Cyber security testing and intrusion detection for synchrophasor systems

Thomas Morris*, Shengyi Pan, Uttam Adhikari, Nicolas Younan and Roger King

Mississippi State University,
Mississippi State, MS 39762, USA
Email: morris@ece.msstate.edu
Email: sp821@msstate.edu
Email: ua31@msstate.edu
Email: younan@ece.msstate.edu
Email: rking@cavs.msstate.edu
*Corresponding author

Vahid Madani

Pacific Gas and Electric Company,
San Francisco, CA 94105, USA
Email: vxm6@pge.com

Abstract: Synchrophasor systems are an emerging technology. Prior to installation of a synchrophasor system a set of cyber security requirements must be developed, new devices must undergo vulnerability testing, and proper security controls must be designed to protect the synchrophasor system from unauthorised access. This paper describes the process taken to develop a set of cyber security requirements for an American Recovery and Reinvestment Act (ARRA) funded synchrophasor project. The paper further describes vulnerability analysis and testing performed on synchrophasor system components. Finally, the paper describes intrusion detection rules written as a response to vulnerabilities discovered in the vulnerability analysis and testing process.

Keywords: cyber security; smart grid; industrial control system security.

Reference to this paper should be made as follows: Morris, T., Pan, S., Adhikari, U., Younan, N., King, R. and Madani, V. (2016) 'Cyber security testing and intrusion detection for synchrophasor systems', *Int. J. Network Science*, Vol. 1, No. 1, pp.28–52.

Biographical notes: Thomas Morris is Director of the Critical Infrastructure Protection Center and Assistant Professor of Electrical and Computer Engineering at Mississippi State University.

Shengyi Pan is a PhD student studying electrical and computer engineering at Mississippi State University.

Uttam Adhikari is a PhD student studying electrical and computer engineering at Mississippi State University.

Nicolas Younan is Department Head, Professor, and James Worth Bagley Chair of Electrical and Computer Engineering at Mississippi State University.

Roger King is William L. Giles Distinguished Professor of Electrical and Computer Engineering and Director of the Center for Advanced Vehicular Studies at Mississippi State University.

Vahid Madani is a Fellow of the IEEE and is responsible for Protection and Control Standards and Modernisation at Pacific Gas and Electric Co. (PG&E), USA.

1 Introduction

Multiple utilities in the USA received grants from the Department of Energy under the American Recovery and Reinvestment Act (ARRA) to create wide area monitoring systems. The ARRA grants require recipient entities to develop a cybersecurity plan which includes a risk assessment as part of parent wide area monitoring systems projects. Wide area monitoring systems require installation of phasor measurement units (PMUs), and substation phasor data concentrators (PDCs), among other devices and software. PMUs and substation PDCs are networked appliances which use routable protocols. As such, these devices may be declared North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) (http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx) critical cyber assets (CCA), depending upon each individual unit's application within the power system. CCA must be housed within an electronic security perimeter and undergo a cyber vulnerability assessment.

The IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security (IEEE, 2000) defines cyber intrusion or electronic intrusion as "Entry into the substation via telephone lines or other electronic-based media for the manipulation or disturbance of electronic devices". PMU and substation PDC are networked appliances and may become the target of attacks against bulk electric power systems. Threats against these devices include denial of service attacks, attacks against open ports and services intended to elevate privilege, attempts to change device settings, attempts to inject malicious device commands, attempts to hijack device access credentials or other confidential information, and attempts to place a man-in-the-middle between devices.

This paper describes the process used to develop a set of cyber security requirements for PMU and PDC installation. Three primary sources were used to derive cyber security requirements; NISTIR 7628: Guidelines for Smart Grid Cyber Security (http://csrc.nist.gov/publications/PubsNISTIRs.html), Department of Homeland Security: Cyber Security Procurement Language for Control Systems, and a set of internal requirements from the utility. Second, this paper describes testing performed to identify PMU and PDC vulnerabilities prior to device installation in a production control system. A Spirent (formerly MU) 4000 Network Analyser was used to perform network congestion testing, denial of service testing, and protocol mutation testing. Testing also included port scanning, OpenVAS vulnerability scanning, network traffic disclosure testing, security setting persistence testing, examination of device storage of passwords, and a man-in-the-middle attack demonstration. Results from the tests were provided to the utility to allow

the utility to work with device vendors to create corrective action plans. Testing also included a device security feature analysis and a mapping of security features to security requirements. PMU and PDC from multiple vendors were tested. Vendor names and product identifiers are withheld from this article to prevent enabling attacks. Finally, this paper includes a section on intrusion detection rules added as a result of cyber security testing. SNORT was used to inspect packets for flooding and protocol mutation attacks.

The body of this article includes a section on related works, a section describing synchrophasor system cyber security requirements development, a section describing cyber security testing of synchrophasor system components, a section describing the intrusion detection system, and finally, a section on future works and conclusions.

2 Related works

The Idaho National Labs (INL) National SCADA Testbed Programme is a large scale test bed program dedicated to control system cybersecurity assessment, standards improvement, outreach, and training. Noted research outcomes from the INL National SCADA Testbed Programme (2008) include published taxonomies of common industrial control vulnerabilities, published lessons learned from security assessments control systems (Fink et al., 2006), participation in standards enhancement and development, and development of recommended procurement language for wireless systems in the advanced metering infrastructure (Idaho National Laboratory, 2009). INL activities primarily involve security assessments, outreach, training, and standards development for the electric power industry. INL partners with industry software and equipment vendors for cyber security assessments of products.

Researchers have performed vulnerability assessments of generation and substation devices to support development of taxonomies of vulnerabilities related to industrial control systems. Fovino et al. (2010) describe a test bed used for vulnerability assessment of components found in a Turbo-Gas Power Plant.

Skaggs et al. (2002) describe a tool, NETGLEAN, testing device for network vulnerabilities. Two well known tools are available for network vulnerability testing of industrial control systems. Wurldtech Security Technologies Inc. (http://www.wurldtech.com/) offers the Achilles Satellite product for testing industrial control system devices. Spirent (www.spirent.com) offers the Spirent Studio test suite for testing networked devices, include industrial control system devices. Both products include protocol mutation and denial of service test suites.

3 Synchrophasor system cyber security requirements development

A set of cybersecurity requirements and recommendations were prepared from review of the National Institute of Standards and Technology Interagency Report (NISTIR) 7628 Guidelines for Smart Grid Cyber Security: Vol. 2, Security Architecture and Security Requirements (http://csrc.nist.gov/publications/PubsNISTIRs.html), Department of Homeland Security (DHS): Cyber Security Procurement Language for Control Systems (http://ics-cert.us-cert.gov/sites/default/files/FINAL-Procurement_Language_Rev4_100809_0.pdf), and utility internal requirements. NISTIR 7628 Vol. 2 includes a process for deriving cyber security recommendations and requirements for smart grid

systems. NISTIR 7628 requirements and recommendations are taken from NIST SP 800-53 Revision 3 (http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf), the Department of Homeland Security *Catalog of Control Systems Security: Recommendations for Standards Developers* (Control Systems Security Program, 2011), and NERC CIP (http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx). Each requirement is traceable to one or more of the aforementioned source documents.

A cross functional team was formed to review and discuss cyber security requirements and recommendations. This team included representatives from the utility, the vendor of PMU and PDC hardware, the vendor of the energy management system (EMS), bulk electric transmission system consultants, and a cyber security researcher from academia. Team members included cyber security engineers, power system engineers, network communications engineers, hardware and software designers, and management representatives. A subcommittee drafted an initial version of cyber security recommendations and requirements for the intended synchrophasor system. The initial draft was circulated to the larger team for review. Finally, multiple meetings were held with all team members to discuss each proposed cyber security requirement in detail. The resulting recommendations and requirements are included in Tables 1 and 2. Tables 1 and 2 list requirements pertinent to system hardware and software components. Requirements related to organisation and management, physical protections, services acquisition, macro information system protection, risk management and assessment, personnel security, planning, maintenance, incident response, information and document management, configuration management, training, and security program management exist but are not listed in Tables 1 and 2.

