disrupting SCADA and in the event of a successful attack reducing the severity of the consequences as described by Henry and Haimes (2009).

An integrated methodology for managing the risk of cyber attacks is reported in Henry (2007). Minimax envelopes are developed for dynamic multi objective models to address scenario uncertainty due to different attacker motives and points of access.

A Network Security Risk Model (NSRM) for cyber risk analysis of the control system is proposed in Henry and Haimes (2009). The model is applied on an example system of a simplified crude oil pipeline pump station. NSRM is an attack model with a directed graph, where nodes represent process components and edges are the linkages from one process component to another. The model defines the state space where transitions take place with transition probabilities in response to attacker's actions.

A survey of available tools for SCADA risk assessment is provided by Ralston et al. (2007). It mainly covers probabilistic risk assessment to estimate the risk from SCADA systems.

A network vulnerability analysis using attack graphs is provided by Phillips and Swiler (1998). The attack paths and their probabilities could be identified and vulnerable system components can also be identified. In attack graphs, each node represents a possible attack state and each edge represents a success probability. The inputs to the system are configuration files, attacker profiles, and attack templates. An example is provided for generation and analysis of graph.

Attack-Trees were first described by Schneier (1999) and are a widely used technology for risk assessment of safety-critical systems. The attack goal is modelled as the root of the tree and various possible ways of accomplishing the goal are the leaves. These make it easier to identify the more probable causes and make predictions. Attack trees visually describe the possible attack paths and can be used for risk assessment as described by Bouchti and Haqiq (2012).

Moore et al. (2001) provide guidance on documenting security attacks in a reusable form through an example. The practicality of an attack tree for a real-world system is governed by re-using an attack pattern. Through the chosen example of an enterprise, the authors describe the documentation of security attacks in a reusable form. Thus it provides a means to organise historical attack data for later analysis.

The attack tree methodology was used by Byres et al. (2004) to model cyber attacks on SCADA systems. The authors provide some examples of risk analysis for attackers' goals of gaining access to the SCADA system, identifying Modbus device and compromising the master, and highlight the security issues. The authors describe their methodology through identifying eleven attackers' goals which were elaborated for their technical difficulty, probability of detection, and underlying critical vulnerabilities. They conclude that all the attack avenues depend on an attacker getting network access. The authors point to more rigorous work that is required for the techniques to be usefully employed.

Ten et al. (2007) used attack trees for vulnerability assessment of SCADA systems. The paper considers an analytical model to measure vulnerabilities of a control centre. The methodology used vulnerability index as likelihood that an attack tree or leaf will be compromised.

Bouchti and Haqiq (2012) extended the attack trees with new modelling constructs and analysis approaches to propose Colored Petri Net (CoPNet) to model intrusion. Petri Net is a mathematical modelling language that can be used as a visual communication tool. Based on the mapping rules, a CoPNet model can be built from Attack trees. CoPNet can model both defences and attacks, unlike an attack tree that can only model attacks. The proposed method is applied to a 3bus power grid and its SCADA network. The model provides better modelling compared to attack trees but has a more complicated form.

Attack trees have been used by Ten et al. (2010) for intrusion modelling. The study is focused on the ports and passwords on control network computers. The vulnerabilities were depicted as a risk table. The hardening through administrative passwords was also tested.

Bayesian attack graph models are applied by Zhang et al. (2015) for power system attack scenarios of breaker trips through IEDs. A mean time-to-compromise (MTTC) model is used to estimate time for successful intrusion of cyber components. Bayesian networks model attack graphs using probabilities. Two attack graph models are considered; first is the attack graph of vulnerabilities, and the second estimates successful intrusion on communications links. The reliability analysis is provided for the attacks considered.

4. Tools and techniques

In this section, we describe the tools that can be used either for gathering more information about an intended target system or those which can actively attack a system with or without such analysis. A summary is provided in Table 3.

4.1. *Scanning tools*

Any information about network addresses or open ports of a potential target can help the attacker to develop an attack methodology. By knowing which ports are open and listening, it is easy to infer about the running programs and then devising an exploit or attack methodology. If the attacker has access to the network, then through freely available tools it is possible to gather information about a system or to actively target it. In general the more information that gets collected the higher will be the damage caused (Pidikiti et al., 2013). Using similar tools as available to a hacker can help to determine the weaknesses of the system and to provide a timely fix.

Nmap (nmap) is a freely downloadable scanning tool that can be used to gather information about a single machine or the whole network. It can provide information about the open ports, services being run and the operating system, and even the firewalls in use, as well as other characteristics. All of this provides valuable information to an attacker to plan the attack. Port scanning is often done before the penetration testing. Traffic to an open port would legitimately pass through a firewall and may be used to determine the Trojan or other malicious code running on a machine. However, Nmap can be run from one of the machines in the network which may be difficult for an intruder.

In contrast to a wired network, packets on a wireless network are easy to intercept because the intruder could intercept packets just by being in the range. There are tools such as Aircrack-NG that let packets to be captured.

Table 3 – Tools and techniques with their main focus, tools used and application.

