

Improving Safety of Industrial Control Systems with Security and Robustness Testing

- Reveal Industrial Control Resiliency Issues
- Document SCADA and Process Control Vulnerabilities
- Prevent Occurrence of Zero-Day Attacks and Network Robustness Problems
- Enable 99.999% Continuity of Critical Services

Problem:

Safeguarding Operations of Process and SCADA Control Systems

The industrialized world relies on a broad spectrum of vital critical infrastructure sectors. These sectors include agriculture and food, water, public health, emergency services, defense industrial base, telecommunications, energy, transportation, banking and finance, chemical, postal and shipping, and key physical assets such as nuclear power plants, dams, government facilities and commercial assets. In addition to physical safety and security, network security for critical infrastructure is crucial because of reliance on electronic systems for operational control. Malfunctions to the industrial control systems in these industries, including faults within programmable logic controllers (PLCs), distributed control systems (DCS), remote terminal units (RTUs) and supervisory control and data acquisition (SCADA) systems can cause safety issues including weakened national security, business and social disruption, physical injury or death, and environmental damage, and damage to the reputation of the business, possibly resulting in a desire for increased regulation.

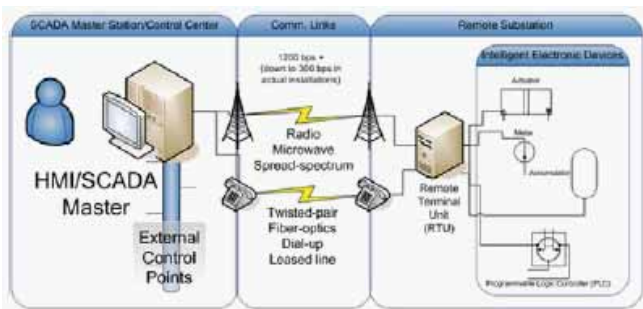


Figure-1: Robustness and safety testing is crucial for IP protocols like DNP3, which controls intra-SCADA communications in process control systems.

Source: <http://www.en.wikipedia.org/wiki/DNP3>

The U.S. Government Accountability Office (GAO) has described a dramatic new escalation in risks to control systems, citing four areas of concern: (1) adoption of standardized technologies with known vulnerabilities, (2) control networks being connected to other networks, (3) having insecure connections, which exacerbate vulnerabilities, and (4) having information about infrastructures and control systems be easily available to the public. Ignoring or improperly addressing industrial control system security or robustness risks can result in disruption of critical systems, damage to equipment, and may cause unpredictable operations or failure of critical infrastructure (see GAO specifics at <http://www.gao.gov/cgi-bin/getrpt?GAO-04-354>).

Simply adding existing IP-based security controls such as firewalls, intrusion detection/prevention, antivirus, encryption, authentication, and other related technologies to control systems will not always ensure plant safety or security. Historically, these technologies are not built into industrial controllers because the systems were considered “closed” and did not use open networking technologies nor were they accessible from the public Internet.

Today, the widespread adoption of Ethernet and TCP/IP technologies in industry has exposed these devices to new threats but not new solutions. For example, adding a layer of security technology to older control systems may trigger operational glitches (e.g., due to increased latency).

Processing requirements for security can exceed close timing tolerances of control systems and cause latency-related delays or even shut down operations. Consequently, manually adding security to Process and SCADA control systems plus IP security testing requires substantial engineering, QA and validation efforts. Security and robustness testing are critical parts of ensuring safety for process control systems because insecurity of the building-block protocols directly impacts operational safety of the attached process system.

Solution:

Mu Security Enables Safer and More Resilient Process Control

Owners and operators of Industrial Control systems now have a new tool for testing and analysis that isolates and documents safety concerns – including protocol implementation weaknesses in any IP-based control system. The protocol testing and measurement systems from Mu Security analyze robustness by enabling, using, and routinely stressing control system resiliency and security as part of a safety process of continuous improvement. The Mu-4000 Security Analyzer automates risk quantification according to the “attack surface” for products or services. The attack surface concept was developed by Microsoft and Carnegie Mellon University and expresses exposure of that product or service to robustness issues including malicious attack. Attack surfaces of DCS, RTUs and PLCs are becoming increasingly complex with the addition of both more complex control protocols (like MODBUS/TCP and EthernNet/IP) and traditional IT protocols like HTTP, NTP, SNMP and FTP to many systems. Also, since control systems are no longer isolated islands of proprietary Industrial Control protocols, software bugs now may expand into exploitable vulnerabilities since they are exposed to an open IP network. Mu Security provides the only system offering comprehensive safety baseline analysis of the total attack surface of a control system within the context of a methodical process of identifying security and

system availability issues for any protocol vital to Industrial Control operations.

For example, the Distributed Network Protocol (DNP3) defines communications procedures for components of process automation and control systems. The DNP was originally designed for a closed network environments so implementations do not expect to receive improperly formatted frames found in IP based networks (DNP3 refers to the case in which DNP's layer-2 frames are transmitted over TCP/IP). Mutations analyzed and measured by the Mu-4000 Security Analyzer system ensure that DNP3 implementations are able to tolerate any kind of abuse that might be encountered as the DNP frames are transported over intervening IP-based networks (packet loss, duplication, corruption, reordering, etc.), as well as proving that an implementation can handle incorrectly formatted DNP frames from less compliant implementations.