Table 1 Recommendations and requirements

Req. #	*Title*	*Description*
AC-4	Access enforcement	The synchrophasor system should enforce assigned authorisations for controlling access.
AC-7	Least privilege	The synchrophasor system should assign and enforce the most restrictive set of rights and privileges or access needed by users for the performance of specified tasks.
AC-8	Unsuccessful login attempts	The synchrophasor system should enforce a defined number of consecutive invalid login attempts by a user during a defined time period.
AC-9	Smart grid information system use notification	The synchrophasor system should display appropriate use banners where applicable.
AC-10	Previous logon notification	The synchrophasor system should notify the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.
AC-12	Session lock	The synchrophasor system should initiate a session lock after an organisation-defined time period of inactivity or upon receiving a request from a user; and retain the session lock until the user reestablishes access.

Source: Derived from NISTIR 7628 (http://csrc.nist.gov/publications/PubsNISTIRs.html)

Table 1 Recommendations and requirements (continued)

Req. #	*Title*	*Description*
AC-21	Passwords	The synchrophasor system should adhere to utility password complexity rules and passwords should be changed according to utility policy.
AU-2	Auditable events	A set of auditable events should be developed for the synchrophasor system.
AU-3	Content of audit records	The synchrophasor system should produce audit records for each auditable event.
AU-8	Time stamps	The synchrophasor system should use internal system clocks to generate time stamps for audit records.
AU-9	Protection of audit information	The synchrophasor system should protect audit information and audit tools from unauthorised access, modification, and deletion.
AU-10	Audit record retention	The synchrophasor system audit logs for a utility specified time period.
AU-16	Non-repudiation	The synchrophasor system should protect against an individual falsely denying having performed a particular action.
IA-5	Device identification and authentication	The synchrophasor system should uniquely identify and authenticate devices before establishing a connection where technically feasible.
SC-3	Security function isolation	The synchrophasor system should isolate security functions from non-security functions.
SC-5	Denial-of-service protection	The synchrophasor system should mitigate or limit the effects of denial-of-service attacks based on an organisation-defined list of denial-of-service attacks.
SC-7	Boundary protection	The synchrophasor system should be appropriately placed within electronic security perimeters.
SC-8	Communication integrity	The synchrophasor system protects the integrity of electronically communicated information.
SC-9	Communication confidentiality	The synchrophasor system should protect the confidentiality of sensitive communicated information.
SC-10	Trusted path	The synchrophasor system should establish a trusted communications path between the user and the synchrophasor system.
SC-12	Use of validated cryptography	All of the cryptography and other security functions that are required shall be NIST Federal Information Processing Standard (FIPS) approved.
SC-19	Security roles	Specific security roles and responsibilities for users of the synchrophasor system should be defined.
SC-20	Message authenticity	The synchrophasor system should provide mechanisms to protect the authenticity of device-to-device communications.

Source: Derived from NISTIR 7628 (http://csrc.nist.gov/publications/PubsNISTIRs.html)

Table 1 Recommendations and requirements (continued)

Req. #	*Title*	*Description*
SC-22	Fail in known state	Devices and software used in synchrophasor system should fail in a known state to prevent loss of confidentiality, integrity, or availability.
SC-26	Confidentiality of information at rest	Synchrophasor system hardware and software should employ cryptographic mechanisms for all critical security parameters to prevent unauthorised disclosure of information at rest.
SC-29	Application partitioning	The synchrophasor system should separate user functionality (including user interface services) from management functionality.
CP-10	Smart grid information system recovery and reconstitution	The utility must have the capability to recover and reconstitute the synchrophasor system to a known secure state after a disruption, compromise, or failure.

Source: Derived from NISTIR 7628 (http://csrc.nist.gov/publications/PubsNISTIRs.html)

Table 2 Recommendations and requirements derived from DHS cyber security procurement language for control systems

Req. #	*Title*	*Description*
PROC.1	System hardening	Vendor(s) shall list required ports and services for normal and emergency operation.
PROC.2	Least privilege	Vendor(s) shall configure systems with least privilege file and account access and provide documentation of the configuration.
PROC.3	Hardware configuration	Vendor(s) shall disable all unneeded communication ports and removable media drives.
PROC.4	Upgrade access control	Vendor(s) shall password protect the BIOS from unauthorised changes.
PROC.5	Patch management	Vendor(s) shall have a patch management and update process.
PROC.6	Perimeter protection	Vendor(s) shall provide detailed information on all communications (including protocols) required through a firewall.
PROC.7	Session management	Vendor(s) shall not permit user credentials to be transmitted in clear text.
PROC.8	Concurrent logins	Vendor(s) shall not allow multiple concurrent logins, applications to retain login information between sessions, provide any auto-fill functionality during login, or allow anonymous logins.
PROC.9	Account logout and timeout	Vendor(s) shall provide user account-based logout and timeout settings.
PROC.10	Warning banner	A standard warning banner developed by the utility and must be displayed when users logon to a utility computer system and/or network.

Source: DHS (http://ics-cert.us-cert.gov/sites/default/files/FINAL-Procurement_Language_Rev4_100809_0.pdf)

Table 2 Recommendations and requirements derived from DHS cyber security procurement language for control systems (continued)

Req. #	*Title*	*Description*
PROC.11	Least privilege	System owners must restrict privileges for all users, interconnected systems, and software based on the principle of least privilege. Where possible, system role accounts and programs must not run with elevated privileges.
PROC.12	Configurable password complexity	Vendor(s) shall provide a configurable account password management system that allows for selection of password length, frequency of change, setting of required password complexity, number of login attempts, inactive session logout, screen lock by application, and denial of repeated or recycled use of the same password.
PROC.13	Password storage	Vendor(s) shall not store passwords electronically or in vendor-supplied hardcopy documentation in clear text unless the media is physically protected.
PROC.14	Emergency security rollback	Vendor(s) shall provide a mechanism for rollback of security authentication policies during emergency system recovery.
PROC.15	Password encryption algorithm	Passwords must be encrypted using a utility approved cryptographic algorithm.
PROC.16	Password complexity	User account passwords to utility defined complexity requirements.
PROC.17	Activity logging	Vendor(s) shall provide a system whereby account activity is logged and is auditable both from a management (policy) and operational (account use activity) perspective.
PROC.18	Audit log time stamping and encryption	Vendor(s) shall time stamp, encrypt, and control access to audit trails and log files where feasible.
PROC.19	Audit log impact on system performance	Vendor(s) shall ensure audit logging does not adversely impact system performance requirements.
PROC.20	Audit log entry contents	Log data shall include the date and time of the event, the unique ID used to initiate the event, the type of event, success or failure, and the name of the object involved.
PROC.21	User accounts with defined role	Vendor(s) shall provide for user accounts with configurable access and permissions associated with the defined user role.
PROC.22	TCP/IP cybersecurity features	Vendor(s) shall provide physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorised modification or use.
PROC.23	Approved cryptographic algorithms	The use of cryptographic algorithms must be limited utility approved algorithms.

Source: DHS (http://ics-cert.us-cert.gov/sites/default/files/FINAL-Procurement_Language_Rev4_100809_0.pdf)

NISTIR requirements address access control (AC), audit requirements (AU), continuity of operations (CP), identification and authentication (IA), and smart grid information system and communication protection (SC). The requirements were derived using the NISTIR 7628 logical interface category 3: interface between control systems and equipment with high availability, without compute or bandwidth constraints. This interface category specifically includes communication interfaces between PMUs and a wide area measurement system. It was assumed that the synchrophasor system would eventually be used to source measurements to wide area protection system applications and therefore high availability was a requirement. It was also assumed that new computer systems and new communication bandwidth would be added to support the synchrophasor system and therefore not compute or bandwidth constraints were assumed.

Procurement requirements from Table 2 were used two ways. The requirements were taken as system cyber security requirements and the procurement requirements will be included as contract terms when purchasing hardware and software systems for the project.

Table 3 Requirements derived from internal utility documents

Req. #	*Title*	*Description*
Util.1	Vulnerability testing	Vulnerability and penetration testing should be performed on new devices proposed for connection to the power system communication network.

Most of the requirements found in internal utility documents overlapped with requirements derived from the other two sources. One requirement which did not overlap was the requirement that a vulnerability assessment be performed on components prior to connection to the power system communication network. This requirement is traceable to NERC CIP standards (http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx).