Category	Subcat	Focus	Tools used	Application	Citations
Machine Learning	Anomaly based	Integrity attacks, MITM, Modbus/TCP	WEKA, EPANET, VMs, k-means	Simulated and real datasets, Water distribution system	Almalawi et al. (2014)
	Anomaly detection	Telecommunications networks	SVM	Datasets	Jiang and Yasakethu (2013)
	Feature filtering	Malware detection	SVM, N-gram analysis	Generic	O'Kane et al. (2013)
	One class classification	Malware intrusions	SVDD, kernel PCA	Real data from gas pipeline testbed and water treatment plant	Nader et al. (2014)
	Reputation system, distributed agents	Sensors	Unsupervised learning, SOM	Sensor networks	Moya et al. (2009)
	Communication protocols	DNP3, gray hole attack	SVM	Trace based simulation	Torrisi et al. (2014)
	Analytics	Cloud based data analytics	OpenPlanet, Hadoop, regression tree, Floe, MapReduce, WEKA, VM	Los Angeles Smart Grid Project	Simmhan et al. (2013)
Intrusion Detection System	Rule based	IEC 60870-5-104	Deep packet inspection, ITACA	Protocol traffic case study	Yang et al. (2013)
	Filtering system	Modbus and DNP311	Firewall	Industrial Network Security Laboratory	Fovino et al. (2012)
	Intrusion tolerance, state machine approach	SCADA master	Hardware, Prime replication	Simple SCADA master, and RDU for electricity transmission and distribution	Kirsch et al. (2014)
	Critical state based	Modbus on PLC	ISML	Joint Research Centre testbed,	Carcano et al. (2011)
Honey Pots	Botnets	Detect new botnets	honeyd	Data traces	Pham and Dacier (2011)
	Analysis	Protection to SCADA, anti-honeypot techniques	Honeywell CDROM	Anti-honeypot techniques	Disso et al. (2013)
	Using proxy	Techniques for low cost honey pots	Honeyd+, Raspberry Pi	Study Slammer, Code Red, Blaster	Winn et al. (2015)
	Malware	Large scale malware collection	nepenthes	nepenthes	Baecher et al. (2006)
	Virus	Virus discovery and fast antivirus dissemination	Dynamic distributed immunisation strategy	Email network	Goldenberg et al. (2005)
Post attack	Forensics	Smart grids	Traces, Leurré.com system	Attack attribution	Erol-Kantarci and Mouftah (2013); Pham and Dacier (2011)

4.2. *Penetration testing*

Tools such as metasploit (Metasploit) can be use for penetration testing. Sploitware (Sploitware) which is a framework designed specifically for penetration testing of SCADA systems can be used to check for SCADA vulnerabilities.

4.3. *Machine learning*

Machine learning techniques are mostly based on statistics and can analyse the process data to isolate anomalous data that signal malicious behaviour. Thus making automated machine learning techniques more appropriate and efficient compared to human analysts (Jiang and Yasakethu, 2013).

Almalawi et al. (2014) proposed an unsupervised anomaly based detection scheme for a water distribution system to detect inconsistent states using k-nearest neighbours (KNN) and clustering using k-means. The inconsistencies could be either inconsistent network traffic pattern or SCADA data (Almalawi et al., 2014). Simulated and real datasets are used to simulate MITM attacks on Modbus/TCP. The authors show their scheme to perform better than supervised and semi-supervised schemes.

Machine learning techniques have been applied to telecommunications; Jiang and Yasakethu (2013) proposed one class SVM for automated anomaly detection from SCADA telecommunications data.

Torrisi et al. (2014) propose SVM based traffic analysis using message direction and timing information to protect against Grey Hole attacks. Unlike other work that is focused on identifying the different protocols in an encrypted tunnel, the authors consider an attack classifying messages that belong to the same application layer protocol, DNP3, and investigate the ability to cause interference in SCADA monitoring. In a grey hole attack, as the solicited responses from the master are let through and the unsolicited messages are dropped, the master would still not be aware of the message drop and thus the attacker can remain undetected. The message drop would result in the operator observation to be off by about

10–20%. Such attacks could be mitigated through use of TCP as the sequence numbering works in both directions and loss would be detected or by modifying the DNP3.0 protocol to use related sequence numbers for both unsolicited and solicited messages.

SVM techniques were used in O'Kane et al. (2013) to identify malware and demonstrate use of an "eigenvector" prefilter to remove irrelevant features from the dataset.

Nader et al. (2014) propose to detect malicious intrusions through machine learning after they have bypassed IDS. The paper investigates l_p-norms in Radial Basis Function (RBF) kernels for intrusion detection using one class classification techniques of support vector data description (SVDD) and the Kernel Principal Component Analysis (KPCA). The selected algorithms are applied on the gas pipeline test bed and compared to other selected methods, was faster, had higher error detection rates, and lowest false alarm rates. Application on a water treatment dataset gave better results for KPCA compared to SVDD.

A cloud based data analysis system for Los Angeles Smart Grid Project is described by Simmhan et al. (2013). It was based on Floe data flow framework which is hosted elastically on VMs and is supported by major cloud providers. The work demonstrates value of cloud computing and data analytics for smart grids but provides insights for mining similar data for just SCADA systems. Some principles for smart grid analysis are provided in Ten Leading Practices for Smart Grid Analytics by Accenture.

4.4. *Network intrusion detection systems (IDS)*

IDS work by inspecting the network traffic and mainly comprise of two approaches: signature based and anomaly based. The signature detection matches traffic to a known misuse pattern, while the anomaly detection works on the normalities in the observed data and can detect unknown attacks (Jain and Tripathi, 2013; Yang et al., 2013).

A review of IDS schemes and a decentralised multi agent scheme is proposed by MacDermott et al. (2012). Digital Bond Quickdraw project (Quickdraw SCADA IDS, online) releases IDS signatures for DNP3, EtherNet/IP and Modbus/TCP that can be used to identify possible attacks (Yang et al., 2013).

A rule-based IDS is proposed by Yang et al. (2013) for IEC 60870-5-104 protocol which is used for basic telecontrol tasks but the messages are in plain text and it also has inherent TCP/IP issues. The authors use Internet Traffic and Content Analysis (ITACA) tool for traffic sniffing. The proposed signature and model based approaches were validated by capturing normal traffic followed by abnormal packets, and effectively identified all abnormal data for the given rules and dataset.

This work has been extended by Yang et al. (2013) for IEC/60870-5-104 protocols by deriving stateful protocol analysis approach (Yang et al., 2014). Stateful analysis compares predetermined acceptable protocol behaviours against observed activities to detect deviations or intrusions. A detection state machine is proposed and applied for stateful IDS for SACDA systems.

Similar to attack tools, there are freely available tools that make it possible to detect and prevent an intrusion. A guide (Scarfone and Mell, 2007) to intrusion detection and protection is available by NIST.

Malicious users understand signature-based technologies and can craft malware that can elude such systems and remain undetected, as described by Winn et al. (2015).