SCADA systems also use Inter-Control Center Communications Protocol (ICCP/TASE.2), another potential source of security vulnerabilities. ICCP/TASE 2 facilitates communications between multiple SCADA control centers. Vulnerabilities include ASN.1 attacks, exploits against the stateful nature of ICCP, and possible issues related to the use of SSL-TLS. Testing by the Mu-4000 automatically locates and documents these vulnerabilities in networking products and control system implementations to expedite vendor remediation, or to provide information to the plant management about weaknesses so that other protection can be employed (in cases where it is infeasible to update or patch a faulty controller).

Benefits:

Ensuring Safety in Industrial Control, 99.999% Service Uptime

Operators of Industrial Control systems share a common goal of safely ensuring secure Process and SCADA control systems to preserve service uptime without unscheduled interruptions. Operators face a particular challenge of providing resilient, robust and secure process control implementations for increasingly complex and older process control systems that lack the processing capability for improved security (either added explicit security protocols or more robust exception handling). Converged IP-based network products for voice and video on the same, shared IP network adds to the complexities of securing control systems for critical infrastructure and requirement of using Security Analyzers.

Operator users previously had limited visibility into the true product or network attack surface, security, safety or robustness metrics of IP-based products they used in a control system. The Mu-4000 Security Analyzer provides an unbiased benchmark for customized measurement of any product's security readiness, robustness, and resiliency before production purchase, deployment or upgrade. Operators use this assessment capability to hold vendors accountable for unsafe, insecure or non-robust products. The analyzer allows operators to proactively document the extent of a product's safety shortcomings including the use of existing test scripts, and to take preventive measures including the validation of signatures for security products, or the deployment of remediation devices such as firewalls or IPS that are able to block exploitation of the discovered protocol implementation flaws.

Operators of critical infrastructure now use the Mu-4000 for:

- **Product Selection:** Security and safety readiness is a key metric to support purchase decisions or upgrades, in addition to robustness, functionality, price and performance.

- **Product Deployment:** Securely deploy product features or introduce configuration changes into the network architecture, which provides the ability to proactively identify and remove robustness issues or vulnerabilities before deployment.
- **Change Control:** Analyze new software or firmware releases or bug fixes before production use, and ensure that no published or previously eliminated safety issues or vulnerabilities are inadvertently used in the network.
- **Threat Assessment:** Security crisis management and problem reporting to a vendor is streamlined with Mu Security's ability to automate and "operationalize" the auditing and vulnerability remediation processes.

Vendors of PLCs, DCS, SCADA and other IP-based software or hardware products for managing Industrial Control systems receive actionable feedback from operator users via documentation of specific weaknesses in their products. Detailed reporting, packet captures and Linux-executables from the Mu-4000 tell developers and vendors which issues are "hot" and enable the vendor to quickly isolate the root cause of the issue. Internally, product vendors use this actionable suite of remediation tools to repair vulnerabilities, chart robustness or resiliency weak spots, tailor signature development or as input to patch/update development.

Development teams and vendors are using Mu-4000 for:

- **Design and Development:** Used by QA and development teams to repair security flaws as early as possible in the development process, with measurable reduction in staffing and support costs.
- **Testing and Customer Problem Resolution:** Safety issues are isolated and information captured by the Mu-4000 Security Analyzer bring quick focus to remediating customer-reported problems - with greatly reduced difficulty to reproduce each issue.
- **Product Upgrades:** Assessment of configuration changes, software upgrades and patches ensure that security regressions or robustness issues like memory leaks or CPU utilization spikes are not inadvertently introduced.
- **Threat Assessment:** Every network has unique settings but vendors focus their testing on the most common configurations. Mutation analysis with published vulnerability analysis provides unprecedented threat assessment coverage.

Industrial Control Protocols Tested by Mu-4000 Security Analyzer

ARP	BOOTP	CDP	DHCP	DNP
GRE	HTTP	ICMPv4	IGMP	IPsec
IPv4	L2TP	LLDP/LLDP-MED ¹	Modbus	MMS
MPLS	PPPoE	SNMP	SSL-TLS	TACACS+
TCP	Telnet	UDP		

¹ LLDP is defined in IEEE 802.1AB-2005; LLDP-MED is defined in ANSI-TIA-1057-2006.

Robustness Testing Ensures Service Security of Critical Infrastructure

The Mu-4000 Security Analyzer offers operators of Industrial Control systems a customizable system for maximizing operational safety and efficiency over IP networks. It helps achieve 99.999% uptime, reduces time spent on product safety workarounds or costly security breaches by averting successful exploits of IP-related vulnerabilities, and limits problems caused by non-robust implementations of the protocols. The Mu-4000 helps both operator users and their product vendor suppliers with the identification and timely repair of safety, robustness and vulnerability issues. Cost-effective and wide-ranging test suites allow the Mu-4000 to address all major protocols affecting critical infrastructure. Security Analyzers are an essential and easy-to-deploy way to benchmark system safety and enable security as a process of continuous improvement.



web: www.musecurity.com | email: info@musecurity.com
address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA
phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317