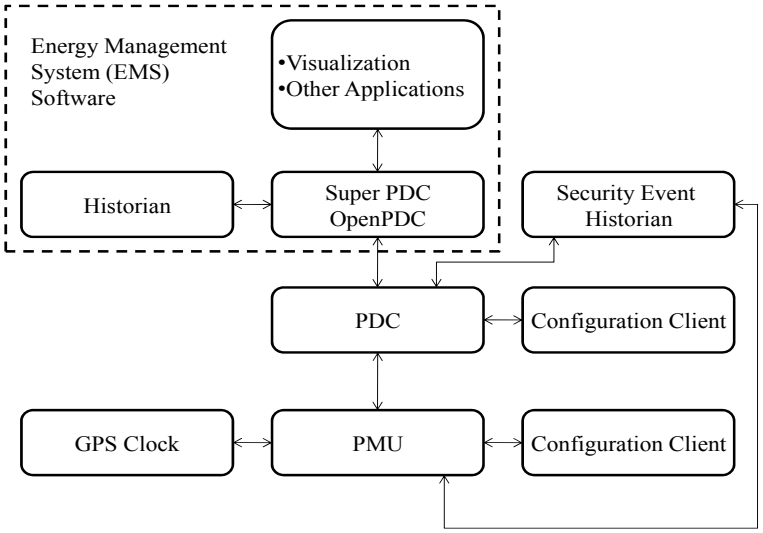
PMUs and PDCs may or may not be declared as CCA, per NERC CIP 002, depending upon the individual use case. As synchrophasor data streams become more tightly coupled with control actions, such as via use special protection schemes, the likelihood that PMU and PDC will be declared as CCA increases. For this work, PMU and PDC were treated as CCA.

4 Synchrophasor system cyber security component testing

The cyber security requirements from the above section were applied to hardware, software, and communication systems throughout the synchrophasor system. A diagram was developed which included all system components and communication interfaces to each component. A sanitised version of the synchrophasor system component diagram is shown in Figure 1. Cybersecurity requirements conformance was handled differently for different sub-systems. EMS conformance and testing was assigned to the EMS software vendor. PMU and PDC conformance and testing was performed in two steps. First, the PMU and PDC hardware vendors performed cyber security testing in house. Second, third party cyber security testing was performed on the PMUs and PDCs. Cyber security

test reports were submitted to the utility and PMU and PDC vendors for review. Cyber security test reports included test results with vulnerabilities ranked using a risk scale proprietary to the utility. All vulnerabilities were addressed by the cyber security team by either changes to firmware executed on the PMU and PDC or by system level architecture changes.

Figure 1 Synchrophasor system component diagram



NISTIR 7628 Volume 2 recommendation SC-5 Denial of Service Protection states "The Smart Grid information system mitigates or limits the effects of denial-of-service attacks based on an organisation-defined list of denial-of-service attacks" (NISTIR 7628, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf). This recommendation leaves the process of identifying denial-of-service vulnerabilities to the utility. Two methods were used to identify denial of service vulnerabilities related to the installation of PMU and PDC. First, network congestion tests were performed to test the device and system's ability to handle high volumes of network traffic. The network congestion tests also include well known denial of service exploits (such Ping flood, Teardrop, LAND attack, etc.). Second, protocol mutation testing was performed to attempt to identify unknown denial of service vulnerabilities specific to the tested PMU and PDC.

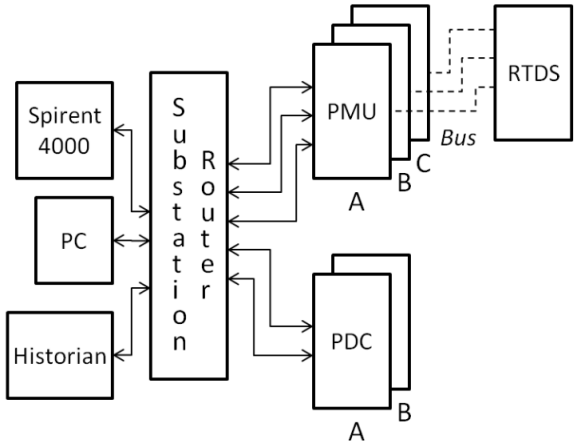
The rest of this section of the paper documents the cyber security test process performed on the PMUs and PDCs.

4.1 Test configuration

Three PMU and two PDC were tested. A Spirent (formerly Mu) 4000 Network Analyser was used to perform denial of service, network congestion, and protocol mutation tests. A personal computer (PC) was used with Wireshark to capture network traffic data logs and to host software used to configure and remotely control the PMU and PDC. The PMUs were connected to a real time digital simulator (RTDS) in a hardware-in-the-loop configuration. The RTDS provided simulated high voltage AC busses for the PMU's to

measure. PMU were connected through a substation router to PDC. PDC concentrated synchrophasor measurement streams from the PMU and forwarded this data to an OpenPDC installation which served as a historian for the system. Figure 2 shows the test bed configuration.

Figure 2 Test bed configuration



PMU periodically (typically at 30, 60, or 120 Hertz) measure voltage, current, and transmit voltage and current phasors (based upon a reference cosine waveform). PMU are time synchronised devices with clocks synchronised to universal time coordinated (UTC) with one microsecond accuracy. Synchrophasor network packets are transmitted from the PMU to a PDC. PMU adhere to the IEEE C37.118 standard which specifies measurement requirements and the synchrophasor measurement format. PMU may communicate over ethernet or serial port. Three PMU's were tested for this work. PMU A and PMU B shared the same vendor, while PMU C was manufactured by a second vendor. Both PMU communicate over ethernet using the IEEE C37.118 protocol.

PDC collect synchrophasor streams from multiple PMU and create a single stream for retransmission to another PDC or historian. PDC perform stream data rate conversion and can be configured to interpolate when data is missing from a stream. PDC adhere to the IEEE C37.118 standard and communicate over ethernet. Two PDC were tested for this work. PDC A and PDC B were manufactured by separate vendors.

4.2 Network congestion testing

The Spirent (formerly Mu) 4000 Network Analyser was used to perform network congestion testing. The Spirent (formerly Mu) 4000 denial of service test suite includes tests for multiple network protocols across all network OSI layers. The denial of service tests validate a device's ability to withstand large volumes of traffic directed at the device. The test engineer should identify relevant network protocols for testing.

Each network congestion test attempts to stress a separate portion of the device's network stack. The tests target a device's ability to process large volumes of a single type of network traffic. Many substation network appliances contain limited memory which can be exhausted and lead to operating system exceptions, cause services to stall, and or

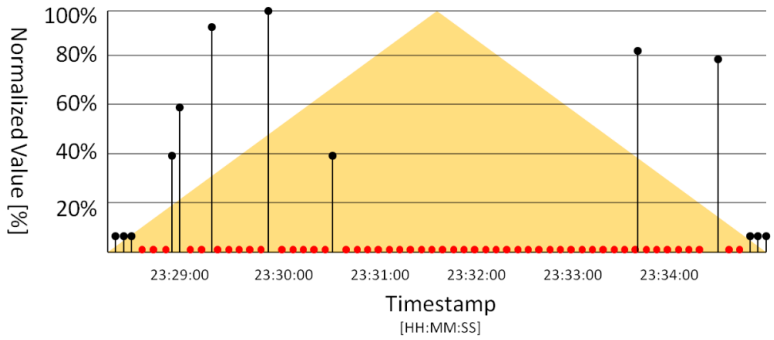
cause the device to reset itself. A set of network layer tests send floods of ARP requests, PPPOE packets, and IPv4 packets to the target device. Network layer variations send random packets of all three types, IP packets with random sizes and random payload, and IP packets with large numbers of IP fragments. A set of ICMP tests were also used. ICMP tests send floods of ICMP echo requests (aka. Ping flood or Smurf attack), ICMP echo packets with large payloads, address mask requests, and source quench messages.

Transport layer tests send floods of TCP and UDP packets to the device under test. TCP tests include variations which stress a device's ability to create and teardown TCP sessions with floods of TCP SYN and TCP FIN packets targeting individual TCP ports and to random TCP ports. UDP tests include random headers, port numbers, and payloads.

Two tests validate device behaviour for illegal packet types. A LAND test sends floods of IP packets with both the source and destination IP address set to the target's IP address. A teardrop test sends fragmented IP packets which have overlapping IP fragments.