Some work has been reported based on machine learning techniques. The communications datasets from SCADA are analysed by Jiang and Yasakethu (2013) with one class SVM to cluster the anomalies and generate an alarm based on perceived severity.

Oman and Phillips (2008) described an implementation of a customised IDS and event monitoring system. The system can assist operators to identify erroneous or malicious settings and activities in the system.

The inadequacy of rule based approaches with reference to firewalls is elaborated in Fovino et al. (2012) by stating that for control systems, even a sequence of licit commands can lead the system to an unsafe state.

IDS based on critical state analysis in a power plant are proposed by Carcano et al. (2011). The authors contend that the system critical states, as a result of cyber attacks or system faults, can be segregated based on IDS that is aware of such critical system states, from known or unknown attacks. The authors develop a new Industrial State Modelling Language (ISML) and use it to define states. By monitoring the system states a critical state can be detected before it occurs by monitoring the distance from a critical state. The proposed scheme can also detect zero day attacks as it is based on system states from known to critical.

Kirsch et al. (2014) describe what they term as a first survivable SCADA system using replication of SCADA master that continues with minimal degradation during cyber attacks. The system runs several copies of SCADA master; thus, the application acts as its own firewall and does not require prior knowledge of attack signatures. The replication protocol assumes that some of the replicas are compromised. The authors propose a state machine approach where all replicas start in the same initial state and cooperate to execute an event that ensures all replicas proceed through the same state sequence. Prime client library is used to link RTUs and HMI to SCADA master. A polling and scalability scenario was used to validate the proposed system.

Snort (Snort) is a free tool for intrusion detection that can analyse traffic, packet logging, and protocol analysis. OSSEC (OSSEC) is another open source tool for intrusion detection. An early detection of an intrusion can help to contain its effect and potential damage (Jiang and Yasakethu, 2013), thus making such techniques extremely useful.

4.5. *Intrusion prevention systems (IPS)*

An IPS performs the intrusion detection and additionally also attempts to prevent/stop certain incidents (MacDermott et al., 2012). An IPS monitors the network for any malicious activity and also attempts at stopping the intrusion and raises an alert. Snort (Snort) can also perform intrusion prevention.

There is little research reported on IPS unlike IDS which is comparatively heavily researched.

4.6. *Honey pots (also conpot)*

Honey pots are computer systems deployed as decoys to attract hackers to attack them and thus record the attackers' actions. Thus sources and intentions of the attackers are obtained without exposing an actual system to exploitation risk. They provide knowledge about the tactics and techniques employed by the malicious users (Winn et al., 2015) and also about the origin of such attack.

The implementation could be a low-interaction honeypot (LIH) that offers limited services or high-interaction honeypot (HIH) that implements a complete system (Baecher et al., 2006; Disso et al., 2013). Honeyd and GenIII honeynet are examples of a LIH and HIH respectively (Baecher et al., 2006). For details of different honeypot based tools and their relative merits, see Baecher et al. (2006).

Honeypot should mimic a device (such as PLC) as part of a larger system to be of interest to the attackers as described by Winn et al. (2015). Honeyd is a cost effective solution to deploy a realistic honeypot. During pilot studies it was used to advertise 75 PLC in Winn et al. (2015). Disso et al. (2013) used honeynet Honeywall CDROM in a virtual machine as a honey pot. A PLC (low interaction) was emulated using HoneyD, and another PLC as high interaction.

Although mimicking an industrial system is complex, the open source honeyd (Honeyd) makes it easier. The attack traces can be stored and analysed to determine the sources of attacks. The information about the potential people interested in acquiring information, hacking, and frequent visits can help to bolster up the defence. On identifying a honey pot, the hackers may employ anti-honeypoting techniques (Winn et al., 2015).

A study to identify and group the traces left on honeypots to the botnets' originating machines is described by Pham and Dacier (2011) that enables identifying new botnets. The traces are represented as time series that could be arranged based on the country of origin of a source. The time series can then be correlated to detect attack events. The attack events then help to identify attacks from the same botnet or a group of botnets.

A large scale collection of malware (Baecher et al., 2006) can help design counter-strategies such as network and host IDS. Baecher et al. introduce Nepenthes as a platform to deploy honeypots as vulnerability modules. It is a scalable solution to emulate different operating systems and authors report experiments by emulating more than 16,000 different IP addresses on a single physical machine. Nepenthes is effective at detecting zero day attacks but is capable of collecting malware that is autonomously spreading. Their system collected 15,500 unique binaries over a four month period, and analysing them with different anti-virus systems detected 80–90% as malicious, that is different anti-virus engines are missing a significant percentage of malware.

Brand et al. (2011) describe a malware rebirthing botnet that can be used to collect malware and rebirth it with new signatures to launch an orchestrated attack and avoid detection by AV software.

Viruses can be countered by propagating the immunisation agent as an epidemic as proposed by Goldenberg et al. (2005). The authors propose using the honey pot architecture for early virus discovery and fast antivirus dissemination. They provide a concrete example of an email network.

4.7. *Security information and event management (SIEM)*

SIEM works by aggregating the information from the selected tools to a central repository for real-time trend analysis. An open-source product is OSSIM (Mahboob and Zubairi, 2013; OSSIM). Mahboob and Zubairi (2013) proposed OSSIM (by AlienVault as above) that is an open source Linux based Security information and event management (SIEM) system for SCADA security by configuring OSSIM. OSSIM can bring together several security tools such as Open source security (OSSEC) and a GUI. OSSIM can correlate events from different sources such as firewalls, anomaly detectors, IDS/IPS, and network switches and combine these with known vulnerabilities. The authors used a PLC (as VM), Honeynet and Honeywall VM for GUI. Snort is used for IDS and OpenVAS for vulnerability scanning. Based on the results mitigation actions (patches) can be taken and the scanning can be performed again. OSSIM assigns a risk value to each event and has many other correlation features not fully explored by the authors.