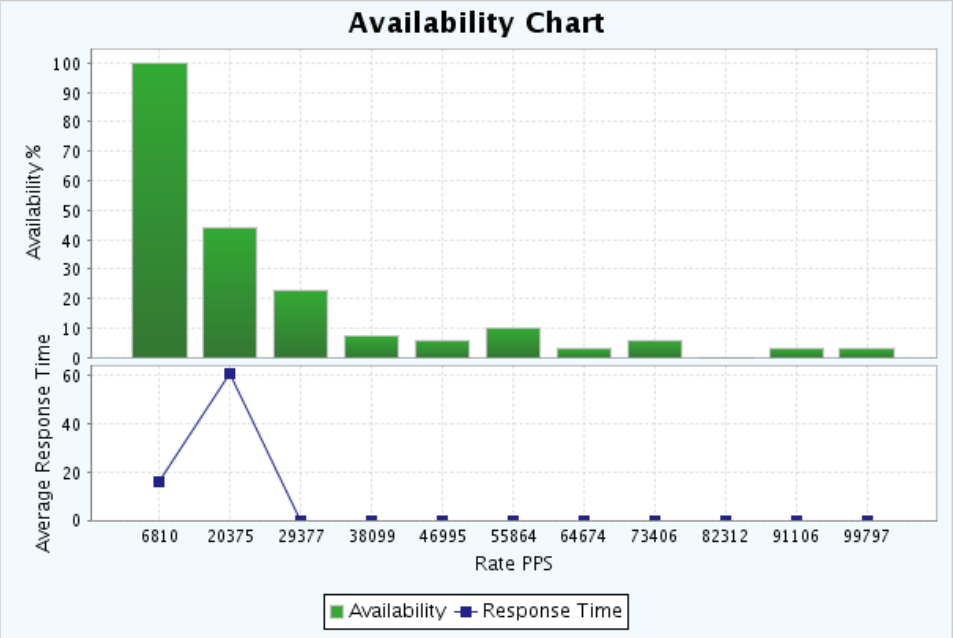
All devices tested eventually became unresponsive when the traffic volume increases beyond that devices ability to process packets. Figure 3 shows typical device behaviour to denial of service tests. The brown triangle shows the rate packets are being transmitted to the target device. As the tester ramps the packet rate it periodically sends the target an instrumentation packet (a query which the tested device is known to support) to test if the device is able to respond. The instrumentation packet may be a TCP session request on a supported port or an ICMP echo request or any other type of packet the target is known to be capable of responding to. The blue vertical lines show the target device responding to instrumentation requests. A taller blue line indicates a slower response time. The red dots indicate failed instrumentation request. As the packet rate increases devices become unresponsive. Some devices may hang or reset themselves when subjected to high packet rates. Many devices are unresponsive during the test, but, become responsive again when the packet rate returns to acceptable levels.

Figure 3 Denial of service test response time chart (see online version for colours)



Understanding the packet rate which causes a device to become unresponsive is important for system planning and for creating an effective denial of service mitigation approach. Figure 4 shows a typical availability chart for a single denial of service test against a device. The availability shows the percent availability (Y-axis), percentage of time that a device is able to respond to instrumentation requests, versus packet transmission rate (X-axis).

Figure 4 Availability chart from congestion testing (see online version for colours)



Utility engineers and network administrators can use the availability chart to define a maximum threshold for traffic congestion at the switch or router within the substation for the different traffic types. Based upon testing results it is recommended that utilities monitor network traffic volume in control system networks to detect transmission of high volumes of traffic. Monitoring systems should alert a human administrator to enable mitigation. Routers in the control system network may be configured to limit traffic sent to the PMU or PDC or may be configured to close ports sourcing offensive amounts of network traffic. Automatically closing router ports is potentially dangerous since critical traffic may use the port. A thorough system review should be performed before enabling automatic port closure. Maximum traffic rate thresholds should be defined for all relevant traffic types.

PMU and PDC transmit continuous streams of measurements at 30, 60, or 120 samples per second. Measurements are time stamped with one microsecond accuracy relative to UTC time. It is important to understand PMU and PDC behaviour after DOS event completes. Testers should confirm that tested devices and network appliances in the route do not queue large volume of IEEE C37.118 data packets which then leads to a synchrophasor stream which is perpetually delayed. PDC hold data from on time PMU to wait for data packets from late arriving PMU streams. A denial of service attack can have a persistent effect if the attacked PMU's date stream becomes consistently late after the attack. PDC eventually drop old data packets and begin to interpolate. PMU and PDC which recover from a denial of service attack should clear their transmit queues to avoid the aforementioned effects.

4.3 Protocol mutation

A second method to test for denial of service vulnerabilities is through protocol mutation, also known as fuzzing. Protocol mutation creates network packets with random contents. Each field in a packet's header, payload, and trailer is assigned a set of variant values. Variant values for a field may include legal values and illegal values. The protocol mutation tester creates a set of packets which include all combinations of all fields with all variant values. The number of combinations grows quickly and protocol mutation can be a slow process. The benefit of protocol mutation is that combinations of fields which may not be thought of by a human can be tested to confirm that the device network stack does not hang or reset when the test packet is processed. Protocol mutation is intended to discover vulnerabilities before they are discovered by an adversary and become exploited zero day vulnerabilities.

The selection of protocols for mutation testing was based on port scanning and device manual review results. All communication protocol supported by a device should be tested. Mutated protocols for the PMU and PDCs included ARP, TCP, UDP, IP, ICMP, DNP3, MODBUS, IEEE C37.118, and HTTP.

The Spirent (formerly Mu) 4000 Network Analyser was used to perform protocol mutation testing. As with the denial of service testing the tester sends groups of mutated packets to the target device. The tester periodically sends instrumentation packets (queries which the tested device is known to support) to confirm that the device under test can still respond. Protocol mutation requires two types of instrumentation packets. The first instrumentation is a communication packet and response pair which is known to work on the target device. This instrumentation is typically unrelated to the mutated protocol. This instrumentation confirms the device network stack is still functioning and responsive. It is possible the portion of the network stack associated with the mutated protocol will hang without affecting other parts of the network stack. For example, a UDP mutation may hang the UDP stack, but leave the TCP stack functioning correctly. The second instrumentation request type is a known good packet of the type being mutated. This instrumentation confirms the portion of the network stack related to the mutated protocol is still functioning and responsive.

Some services were capable of assignment to a variable TCP or UDP port number. In this case, protocol mutation was repeated for multiple ports. A good strategy for testing services with variable ports is to repeat testing with port assigned to multiple port numbers in the well known space (0–1023), multiple port numbers in the registered port range (1,023–49,151), and multiple port numbers in the private range (49,152–65,535). Some services are capable of assignment to a fixed set of port numbers. In this case, it is good practice to test at all legal port assignments.

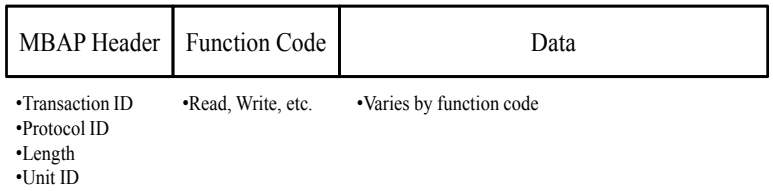
The Spirent (formerly Mu) 4000 includes built-in protocol mutation capabilities for many well known protocols. Some protocols are not supported. For example, IEEE C37.118 is not natively supported. Also, newly developed protocols may not initially be supported. The Spirent (formerly Mu) 4000 is capable of learning protocols from Wireshark packet captures. After learning a protocol the Spirent (formerly Mu) 4000 scenario builder can generate protocol mutations to test a device. The scenario builder feature was used for IEEE C37.118 protocol mutation. Only frames received as input by the target device should be mutated and sent to the target device. Mutated IEEE C37.118 commands frames were mutated and sent to PMUs. Mutated IEEE C37.118 configuration and data frames were sent to the PDCs.

Protocol mutation testing may identify individual packets which cause device failures including hanging network stacks or causing the device under test to reset itself. Protocol Mutation testing may also identify combinations of packets which cause similar device failures. In both cases careful study is required to determine the root cause of the failure. Mitigation of detected vulnerabilities can be achieved with a firewall or signature based intrusion prevention system (IPS) rules to block problem traffic. Vulnerabilities identified using protocol mutation should also be reported to the device vendor. Protocol mutation identified multiple issues on devices tested for this work. Issues included crashing of individual network services, crashing of applications running on devices, and unintended soft resetting of affected devices.

The Spirent (formerly Mu) 4000 works best as a client which sends mutated packets to a server. The Spirent (formerly Mu) 4000 uses randomisation algorithms and constrained randomisation algorithms to fuzz servers. The Spirent (formerly Mu) 4000 is less capable of fuzzing server to client responses, especially responses which are dependent upon the previous packet sent from the client. To overcome this issue an in-line fuzzer was developed to mutate server to client packets. The current version of the in-line fuzzer simply varies random bits of the server to client response to attempt to break random protocol rules. This method has proven effective at identifying vulnerabilities. A fuzzer is needed which properly mutates server to client responses based upon previous client to server packets and system state. The remainder of this section is analysis of the needs of such a fuzzer for MODBUS and IEEE C37.118 packets.

Many PMU and PDC provide a MODBUS/TCP server for remote control and for system monitoring. An EMS will often act as the MODBUS/TCP client. Figure 5 shows a MODBUS/TCP packet broken into three segments, the MBAP header, the function code, and the data segment.

Figure 5 MODBUS/TCP packet contents



Protocol mutation of MODBUS/TCP makes changes to packet contents which violate rules. The transaction ID field is a single byte which can take any value. MODBUS/TCP packets occur in query response pairs. The transaction ID field should match for a query and response pair. PMU and PDC are servers and therefore should respond to MODBUS/TCP queries with a transaction ID matching the query. Fuzzing examples of this field include using all possible transaction IDs and use transaction IDs out of order. For protocol mutations against a MODBUS/TCP client, the EMS, the transaction ID in the response can be changed to not match that of the query. This checks the EMS's ability to handle out of order responses and or responses which do not match a query. The MODBUS/TCP protocol ID field is a single byte which is always 0×0. Setting the protocol ID to non-zero values ensures that network stacks do not have errors for this unexpected value. Non-zero protocol ID values should be sent to both clients and servers.

The MODBUS/TCP length field is a single byte field which specifies the number of bytes remaining in the packet, in other words the length in bytes of the unit ID, the function code, and data segment. Fuzzing the length field can be accomplished by setting the length to values which do not match the remaining payload size. The length field should not exceed 256 in practice. Testing values above 256 is important. In testing some devices had errors when the length field was less than the actual remaining packet length. The unit ID field is a single byte which takes a predefined value to unique to each remote slave. It is common for this field to be limited to values between 0 and 247 since this was the legal address range supported by predecessor MODBUS/RTU and MODBUS/ASCII technologies. Attempting addresses outside of this range is important. MODBUS/TCP servers may have a predefined unit ID. Sending queries with a unit ID which does not match the server's assigned value is important. MODBUS/TCP servers may have a white list of connected unit IDs. Sending MODBUS/TCP responses not in this white list is important. The MODBUS/TCP function code field is a single byte. This field is limited by the MODBUS to a limited set of values. MODBUS servers typically further limit function code support to a subset of legal values. It is important to send illegal and unsupported function code values to MODBUS servers; PMU and PDC. It is important to send illegal and unsupported function code values to MODBUS clients; EMS. The function code must match in the query and response. Therefore it is important to send MODBUS clients responses with function codes which do not match the function code from the matching query. Some MODBUS function codes have a white list of sub-codes (found in the data segment). It is important to test the condition where sub-codes do not match the function code. The MODBUS/TCP data segment varies in size based upon the packet type (query or response) and the function code. Some function codes, such as read coils and write coils, include a quantity field (found in the data segment) which specifies the amount of data to read or write. Responses to these function codes have similar fields to specify the amount of data returned. It is important to test scenarios where the quantity field does not match the amount of data actually in the data segment. MODBUS responses have specified error codes for each function code. Error codes have specified exception code values for each error code. It is important to send invalid function code, error code, and exception code triplets to MODBUS clients. It is important to send MODBUS/TCP packets with very long data segments to test for buffer overflow vulnerabilities in the network stack. MODBUS/TCP does not include an application layer cyclic redundancy check (CRC) field. Instead MODBUS/TCP relies on the TCP CRC value to error check the MODBUS/TCP payload. It is important to send MODBUS/TCP queries and responses to servers and clients respectively which have incorrect CRC values.

IEEE C37.118 includes 4 types of packets; header, command, configuration, and data. Header and command packets are transmitted from the PDC to the PMU. Configuration and command packets are transmitted from the PMU to the PDC.

All 4 frame types include a 2-byte synchronisation word (SYNC). The first byte of the SYNC is defined as always 0xAA. It is important to check other values for this field. The second byte of the SYNC field includes a reserved bit, three bits to designate the frame type, and four bits for version number. There are five legal frame types. Illegal frame types should be sent; 0b101, 0b110, 0b111. All 16 possible version number possibilities should be sent; though only some have been defined to date. All four IEEE C37.118 frame types include a 2-byte frame size field. Frames should be sent with frame sizes which do not match the actual FRAMESIZE. Also, very large frame sizes should be

sent to test for buffer overflow possibilities. A four frame types include a 2-byte IDCODE field. This value is the PMU or PDC ID number. The values 0 and 65,535 are reserved and therefore should be tested. PMU and PDC typically have pre-programmed ID values. Frames with IDCODE values not assigned to the target device should be tested. All four IEEE C37.118 frame types include a 4-byte SOC field. The SOC field is a time stamp that counts the number of seconds since Jan-01-1970. The field is limited to 136 years which means the max value is 0xB34C00. Above 0xB34C00 the count is supposed to roll over. It is important to test values greater than 0xB34C00. All 4 IEEE C37.118 frame types include a 4-byte FRACSEC field. This field is broken into two parts. The most significant four bits of FRACSEC (bits 31-28) are used to document the presence of a leap second. Bit 31 is reserved and therefore transmitting a 1 in this bit should be tested. Bits 30 (LEAP) indicates a leap second is occurring. Bit 29 (LEAPED) indicates a leap second occurred in the last 24 hours. Bit 28 (TOLEAP) indicates a leap second will occur in the next second. Various fuzzing scenarios can be derived for these fields. First, the leap second bits should be asserted at times and dates when they are not expected. Seconds, LEAP should be set without first setting TOLEAP in the previous second. LEAP should be set without setting LEAPED in the following second and 24 hours. TOLEAP should be set with no following LEAP assertion. LEAPED should be asserted when not preceded by TOLEAP or LEAD combinations. Finally, all three bits (LEAP, LEAPED, TOLEAP) should be asserted at random times. The next 4 bits of FRACSEC (bits 27-24) are defined by a table to indicate clock faults and clock synchronisation values. There are multiple reserved values (0b1100, 0b1101, 0b1110) which should be tested. The remainder of the FRACSEC field is a number fraction of a second. This value is depended upon the TIMEBASE value from the PMU configuration frame. This value can be changed when configuring the PMU. FRACSEC values which do not match with the programmed TIMEBASE should be tested. Finally, all four IEEE C37.118 frame types include a 2-byte CHK field which is a 16-bit CRC. Frames with invalid CRC values should be tested. Some fuzzers make changes to valid packets by randomly flipping bit values. In this case the fuzzer should ensure that the CHK field is correct to ensure that more that the CRC logic is being tested.

The IEEE C37.118 data frame has multiple unique fields. Since data frames are transmitted from the PMU to PDC fuzzing data frames is limited to the PDC. The STAT field is a 2-byte field which provides PMU status. This field includes multiple reserved and user defined bits. All combinations of these bits should be tested. The PHASORS, FREQ, DFREQ, ANALOG, and DIGITAL fields all vary in size according to values in the configuration frame. The configuration frame is sent from the PMU to PDC during initial session start-up. Tests should include varying the number of values in these fields to not match the configuration frame definitions. Variation should include 0 bytes, larger, and smaller number of bytes for each field. PDC concentrate multiple synchrophasor streams from PMU into a single stream of IEEE C37.118 data frames. As such the size of the data frames output from PDC varies according to the number of PMU which is defined in a configuration from sent from the PDC to its upstream client, an EMS, state estimator, or openPDC. It is important to test varying data frame sizes. Very large sizes should be tested to check for buffer overflow vulnerabilities. Also, it is important to test data frame sizes which do not match the configuration frame.