4.8. *Ethical or white-hat hacking*

The term white-hat hacking means to perform the same actions as that of a real or black-hat hacker to determine the security weaknesses in a system with the intention to fix them before exploitation. Encouragement through recognition and rewards for finding and reporting vulnerabilities will bring such skills to prominence and help protect systems from malicious black-hat hackers. At a more formal level (ENISA, 2014) describes the certification of the cyber security skills.

4.9. *Forensic science*

It may be useful to do post attack analysis for protecting the systems as investigated by Erol-Kantarci and Mouftah (2013) against similar future attacks. It is a new research area for SCADA with similarities to digital forensic in other areas. Valuable information can be gleaned from events preceding an attack. However as pointed by the authors there are some challenges such as live analysis and issues like privacy of data etc. that need to be overcome.

Forensics (Pham and Dacier, 2011) has also been applied to honey pot traces to identify new botnets originating from the same source machines or countries.

5. Conclusion

SCADA systems have gained prominence and widespread use beyond the traditional applications for highly critical systems such as power generation and transportation systems. Internet connectivity has changed the threat landscape and the recent interest and ability to monitor and control processes over the mobile network means even more diverse entry points. Thus effective strategies are required that can provide adequate protection against cyber-security threats and attacks. Perhaps the most important transformation needed is a different threat perception for SCADA systems.

Current strategies such as simulation, modelling and other approaches reported in the research literature for determining the efficacy of a system against a cyber-attack have been reviewed in this paper. These techniques can be used to uncover the system vulnerabilities by determining the degree of protection against a possible attack. This helps the system developers and providers to assess their systems before commissioning, and system users/clients to be aware of security provisions and compliance to regulatory requirements.

In view of the fast changing cyber threat landscape, adoption of security techniques will be offset by corresponding new threats being evolved. Hence there would always be a need for continuous evaluation and evolution of cyber defence practices to match the corresponding threats. The guidelines provided by the agencies (Protecting Industrial Control Systems, 2011; Scarfone and Mell, 2007; Stouffer, 2013) are steps in the right direction to lay down industry's best practices. One of the promising techniques in this category is penetration testing, especially by third party that can help to expose hidden vulnerabilities (Igure et al., 2006) and implement corrective action enabling system validation and remedy of any security weaknesses.

There are other promising techniques, such as simulation, modelling, and security assessment and honey pots. This, coupled with the desire of the SCADA vendors to provide integration with commercial database systems, will make it possible for real time data analytics to identify a threat vector before it strikes. The selected techniques are important for the system developers to confirm adherence to security policies and certify a degree of protection against threats.

6. Future research directions

Recent technological developments in communications and networking have revolutionised the control and process networks making it much easier to access the data remotely and conveniently. The current research for cyber security protection has many promising techniques.

The emerging techniques such as SDN (highlight reconfigurability) and virtualisation platform provides many benefits such as copying, restoring, deleting and backing-up virtual machines (VMs) on the fly. High Availability and Vmotion which enable continued operation of a virtual machine during migration. The virtualisation platform provides many benefits such as isolation, snapshots, migration and restoring of virtual machines. Virtualised deployments are thus easier to protect compared to physical servers. Through update manager the vital updates can be automatically downloaded and applied.

Cloud computing is still a new technology for SCADA (Piggin, 2014). The control and monitoring industry has not yet fully embraced cloud computing because it is different from conventional IT systems. With further increase in network speeds, reliability and storage technologies, SCADA servers could be hosted on the cloud infrastructure. The advantages would be an easy enforcement of security standards, data analytics and disaster recovery. A technology similar to cloud that is gradually being adopted by the control industry is virtualisation. With a private cloud (Simmhan et al., 2013) or virtual infrastructure an organisation can have the benefits of on-site SCADA deployment and the benefits of disaster recovery, migration, and high availability. This also ensures keeping the data latency to a minimum.

In future, more open communications standards for SCADA systems are expected to be adopted reversing the trend where most of the products were closed and proprietary. There are open source projects such as OpenSCADA (OpenSCADA). Although debatable (Clarke et al.) whether better protection is offered by a closed system by "obscurity" of its implementation, or an open system, where the source is a public domain with a possibility for misuse by implementing a targeted attack. In the case of open systems, the user community can help by providing fixes both before and after vulnerability gets exploited through an attack. Such fixes could be quicker as there are more people using the system with full knowledge with more likelihood to uncover a potential threat.

The OPC UA (Unified Architecture) is an open industrial (Cavalieri et al., 2010; Leitner and Mahnke, 2006) Machine-to-Machine communication protocol that replaced OPC DA. OPC UA is a set of 9 standards, with one devoted to security. The general concept is to simplify the SCADA communication interface by providing a common medium of communication (Wu et al., 2011). used OPC communication from SCADA systems to collect system data for modelling a water distribution network. The data from the OPC server could similarly be used to investigate real-time cyber security issues by applying data analysis techniques.

Machine learning and data analytics have now advanced and are increasingly being used in new application domains. The large data generated (Tesfahun and Bhaskari, 2016) in a smart system can be used to extract information through data analytics for effective management. Machine learning techniques can be very useful for implementing strategies using an anomaly based unsupervised detection (Almalawi et al., 2014) approach for detecting attacks on SCADA systems. Future deployments of SCADA projects would see tighter integration between the process data and machine learning based data analysis engines observing historical data for anomalous behaviour to thwart cyber security breaches.

With industry regulations mandating cyber security for the SCADA systems, vendors will provide more built-in security features in their systems against cyber-attacks. For example, features such as multiplexing proxies.

There is also a lot of ongoing work to improve the communications protocols (Jain and Tripathi, 2013) to provide better protection against attackers. For example, security was added to DNP3 protocol by creating its extension called DNPSec (Fovino et al., 2009). These developments are to be seen in the context of emerging IoT or smart devices which are now common in SCADA networks. There are both benefits and pitfalls to their use with the security as the main hurdle to their widespread adoption. IoT with its unique IPv6 addresses is both an opportunity and challenge for cyber security.