The IEEE C37.118 configuration frame has multiple unique fields. Since configuration frames are transmitted from the PMU to PDC fuzzing data frames is

limited to the PDC. Fuzzing PDC configuration frames is a challenge because the PDC typically requests the configuration frame only once when the session is initiated. The PDC can be forced to request a configuration frame update by asserting bit 10 in the STAT word of a data frame send from the PMU to PDC. Bit 10 of the STAT word indicates the configuration has changed and the PDC should request to read the configuration files. The TIME_BASE field is four bytes. The most significant byte of TIME_BASE is reserved. Tests should be conducted with these bits set to non legal values (0–255). The NUM_PMU field 2-byte field which specifies the number of PMU in a data frame. This field can legally be up to 65,535. However, the actual limit is less than 65,535 since the maximum FRAMESIZE is 65,535. The actual limit depends upon the values of PHNMR, ANNMR, DGNMR, and FORMAT which set the number of phasors, analogue values, digital values, and format of said values for each PMU in the frame. Testing combinations of NUM_PMU and the PHNMR, ANNMR, DGNMR, and FORMAT which result in greater than 65,535 bytes in the data frame is important. Also, testing combinations of NUM_PMU and PHNMR, ANNMR, DGNMR, and FORMAT which result in do not match the data in the data frames is important. The CHNAM field is specified as 16*(PHNMR+ ANNMR +16 *DGNMR). Testing combinations of CHNAM, PHNMR, ANNMR, and DGNMR which do not adhere to the previous definition is important. The FORMAT field specifies the data type of FREQ, DFREQ, PHASORS, and ANALOG fields from the data frame. Testing combinations of FORMAT which do not match the values in the FREQ, DFREQ, PHASORS, and ANALOG fields in the data frame is important. Bits 15-4 of the FORMAT field are reserved. Testing non-zero fields in this field is important. The PHUNIT field of the configuration frame is four bytes. The most significant byte has legal values of 0 or 1. Testing should be completed to send values 2–255 in this byte. The ANUNIT field is a 4-byte field. The most significant byte of this field has several constraints. Values 3–4 are undefined by the specification. Values 5–64 are reserved. Values 65–255 are user definable. All values from 3–255 should be tested. THE DIGUNIT is 4-byte mask of the DIGITAL field from the data frame. Bits 63-48 and 32-16 are a mask which indicates the normal status of the digital bit corresponding to that bit lane. Test should be conducted to change normal status bit values for bits not in use in the DIGITAL field of the data frame. Test should also be conducted to inverts the normal value for bits which are in use in the DIGITAL field in the data frame. Bits 47-33 and 15-0 are masks which indicate which bytes are in use. Tests should be conducted to deselect DIGITAL field bits which are actually in use and select DIGITAL field bits which are not actually in use. The FNOM field is a 2-byte field which sets the nominal frequency. Only two values are allowed 0 and 1. Tests should be conducted for values from 2–65,535. The DATA_RATE field is a 2-byte signed integer representing the number of frames per second. Typically this value will be 30, 60 or 120 frames per second. However, the legal values are [–32,767, 32,767]. Testing should be conducted for multiple values throughout this range. Additionally, the value 0x8000 should also be tested since it fits in the field but is not specified as legal since it is effectively –0. CFGCNT is a 2-byte field which indicates the number of configuration changes since installation. This value should be varied out of order and changed to large values to test PDC response.

The IEEE C37.118 command frame has two unique fields. Command frames are sent to PMU. Command frames may also be sent to the upstream facing interface of the PDC.

The CMD field is a 2-byte field specifying the command. There are six defined values for this field. Undefined values should be sent to the device to test behaviour. EXITFRAME is a variable length field from 0–65,518 bytes. This size is limited by the FRAMESIZE field in the command frame. The value of EXITFRAME is user defined. Tests should be conducted to send non-zero size EXITFRAMEs. Also, test should be conducted in which the FRAMZSIZE is too large or too small based upon the size of the EXITFRAME field.

The IEEE C37.118 header frame has one type of unique field. Header frames are read from the PMU and therefore fuzzing of header frames is directed at the PMU. The header frame may have up to K ASCII bytes of data. The number of bytes of data is the FRAMESIZE – 16. The maximum number of data bytes is therefore 65,519. Header frames should be tested with non-ASCII characters in the data bytes of a header frame. Header frames with non-printable characters should also be tested in the data byte fields. Finally, testing should be conducted when the FRAMESIZE specified incorrect for the number of data bytes transmitted.

4.4 Other testing

NISTIR 7628 recommends communication integrity for synchrophasor systems. Communication integrity and communication confidentiality is not addressed by IEEE C37.118. VPN tunnelling between the control centre and substation can be used to provide these features (OpenVAS, http://www.openvas.org/). At a minimum, passwords should be encrypted when transmitted to PMU or PDC. Wireshark was used to capture network traffic during a remote login attempt to confirm passwords were not sent as plaintext. Careful review of network logs is necessary to find the transmitted password. Passwords may be transmitted as ASCII or obfuscated with XOR schemes or other schemes which are not based on approved cryptographic methods.

NERC CIP standards require unused ports and services on CCA to be disabled. Two open source software tools, NMAP Security Scanner (http://www.nmap.org) and OpenVAS (http://www.openvas.org/) were used to perform port scans of the tested PMU and PDC. NMAP and OpenVAS both identify open TCP and UDP ports and both attempt to identify the service running on open ports. Port scan results were used to build a table of open ports and services on the tested devices. Open ports and services were cross referenced with a list of required services. Unused ports and services should be disabled. A device may support electronically configuring ports to be off. Alternatively, firewalls may be used to block access to the port. Firewalls should be configured to deny all traffic except for white listed traffic types. Port scan results were also used to attempt to identify ports and services with known published vulnerabilities. NMAP and OpenVAS attempt to identify service name, service revision, and operating system revision information for open ports (in addition to transport protocol and port number). This information can be cross checked against published vulnerability databases including US Computer Emergency Readiness Team (US-CERT), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and Common Vulnerabilities Exposures (CVE).

4.5 Device security feature analysis

PMU and PDC user manuals were reviewed for cybersecurity features. Identified cyber security features were listed in the PMU and PDC test reports. Cyber security features were also tested in a laboratory setting to confirm functionality.

PMU and PDC commonly use passwords for access enforcement meeting the NISTIR 7628 AC-4 requirement. All PMU and PDC tested met the principle of least privilege (NISTIR 7628 AC-7, DHS PROC.2) by requiring passwords to be entered before modifying device configuration or settings. In cases where a device user was able to manipulate settings and configuration via the device faceplate password entry was required. In cases were remote settings and configuration were allowed password entry was required prior to allowing changes. All devices included features to limit device access after a configurable number of failed password attempts (NISTIR 7628 AC-8). Typically, the number of failed password attempts to bar access was configurable. The time period users were locked out after triggering the failed password lock out was also typically configurable. NISTIR 7628 AC-9 and DHS procurement requirement PROC.10 require appropriate use banners where applicable. As previously mentioned, some of the tested devices allowed settings and configuration changes via the device faceplate. The team found that this requirement did not apply to the device faceplate since it was not feasible to add appropriate use banners in that location. Remote access for settings and configuration changes is typically performed by an accompanying software product. The team found that it was applicable to add appropriate use banners defined by the utility when these software tools are started. The team found that it was not applicable to report previous logon information (NISTIR 7628 AC-10) device users at the faceplate. The team found that it was applicable to report previous logon information to remote users. Many tested devices did not support this feature. All devices tested included a session lock feature (NISTIR 7628 AC-12) which ended password protected privileged sessions after a user defined time out period. In many cases devices did not adhere to password complexity requirements (NISTIR 7628 AC-21). NERC CIP 007-3 (http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx) requires device passwords to be at least 6 characters with a mix of alpha, numeric, and special characters. In some cases passwords were limited to numeric characters only. In some cases passwords did not meet length requirements. DHS Procurement Requirement PROC.12 requires devices to support configurable password complexity. No tested devices provide this feature and it was found to be technically infeasible for the devices to support this requirement. DHS Procurement Requirement PROC.4 specifically requires password protection of BIOS changes. PMU and PDC include firmware which can be upgraded. All tested devices required password entry before upgrading this device firmware. Typically this password was separate from other device passwords. NISTIR 7628 AU-16 requires the synchrophasor system to protect against individuals falsely denying having performed a particular action. Many devices tested used shared passwords. Shared passwords may allow users to perform actions and then deny them afterward. Shared passwords are used at the device faceplate. In this case utilities have physical security in place which limits access to substations and requires substation visitors to physically sign in or swipe a badge to enter the substation door. The team found this physical security coupled with device security logs would meet non-repudiation requirements. Shared passwords were also used in remote access scenarios. The remote clients included with some devices used two layers of password protection. Shared passwords were required when settings or

configuration changes were made while individual username and passwords were optionally required to start the remote client. The team found that the optional individual username and password feature should be used to meet the non-repudiation requirement. Additionally, the individual username must also be included in security data logs. NISTIR 7628 SC-9 requires communication confidentiality. The team found this requirement to be relevant to remote logon credential protection. Multiple tested devices did not encrypt passwords before transmission. Finally, NISTIR 7628 SC-26 requires confidentiality of information at rest. DHS Procurement requirement PROC.13 requires that passwords should not be stored electronically. Multiple devices stored passwords internally and did not adequately protect the stored passwords. Passwords were sometimes viewable in an encrypted form. The encryption algorithms used to protect stored passwords did not meet NISTIR 7628 SC-12 and DHS PROC.23 requirements.