In future, there will be a need for a lot more collaboration (Slay and Miller, 2008) between researchers, academics, vendors, developers, and government agencies to design foolproof solutions through integrated and cohesive efforts to meet the security challenges.

Acknowledgement

The authors gratefully acknowledge funding support from Innovate UK for sponsoring the KTP project at London South Bank University, in collaboration with Firstco Ltd.

REFERENCES

Aircrack-NG. [online]. Available from: https://www.aircrack-ng.org/. [Accessed 25.06.17].

Almalawi A, Yu X, Tari Z, Fahad A. An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. Comput Secur 2014;46:94–110.

August T, August R, Shin H. Designing user incentives for cybersecurity. Commun ACM 2014;57(11):43–6.

Backhaus S, Bent R, Bono J, Lee R, Tracey B, Wolpert D, et al., Cyber-physical security: a game theory model of humans interacting over control systems. arXiv:1304.3996 [cs.GT].

Baecher P, Koetter M, Holz T, Dornseif M, Freiling F. The Nepenthes platform: an efficient approach to collect malware. LNCS 2006;4219:165–84.

Boldea CN. SCADA virtual test environment development; [online]. Available from: www.eea-journal.ro/includes/showArticle.php?identificatorArticol=310. [Accessed 25.06.17].

Bouchti AE, Haqiq A. Modeling cyber-attack for SCADA systems using CoPNet approach. In: International conference on complex systems (ICCS); Nov 2012. pp. 1–6,

Brand M, Valli C, Woodward A. A threat to cyber resilience: a malware rebirthing botnet. In: International cyber resilience conference; 2011.

Byres EJ, Franz M, Miller D. The use of attack trees in assessing vulnerabilities in SCADA systems. In: International infrastructure survivability workshop (IISW '04), Lisbon, Portugal; 2004.

Bytschkow D, Zellner M, Duchon M. Combining SCADA, CIM, GridLab-D and AKKA for smart grid co-simulation. In: IEEE innovative smart grid technologies conference; 2015.

Carcano A, Coletta A, Guglielmi M, Masera M, Nai Fovino I, Trombetta A. A multidimensional critical state analysis for detecting intrusions in SCADA systems. IEEE Trans Ind Inform 2011;7(2).

Cavalieri S, Cutuli G, Monteleone S. Evaluating impact of security on OPC UA performance. In: 3rd conference on human system interactions (HSI); 23 Jul 2010.

Chabuksawar R, Sinopoli B, Karsai G, Giani A, Davies A, Neems H, et al. Simulation of network attacks on SCADA systems. In: First workshop on secure control systems; 2010. [Accessed 25.06.17].

Cherdantseva Y, Burnap P, Blyth A, Eden P, Jones K, Soulsby H, et al. A review of cyber security risk assessment methods for SCADA systems. Comput Secur 2016;56:1–27.

Ciancamerla E, Minichino M, Palmieri S. Modeling cyber-attacks on a critical infrastructure scenario. In: Fourth international conference on information, intelligence, systems and applications, IISA; Jul 2013. pp. 1–6.

Clarke R, Dorwin D, Nash R. Is open source software more secure? [online]. Available from: https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/oss(10).pdf. [Accessed 25.06.17].

Constantin L. New Havex malware variants target industrial control system and SCADA users, PC World, Jun 2014.

Ćardenas AA, Amin S, Sastry S. Research challenges for the security of control systems. In: Proc. of the 3rd conference on hot topics in security, HOTSEC '08, Article No. 6; 2008.

Curtis, K. A DNP3 Protocol Primer; 2005. [online]. Available from: http://www.dnp.org/pages/aboutdefault.aspx. [Accessed 25.06.17].

Davies A, Karsai G, Neems H, Giani A, Sinopoli B, Chabuksawar R. TRUST for SCADA: a simulation-based experimental platform, presentation [online]. Available from: http://slideplayer.com/slide/3377726/.

Dell Security Annual Threat Report; 2016. [online]. Available from: http://www.netthreat.co.uk/assets/assets/dell-security-annual-threat-report-2016-white-paper-197571.pdf. [Accessed 25.06.17].

Disso JP, Jones K, Bailey S. A plausible solution to SCADA security honeypot systems. In: Proc. 2013 eighth international conference on broadband, wireless computing, communication and applications; Oct 2013.

Dondossola G, Garrone F, Szanto J. Supporting cyber risk assessment of power control system with experimental data. In: IEEE PCSE power systems conference and exposition, Seattle, Washington, USA; 15–18 Mar 2009.

Dong X, Lin H, Tan R, Iyer RK, Kalbarczyk Z. Software-defined networking for smart grid resilience: opportunities and challenges. In: Proc. of the 1st ACM workshop on cyber-physical system security, New York, NY, USA; 2015, pp. 61–8.

Downs JJ, Vogel EF. A plant-wide industrial process control problem. Comput Chem Eng 1993;17(3):245–55.

ENISA, Good practices and recommendations for developing harmonised certification schemes; Dec 2014.

Erol-Kantarci M, Mouftah HT. Smart grid forensic science: applications, challenges, and open issues. IEEE Commun Magaz 2013;51(1):68–74.

Farooqui AA, Zaidi SSH, Memon AY, Qazi S. Cyber security backdrop: A SCADA testbed. In: IEEE conference on computing, communications and IT applications, ComComAp 2014, Beijing; Oct 2014. pp. 98–103.

Fovino IN, Coletta A, Carcano A, Masera M. Critical state-based filtering system for securing SCADA network protocols. IEEE Trans Industr Electron 2012;59(10).

Fovino IN, Carcanoa A, Maseraa M, Trombettab A. An experimental investigation of malware attacks on SCADA systems. Int J Crit Infrastr Protect 2009;2(4):139–45.

Genge B, Siaterlis C. Physical process resilience-aware network design for SCADA systems. Comput Electr Eng 2014;40(1):142–57.

Genge B, Siaterlis C, Fovino IN, Masera M. A cyber-physical experimentation environment for the security analysis of networked industrial control systems. Comput Electr Eng 2012;38(5):1146–61.

Giani A, Karsai G, Roosta T, Shah A, Sinopoli B, Wiley J. A test bed for secure and robust SCADA systems, Special issue on the 14th IEEE real-time and embedded technology and applications symposium, vol. 5, no. 2, Jul 2008.

Goldenberg J, Shavitt Y, Shir E, Solomon S. Distributive immunization of networks against viruses using the 'honey-pot' architecture. Nat Phys 2005;1:184–8.

Guide to industrial control systems (ICS). NIST Special Publication 800-82, Revision 2; May 2015.

Hahn A, Kregel B, Govindarasu M, Fitzpatrick J, Adnan R, Sridhar S, et al., Development of the powercyber SCADA security testbed. In: Proc. of the sixth annual workshop on cyber security and information intelligence research; 2010.

Hemingway G, Neema H, Nine H, Sztipanovits J, Karsai G. Rapid synthesis of HLA-based heterogeneous simulation: a model-based integration approach. J Simul 2012;88(2):217–32. Available from: http://www2.engr.arizona.edu/~sprinkjm/research/c2wt/uploads/Internal/Heterogeneous-Simulation.pdf.

Henry MH. Minimax envelopes for total cyber risk management in process control networks [Ph.D. Dissertation]. Department of Systems and Information Engineering, University of Virginia, 2007.

Henry MH, Haimes YY. A comprehensive network security risk model for process control networks. Risk Anal 2009;29(2).

Honeyd: Open source tool for creating Honeypots. [online]. Available from: www.honeyd.org/. [Accessed 25.06.17].

Hug G, Giampapa JA. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans Smart Grid 2012;3(3):1362–70.

Huitsing P, Chandia R, Papa M, Shenoi S. Attack taxonomies for the Modbus protocols. Int J Critic Infrastr Protect 2008;1:37–44.

IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)– Framework and Rules, In: IEEE Std 1516-2010 (Revision of IEEE Std 1516-2000), pp.1–38, 2010.

Igure VM, Laughter SA, Williams RD. Security issues in SCADA networks. Comput Secur 2006;25:498–506.

Information Security Management (ISMS), ISO/IEC 27001 [online]. Available from: http://www.bsigroup.com/en-GB/iso-27001-information-security/.

Jain P, Tripathi P. SCADA security: a review and enhancement for DNP3 based systems. CSIT 2013;1(4):301–8. doi:10.1007/s40012-013-0024-2.

Jiang J, Yasakethu L. Anomaly detection via one class SVM for protection of SCADA systems. In: International conference on cyber-enabled distributed computing and knowledge discovery (CyberC); 2013.

Jin D, Nicol DM, Yan G. An event buffer flooding attack in DNP3 controlled SCADA systems. In: Proc. of winter simulation conference, AZ, USA; 2011. pp. 2614–26.

Kesler B. The vulnerability of nuclear facilities to cyber attack. Strat Insights 2011;10(1).

Kirsch J, Goose S, Amir Y, Wei D, Skare P. Survivable SCADA via intrusion-tolerant replication. IEEE Trans Smart Grid 2014;5(1):60–70.

Langner R. Stuxnet- Dissecting a cyberwarfare weapon. IEEE Secur Privacy 2011;9(3):49–51. doi:10.1109/MSP.2011.67.

Leitner SH, Mahnke W. OPC UA – service-oriented architecture for industrial applications. [online]. Available from: http://pi.informatik.uni-siegen.de/stt/26_4/01_Fachgruppenberichte/ORA2006/07_leitner-final.pdf. [Accessed 25.06.17].

Leszczyna R, Fovino IN, Masera M. Simulating malware with MalSim. J Comput Virol 2008;6(1):65–75.

Li F, Shen L, Si Y, Niu J. A method to enhance SCADA systems survivability through simulation technology. In: 2009 International conference on measuring technology and mechatronics automation, ICMTMA; Apr 2009.

Li S, Tryfonas T, Li H. The internet of things: a security point of view. Int Res 2016;26(2):337–59.

Li W, Xie L, Deng Z, Wang Z. False sequential logic attack on SCADA system and its physical impact analysis. Comput Secur 2016;58:149–59.

MacDermott A, Shi Q, Merabti M, Kifayat K. Intrusion detection for critical infrastructure protection, 2012 PGNet.

Mahboob A, Zubairi JA. Securing SCADA systems with open source software. In: 10th International conference on high capacity optical networks and enabling technologies (HONET-CNS); Dec 2013.

Mahoney W, Gandhi RA. An integrated framework for control system simulation and regulatory compliance monitoring. Elsevier Int J Crit Infrastr Protect 2011;4(1):41–53.

Mallouhi M, Al-Nashif Y, Cox D, Chadaga T, Hariri S. A test bed for analyzing security of SCADA control systems (TASSCS). IEEE PES Innovative Smart Grid Technologies (ISGT), Jan 2011, pp. 1–7.

Markovic-Petrovic JD, Stojanovic MD. Analysis of SCADA system vulnerabilities to DDoS attacks. In: 11th International conference on telecommunication in modern satellite, cable and broadcasting service, TELSIKS, Oct 2013.

Mathioudakis K, Frangiadakis N, Merentitis A, Gazis V. Towards generic SCADA simulators: A survey of existing multi-purpose co-simulation platforms, best practices and use-cases, [online]. Available from: http://conf-scoop.org/ACE-2013/6_Kostas_ACE.pdf. [Accessed 25.06.17].

Maynard P, McLaughlin K, Haberler B. Towards understanding Man-in-the-middle attacks on IEC 60870-5-104 SCADA networks. In: International symposium for ICS & SCADA cyber security research (ICS-CSR), St Polten, Austria, Sep 2014. [Accessed 25.06.17].

Metasploit. [online]. Available from: https://www.metasploit.com/. [Accessed 25.06.17].

Mets K, Ojea JA, Develder C. Combining power and communication network simulation for cost-effective smart grid analysis. IEEE Commun Surveys Tutor 2014;16(3):1771–96.