The tested PMU and PDC included features to log security events. This meets NISTIR 7628 requirement AU-2 and DHS procurement requirement PROC.17. Logged events included notification of multiple password failures, notification of password changes, notification of password entry for settings and configuration changes, and notification of firmware updates. NISTIR 7628 requirement AU-3, AU-8 and DHS procurement requirement PROC.18 specify the content of logged events. Logged events should include a timestamp, the username associated with the event, the type of event, and the outcome of the event. Device event logs were found to include adequate information with the exception of the username field. The username was not present in security logs for events performed from a faceplate when shared passwords were used without individual account for each user. Devices which included separate user accounts for remote access did add the username to security event logs for each recorded event. The tested PMU and PDC were not designed for long term event log storage (NISTIR 7628 AU-10). This is unfeasible for most field devices which have limited storage capabilities. As such the cyber security team recommended use of a separate server to gather and store security events. This separate server is shown in Figure 1 as the security event historian. The security team worked with device vendors to devise a mechanism for extracting security events from the field devices. This process can be done via MODBUS query response on some systems, via network services such as file transfer protocol (FTP) (http://tools.ietf.org/html/rfc959) on some device, or via proposed services such as Syslog (The Syslog Protocol, http://tools.ietf.org/html/rfc5424) on systems.

NISTIR 7628 requirement SC-8 requires that the synchrophasor system protect the integrity of electronically communicated information. NISTIR 7628 requirement SC-10 requires establish a trusted communications path between the user and the synchrophasor system. NISTIR 7628 requirement SC-20 requires the synchrophasor system to provide mechanisms to protect the authenticity of device-to-device communications. The synchrophasor system includes two types of messages which should be covered by these features. First, the PMU and PDC can be configured remotely. Settings and configuration changes were found to be transmitted using common industrial communication protocols such as MODBUS and DNP3. These protocols do not include features for integrity, trusted path, and message authenticity. The security team recommends the use of SSL or IPSEC to meet these requirements for MODBUS and DNP3 network traffic. This would allow use of the existing industrial protocols while adding integrity, trusted path, and

message authenticity features at higher network layers. Second, all tested PMU and PDC transmit synchrophasor measurements using the IEEE C37.118. IEEE C37.118 also does not include message authenticity features. Stewart et al. (2010) discuss the feasibility of using IPSEC to protect synchrophasor communications. Feasibility depends upon the applications which will use the synchrophasor measurements. Wide area visualisation applications can accept the delay associated with IPSEC. Some wide area protection systems which will use synchrophasor measurements will not be able to accept IPSEC delays. IEC 61850 90-5 has been proposed as a secure alternative to IEEE C37.118. IEC 61850 90-5 will transport IEEE C37.118 and include authentication, confidentiality, and key distribution features. The security team recommends use of IEC 61850 90-5 to meet NISTIR 7628 requirement SC-8, SC-10, and SC-20. Use of IEC 61850 90-5 will also support meeting the NISTIR 7628 requirement SC-9 requirement for communication confidentiality.

5 Monitoring for electronic intrusion

NERC CIP 005-3 requirement 3.2 (http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx) requires utilities to implement monitoring process to detect and alert for unauthorised access attempts and actual unauthorised access to protected information systems. NISTIR 7628 requirement SC-7 requires that the utility monitor network traffic at the electronic security perimeter. NISTIR 7628 requirement SI-4 requires monitoring the information system to detect attacks and unauthorised activities. This section of the paper documents an intrusion detection methodology proposed to detect and alert for exploits of vulnerabilities discovered in the cyber security testing process described above. This section also documents an intrusion detection system approach which leverages synchrophasor data to enable detection of attacks against over current protection schemes.

The SNORT intrusion detection and prevention system was used to provide proof of concept rules to the utility to detect and mitigate exploits against vulnerabilities identified in system cyber security reviews and testing.

As previously mentioned the Spirent (formerly Mu) 4000 network analyser was used to target PMU and PDC network interfaces with network congestion or flood attacks on various network layers and services. Flooding attacks can cause a targeted device to reset itself, cause a device network stack to crash, cause applications running on a device to crash, or simply cause a temporary loss of communication with the device. In testing the most common affect of flooding attacks was a temporary loss of communication which was restored after the flooding attack stopped. Figure 6 shows a response chart for a TCP SYN flood directed at a PMU or PDC network interface. The Y-axis shows the normalised rate of flooding. For the flood attack shown in Figure 6 the maximum packet rate is 100,000 packets per second (pps). The X-axis of Figure 6 shows the time stamp during the test. As time increases the flood rate is increased linearly until 100% is reached, when the rate is then linearly decreased back to 0%. Periodically during the test the Spirent (formerly Mu) 4000 injects a packet with known response called an instrumentation packet. The Spirent (formerly Mu) 4000 measures the response time for instrumentation packets throughout the test. Instrumentation packet response times are shown in Figure 6 as blue vertical lines. The red dots along the X-axis indicate that the device under test did not respond to the instrumentation within the timeout period.

Figure 6 TCP SYN flood attack response chart (see online version for colours)

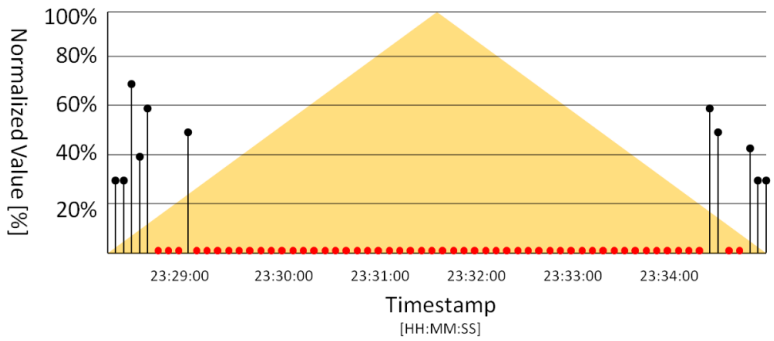
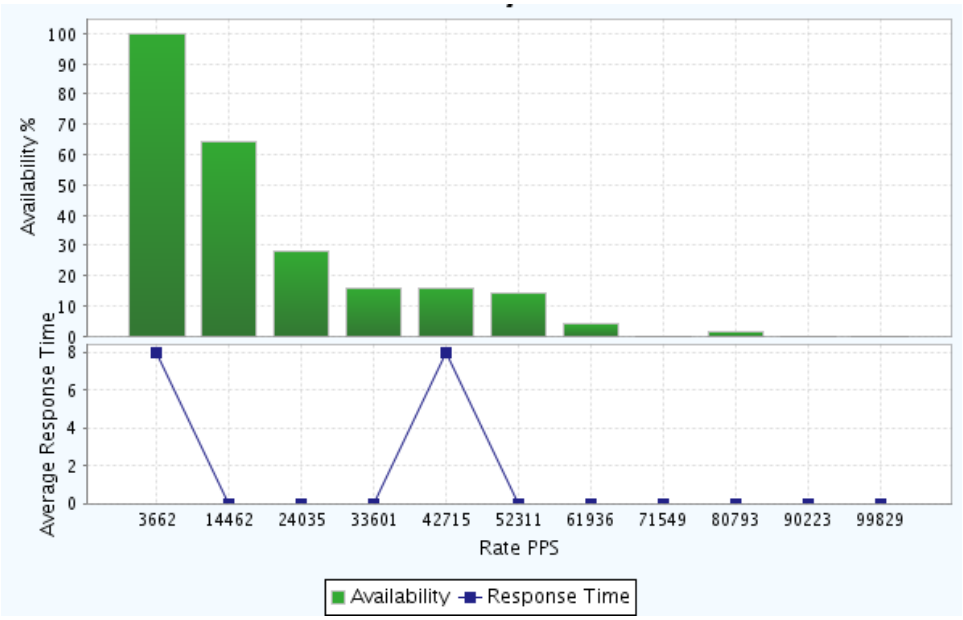


Figure 7 shows an availability chart for the device under test for the TCP SYN flood attack. The Y-axis shows the percent availability, the percentage of time the device was able to respond to instrumentation packets at the packet per second rate shown on the X-axis. From Figure 7 we see that the device is unable to respond as the flood rate increases. The device under test shows less than 50% availability at 24,035 pps and less than 10% 61,936 pps.