Microsoft Security Bulletins. [online]. Available from: https://technet.microsoft.com/en-us/security/bulletins.aspx. [Accessed 25.06.17].

Mo Y, Chabukswar R, Sinopoli B. Detecting integrity attacks on SCADA systems. IEEE Trans Contr Syst Technol 2014;22(4):1396–407.

Moore AP, Ellison RJ, Linger RC. Attack modelling for information security and survivability, Technical note, CMU/SEI-2001-TN-001, 3-15-2001. Software Engineering Institute, Carnegie Mellon University, 2001.

Morris T, Vaughn R, Dandass YS. A testbed for SCADA control system cybersecurity research and pedagogy. In: Proc. of the seventh annual workshop on cyber security and information intelligence research; 2011.

Moya JM, Araujo A, Bankovic Z, de Goyeneche J, Vallejo JC, Malagón P, et al. Improving security for SCADA sensor networks with reputation systems and self-organizing maps. Sensors (Basel) 2009;9:9380–97. doi:10.3390/s91109380.

nmap. [online]. Available from: https://nmap.org/. [Accessed 25.06.17].

Nader P, Honeine P, Beauseroy P. l_p -norms in one-class classification for intrusion detection in SCADA systems. IEEE Transactions on Industrial Informatics 2014;10(4):500–9.

National SCADA Test Bed. Available from: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf. [Accessed 25.06.17].

NETA. [online]. Available from: www.omnetpp.org/component/content/article?id=3712:neta-release. [Accessed 25.06.17].

Novak P, Šindelař R, Mordinyi R. Integration framework for simulations and SCADA systems. Elsevier Simul Model Pract Theory 2014;47:121–40.

O'Kane P, Sezer S, McLaughlin K, Im EG. SVM training phase reduction using dataset feature-filtering for malware detection. IEEE Trans Inf Foren Secur 2013;8.

Oman P, Phillips M. Intrusion detection and event monitoring in SCADA networks. In: Goetz E, Shenoi S editors. Critical Infrastructure Protection. ICCIP 2007, vol. 253. IFIP

International Federation for Information Processing. Boston, MA: Springer; 2008.

OpenSCADA. [online]. Available from: http://openscada.org/. [Accessed 25.06.17].

OSSEC. [online]. Available from: http://ossec.github.io/. [Accessed 25.06.17].

OSSIM. [online]. Available from: https://www.alienvault.com/products/ossim. [Accessed 25.06.17].

Pauna A, Moulinos K. Window of exposure. . . a real problem for SCADA systems? ENISA Recommendations for Europe on SCADA patching, Dec 2013.

Peterson D. Quickdraw IDS 4.1 Release, [Online]. Available from: http://www.digitalbond.com/blog/2011/02/28/quickdraw-ids-4-1-release/ [Accessed 25.06.17].

Pham VH, Dacier M. Honeypot trace forensics: the observation viewpoint matters. Elsevier Future Gen Comput Syst 2011;27(5):539–46.

Phillips C, Swiler LP. A graph-based system for network-vulnerability analysis. In: Proc. of the 1998 workshop on new security paradigms (NSPW '98); 1998. p. 71–79.

Pidikiti DS, Kalluri R, Kumar RKS, Bindhumadhava BS. SCADA communication protocols: vulnerabilities, attacks and possible mitigations. CSIT; 2013.

Piggin RSH. Securing SCADA in the cloud: Managing the risks to avoid the perfect storm. In: IET & ISA 60th International instrumentation symposium; Jun 2014.

Protecting Industrial Control Systems. Recommendations for Europe and Member States. ENISA; 2011.

Queiroz C, Mahmood A, Tari Z. SCADASim – a framework for building SCADA simulations. IEEE Trans Smart Grid 2011;2(4):589–97.

Queiroz C, Mahmood A, Tari Z. A probabilistic model to predict the survivability of SCADA systems. IEEE Transactions on Industrial Informatics 2012;9(4):1975–85.

Ralston PAS, Graham JH, Hieb JL. Cyber security risk assessment for SCADA and DCS networks. Elsevier ISA Trans 2007;46(4):583–94.

Roberts P. SCADA vendors still need security wake-up call, [online]. Available from: https://threatpost.com/scada-vendors-still-need-security-wake-call-102410/74603/. [Accessed 25.06.17].

Scarfone K, Mell P. Guide to intrusion detection and prevention systems (IDPS). NIST Special Publication 800-94; 2007.

Scarfone K, Souppaya M. User's guide to securing external devices for telework and remote access. NIST Special Publication 800-114, Nov 2007.

Schneier B. Attack Trees. Dr. Dobb's Journal of Software Tools 24, Dec 1999, pp. 21–2.

SCADA, SCADA Market by Component (Programmable Logic Controller, Remote Terminal Unit, Human Machine Interface, Communication Systems), Architecture (Hardware, Software, Services), Application, and Geography – Global Forecast to 2022, [online]. Available from: http://www.marketsandmarkets.com/PressReleases/supervisory-control-data-acquisition.asp. [Accessed 25.06.17].

Simmhan Y, Aman S, Kumbhare A, Liu R, Stevens S, Zhou Q, et al. Cloud-based software platform for big data analytics in smart grids. Comput Sci Eng 2013;15(4):38–47.

Slay J, Miller M. Lessons learned from the maroochy water breach. In: Goetz E, Shenoi S editors. Critical Infrastructure Protection. ICCIP 2007, vol. 253. IFIP International Federation for Information Processing. Boston, MA: Springer; 2008.

Snort. [online]. Available from: https://www.snort.org/. [Accessed 25.06.17].

Sploitware. [online]. Available from: https://github.com/enaqx/sploitware. [Accessed 25.06.17].

Sridhar S, Manimaran G. Data integrity attacks and their impacts on SCADA control system. In: IEEE PES General Meeting, pp. 1–6, Jul 2010.