Figure 7 TCP SYN flood availability chart (see online version for colours)



SNORT rules are capable of tracking the number of packets from a given source in a specified time period. Such SNORT rules can alert if a flooding attack is detected. A SYN flood rule for an IEEE C37.118 interface should take into account the normal and extraordinary, yet still valid, volumes of traffic expected on the network interface. In normal operation, using IEEE C37.118, the PDC sends commands to the PMU to request a configuration file. The PMU responds with a configuration file and then begins to

stream synchrophasor measurements, data packets, at 30, 60, or 120 packets per second. This process should generate one TCP session and therefore only one TCP SYN packet should be sent per synchrophasor session. A PDC may connect to multiple PMU and therefore may have multiple active TCP sessions on port 4,712, the port assigned for IEEE C37.118. PMU and PDC also commonly have other TCP services. Each open port of the tested PMU and PDC was tested with TCP SYN flood attacks. In all case devices were 100% responsive to TCP SYN floods of less than or equal to 1,000 packets per second. The two rules below detect TCP SYN flood attacks against any port on PMU or PDC. The rules alert for more than 1000 TCP packets in one second. This threshold value can likely be significantly decreased without causing spurious alerts.

```
alert tcp any any -> $PDCIP any (msg:"Syn Flood to PDC";\
flags:S,CE; flow:to_server; threshold: type threshold, track \
by_src, count 1000, seconds 1; priority:3; sid:1000001;)

alert tcp any any -> $PMUIP any (msg:"Syn Flood to PMU";\
flags:S,CE; flow:to_server; threshold: type threshold, track \
by_src, count 1000, seconds 1; priority:3; sid:1000002;)
```

Flooding attacks performed in device testing included ARP floods, IP floods, TCP SYN floods, TCP SYN FIN floods, UDP floods, ICMP floods. In each case SNORT rules can be derived to detect the floods.

Protocol mutation testing was performed with the Spirent (formerly Mu) 4000. Protocol mutation, also known as fuzzing, checks device response to broken protocol rules. Protocol mutation can be performed at any network layer. In this section we provide MODBUS/TCP and IEEE C37.118 protocol mutation examples.

One MODBUS/TCP device tested reset itself when the LENGTH field of was less than the actual length remainder of the MODBUS/TCP packet. The rule below confirms that the specified bytes remaining are actually in the packet. This rule was taken from a rule set developed by Digital Bond (Quick Draw SCADA IDS, http://www.digitalbond.com/tools/quickdraw/).

```
alert tcp $MODBUS_SERVER 502 <> $MODBUS_CLIENT any
(flow:established;\
byte_jump:2,4; isdataat:0,relative; msg:"SCADA_IDS: Modbus TCP -\
Incorrect Packet Length, Possible DOS Attack"; \
reference:url,digitalbond.com/tools/quickdraw/modbus-tcp-rules; \
classtype:non-standard-protocol; sid: 1000003; rev:1;
priority:2;)
```

Because much of this work was done under confidentiality agreement, other SNORT rules written were not included in this paper as they would indirectly divulge the vulnerabilities identified in testing.

6 Future work and conclusions

Synchrophasor systems are an emerging technology. Prior to installation of a synchrophasor system a set of cyber security requirements must be developed, new devices must undergo vulnerability testing, and proper security controls must be designed to protect the synchrophasor system from unauthorised access.

In this paper we described the process used to develop a set of cyber security requirements in the design stage of a synchrophasor project. A set of cyber security rules was derived from review of the NISTIR 7628 Guidelines for Smart Grid Cyber Security, DHS Security Procurement Language for Control Systems, and from utility internal requirements. Resulting rules were listed in the paper. Next, the paper discussed a cyber security vulnerability analysis and testing process. The testing process included network congestion and protocol mutation testing of multiple PMUs and PDCs. The testing section provides limited results due to confidentiality agreements and ethical reporting requirements. The testing section also discussed short comings of the fuzzing tool used and described the need for IEEE C37.118 and MODBUS/TCP fuzzers capable of fuzzing server to client interactions prior client to server packet contents and system state. Next the paper discussed the process of reviewing synchrophasor system components against the drafted cyber security requirements. Each requirement was discussed in the context of the synchrophasor system and recommendations were provided for meeting requirements. Finally, a discussion was offered on writing SNORT intrusion detection rules based upon the results of cyber security testing.

References

Control Systems Security Program (2011) *Catalog of Control Systems Security: Recommendations for Standards Developers*, September, National Cyber Security Division, Department of Homeland Security [online] http://ics-cert.us-cert.gov/sites/default/files/CatalogofRecommendationsVer7.pdf (accessed 21 May 2013).

Department of Homeland Security (DHS), *Cyber Security Procurement Language for Control Systems* [online] http://ics-cert.us-cert.gov/sites/default/files/FINAL-Procurement_Language_Rev4_100809_0.pdf (accessed 21 May 2013).

File Transfer Protocol, RFC 959 [online] http://tools.ietf.org/html/rfc959.

Fink, R., Spencer, D. and Wells, R. (2006) *Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems*, Idaho National Laboratory, Idaho Falls, Idaho, September.

Fovino, I., Masera, M., Guidi, L. and Carpi, G. (2010) 'An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants', in *Human System Interactions (HSI), 2010 3rd Conference on*, pp.679–686.

Idaho National Laboratory (2009) *Wireless Procurement Language in Support of Advanced Metering Infrastructure Security*, Idaho Falls, Idaho, August [online] http://www.inl.gov/scada/publications/d/inl-ext-09-15658_ami_proc_language.pdf (accessed 21 May 2013).

IEEE (2000) *IEEE Guide for Electric Power Substation Physical and Electronic Security*, IEEE Std 1402-2000, doi: 10.1109/IEEESTD.2000.91305.

INL NSTB Programme (2008) *Common Cyber Security Vulnerabilities Observed in Control System Assessments*, Idaho National Laboratory, Idaho Falls, Idaho, November [online] http://www.inl.gov/scada/publications/d/inl_nstb_common_vulnerabilities.pdf (accessed 21 May 2013).

Spirent [online] http://www.spirent.com/ (accessed 21 May 2013).

National Institute of Standards and Technology, Recommended Security Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 3 [online] http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf.

NISTIR 7628, *Guidelines for Smart Grid Cyber Security*, 2010 [online] http://csrc.nist.gov/publications/PubsNISTIRs.html (accessed 21 May 2013).

NMAP Security Scanner [online] http://www.nmap.org.

North American Electric Reliability Corporation, *Critical Infrastructure Protection (CIP) Standards* [online] http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (accessed 21 May 2013).

Open Vulnerability Assessment System (OpenVAS) [online] http://www.openvas.org/.

Quick Draw SCADA IDS [online] http://www.digitalbond.com/tools/quickdraw/.

Skaggs, B., Blackburn, B., Manes, G. and Shenoi, S. (2002) 'Network vulnerability analysis', *Circuits and Systems, MWSCAS-2002, The 2002 45th Midwest Symposium on*, 4–7 August, Vol. 3, pp.III–495.

Stewart, J., Maufer, T., Smith, R., Anderson, C. and Ersonmez, E. (2010) *Synchrophasor Security Practices* [online] https://www.selinc.com/WorkArea/DownloadAsset.aspx?id=8502 (accessed 21 May 2013).

The Syslog Protocol, RFC 5424 [online] http://tools.ietf.org/html/rfc5424.

Wurldtech Security Technologies Inc. [online] http://www.wurldtech.com/.