Srivastava A, Morris T, Ernster T, Shengyi CV, Adhikari U. Modeling cyber-physical vulnerability of the smart grid with incomplete information. IEEE Trans Smart Grid 2013;4(1).

Stouffer K. NIST Briefing: ICS Cybersecurity Guidance – NIST SP 800-82. Guide to ICS Security, Aug 2013.

Süß JG, Pop A, Fritzson P, Wildman L. Towards integrated model-driven testing of SCADA systems using the Eclipse modeling framework and Modelica. In: Proc. of 19th Australian conference on software engineering, pp. 149–159; 2008.

Symantec Security Response, Dragonfly: Cyberespionage attack against energy suppliers, [online], 2014. Available from: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf [Accessed 25.06.17].

Ten CW, Liu CC, Govindarasu M. Vulnerability assessment of cybersecurity for SCADA systems using attack trees. In: IEEE Power Engineering Society General Meeting, Jun 2007.

Ten CW, Liu CC, Manimaran G. Vulnerability assessment of cybersecurity for SCADA systems. IEEE Trans Power Syst 2008;23(4).

Ten CW, Manimaran G, Liu CC. Cyber security for critical infrastructures: attack and defence modelling. IEEE Trans Syst Man Cybernet A Syst Humans 2010;40(4).

Ten Leading Practices for Smart Grid Analytics. Accenture Report. [online]. Available from: https://www.accenture.com/gb-en/accenturesmartsolutions-sustainability. [Accessed 25.06.17].

Tesfahun A, Bhaskari DL. A SCADA testbed for investigating cyber security vulnerabilities in critical infrastructures. Autom Contr Comput Sci 2016;50(1):54–62.

Torrisi NM, Vukovic O, Dan G, Hagdahl S. Peekaboo: a gray hole attack on encrypted SCADA communication using traffic analysis. In: IEEE international conference on smart grid communications, Nov 2014.

Urias V, Leeuwen BV, Richardson B. Supervisory command and data acquisition (SCADA) system cyber security analysis using a Live,Virtual, and Constructive (LVC) testbed. In: MILCOM 2012 IEEE military communications conference, Oct 2012, pp. 1–8.

Vijayan B. Stuxnet renews power grid security concerns, Computerworld. [online], Jul 26, 2010. Available from: http://www.computerworld.com/article/2519574/security0/stuxnet-renews-power-grid-security-concerns.html. [Accessed 25.06.17].

White paper, Web services security – the technology and its concerns, [online]. Available from: https://www.acunetix.com/websitesecurity/web-services-wp/. [Accessed 25.06.17].

Winn M, Rice M, Dunlap S, Lopez J, Mullins B. Constructing cost-effective and targetable industrial control system honeypots for production networks. Elsevier Int J Crit Infrastr Protect 2015;10(C):47–58.

Wu W, Gao J, Yuan Y, Zhao H, Chang K. Water distribution network real-time simulation based on SCADA system using OPC communication. In: 2011 IEEE international conference on networking, sensing and control (ICNSC), Delft, pp. 329–334. doi: 10.1109/ICNSC.2011.5874916, 2011.

Xie F, Peng Y, Zhao W, Han X, Li H, Zhang R, et al., Using simulation platform to analyze radio modem security in SCADA. In: 7th International symposium on resilient control systems (ISRCS), 2014, pp. 19–21 Aug. 2014.

Yang L, Cao X, Li J, Wang A, Tan W, Yu Z. Research on FNN-based security defence architecture model of SCADA network. In: Proc. of IEEE 2nd international conference on cloud computing and intelligent systems, CCIS2012, Nov 2012.

Yang Y, McLaughlin K, Littler T, Sezer S, Wang HF. Rule-based intrusion detection system for SCADA networks. In: Proc. 2nd

IET conference in renewable power generation (RPG 2013), pp. 9–11, Sep 2013.

Yang Y, McLaughlin K, Sezer S, Yuan YB, Huang W. Stateful intrusion detection for IEC 60870-5-104 SCADA security. In: IEEE PES general meeting, conference & exposition, 27–31 July 2014.

Zhang Y, Wang L, Xiang Y, Ten CW. Power system reliability evaluation with SCADA cybersecurity considerations. IEEE Trans Smart Grid 2015;6(4):1707–21.

Zhang ZJ, Yang Z, Zhu LH, Xiao L, Zhao L. A survey of SCADA test bed. Int J Wireless Mobile Comput 2015;8(1):9–14.

Zhu B, Joseph A, Sastry S. A taxonomy of cyber attacks on SCADA systems. In: IEEE international conference on Internet of Things, and cyber, physical and social computing; 2011.

Sajid Nazir (PhD, FHEA, SMIEEE, MIET, AMAPM) is a Senior Engineer at Firstco Ltd., UK. He received PhD degree in Electrical Engineering from Strathclyde University, Glasgow, UK in 2012. He has worked on remote video monitoring projects as a Research Fellow at University of Aberdeen from 2012 to 2015. He also worked on virtualisation, CCTV and SCADA projects as a KTP Associate with the School of Engineering, London South Bank University, London, and Firstco Ltd., UK. He has authored one book and over 40 research publications. His research interests include video communications, machine learning, industrial systems and networking.

Shushma Patel (BSc (H), PhD., FBCS, CITP) is Professor of Information Systems in the School of Engineering at London South Bank University. She studied Life Sciences as an undergraduate, before completing a PhD from the Faculty of Medicine, University of London. She has more than 30 years of teaching and research experience in Cognitive Informatics, and Qualitative Research. She has worked on many EU and commercially funded projects, exploiting innovative technologies for business solutions. Her current interest in cyber security is informed by her considerable experience working with industry and in particular her interest in user behaviours.

Dilip Patel Professor Emeritus at London South Bank University. His academic career in computer science spans over 30 years. He has published extensively in the areas of object technology, cognitive informatics and database technologies. He was an editorial advisory board member for the book Model-Driven Domain Analysis and Software Development: Architectures and Functions. Dilip is also on the editorial board for The International Journal of Software Science and Computational Intelligence.