

# IEC 61850

## Communications Networks and Systems in Substations

- Specifies Unified Schema for Organizing Data in Heterogeneous Power System Devices
- Enables Integrated Automation of Power Systems in Substations
- Mu-4000 Identifies Vulnerabilities in IEC 61850 Implementations

### Where is IEC 61850 Used?

The Communications Networks and Systems in Substations protocol (IEC 61850) enables a new networking approach for power system automation in substations. Traditional communications were geared around slow transmission speeds, which constrained the rate of data flow and forced operators to configure and operate power systems on an expensive, mostly manual basis. IEC 61850 was designed for higher-speed networks that can carry more data. More capacity and speed enables automated control actions that are initiated by computers in the substation rather than by a human at a distant central site. The protocol specifies how power system devices should organize data in a consistent way for all types and brands of devices, and related services.

The abstraction of data items/objects and services provided by IEC 61850 are independent of underlying protocols. This abstract data model is mapped to a specific protocol stack based on MMS (ISO/IEC 9506), TCP/IP and Ethernet.

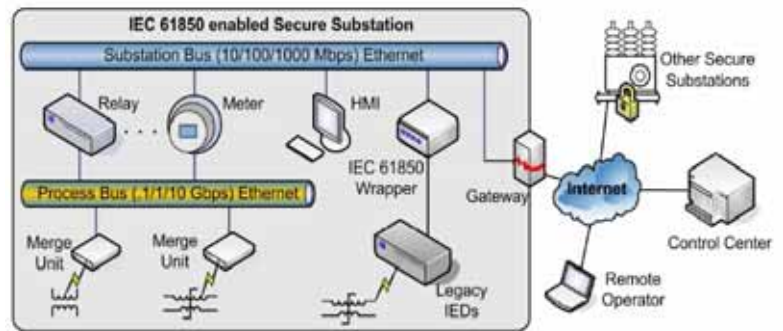


Figure-1: IEC 61850 SUBSTATION ARCHITECTURE  
Source: <http://seclab.uiuc.edu/docs/iec61850-intro.pdf>

### Mu-4000 Identifies IEC 61850 Vulnerabilities

The safety of industrial control devices using the Internet for communications is a serious issue given the vast number of potential vulnerabilities in applications that incorrectly implement standard protocols. IEC 61850 is a relatively new protocol so implementers and operators of critical infrastructure may get a false sense of security by relying only on firewalls, intrusion detection/prevention, and other perimeter security solutions. The key vulnerability of IEC 61850 is that to be functional, it must use a communications platform for industrial intelligent electronic devices (IEDs) and servers. The protocol maps to MMS for transport over OSI or TCP/IP protocols, so IEC 61850 implementations are exposed to a large potential cast of vulnerabilities.

	ACSI Core Services	SMV	GOOSE
Application	MMS (ISO/IEC 9506)		
Presentation	ISO Presentation (ISO 9576) ASN.1 (ISO/IEC 8824/8825)		
Session	ISO Session (ISO 8327)		
Transport	ISO Transport (ISO/IEC 8073) Transport Class 0		
	RFC 1006		
Network	TCP (RFC 793)		
	IP (RFC 791) ARP (RFC 826)		
Data Link	Logical Link Control (ISO 8802), 802-3 Ethertype Media Access Control (ISO 8803)		

Figure-2: IEC 61850 PROTOCOL STACK  
Source: <http://seclab.uiuc.edu/docs/iec61850-intro.pdf>

From a communications perspective, industrial IEDs are relatively brittle and may easily become confused by conflicting (i.e., not perfectly interoperable) 61850/MMS implementations. The Mu-4000 provides dozens of attack suites and mutations that negatively test IEC 61850 implementations over MMS for vulnerabilities that could place critical infrastructure in hazardous, even life-threatening situations caused by failures of the protocol implementations. The lack of robustness and security for these protocols could compromise safety mechanisms that depend on the proper functioning of the IEC 61850 control networks.

### IEC 61850 Primer

A power substation's communications network is crucial for transmitting data to and from microprocessor-based controllers of sensors managing power generation, control and distribution equipment. A substation control system uses the network to issue commands to IEDs to maintain the desired status of a power grid.

Work on next-generation communications architecture for power substations began in the 1960s and culminated in IEC 61850 (published in 2005), which is a high level description of substation automation. Essentially, IEC 61850 helps power substations migrate from the analog to digital world. It standardizes data names for logical devices containing logical nodes for automatic control, metering and measurement, supervisory control, generic functions, interfacing/archiving, protection, sensors, instrument transformers, switchgear, power transformers and other equipment. IEC 61850 also creates a comprehensive set of services for logical devices and nodes, implements them within standard protocols and hardware, and defines a process bus. The protocol's stack (see Figure-2) maps to many other standard protocols, including MMS, ASN.1, TCP, IP and others, so IEC 61850 objects and services are strongly dependent on proper implementations of associated and underlying protocols.

### Potential Weaknesses of IEC 61850

Since this protocol is relatively new, its requirements are subject to interpretation so implementation quality will vary and they may not interoperate perfectly. The industry hopes the commonality of implementations will improve over the next few years. But without a systematic and thorough search process, there is no proactive way to find implementation flaws that may cause system downtime, substation outages or reduced safety. The ad-hoc discovery of such vulnerabilities is impractical because there is a significant diversity of configurations in which an IEC 61850 implementation may be operating, so there are many more hiding places for robustness issues. Also the danger of failures (to safety, to the power grid) is too great for a "seat of the pants" approach.

### POTENTIAL IEC 61850 WEAK SPOTS

By depending on MMS, IEC 61850 inherits many negotiation techniques and commands with expected responses, which makes implementation complex and prone to error.
The stateful protocol is vulnerable to out-of-order, unexpected or incorrectly formatted packets.
Relies on Abstract Syntax Notation (ASN.1) structures that are difficult to implement correctly, thus are easy to abuse and exploit.

### BENEFITS OF MU-4000

The Mu-4000 statefully attacks MMS across multiple message types.
Extensive mutation library sends valid protocol packets out of order and in the wrong state to uncover implementation flaws that lead to crashes or reduced performance.
Sends unexpected legal and malformed ASN.1 structures that implementers did not anticipate to uncover implementation flaws that manifest as crashes or performance degradation.

Table-1.

The IEC 61850 virtual LAN high-speed profiles employ three protocols that are transmitted using non-routable multicast datagrams. Message transmission must occur within four milliseconds so the protocol prohibits use of full encryption. Improperly implemented security protocols may introduce latency on machines in a substation and interfere with transmission of multicast datagrams. Authentication is the only security measure included in the protocol.

A significant weakness for IEC 61850 is that it maps to MMS as the communications platform, which itself has a wide range of potential vulnerabilities that might plague implementations depending on the configuration and network environment. With improper implementation, stateful violations or attacks, including out-of-order or unexpected packets, could easily bring down IEDs that depend on MMS. MMS also uses binary data structures encoded using Abstract Syntax Notation number one (ASN.1) that is well-known to be difficult to implement correctly.

### About the Mu-4000 Analyzer

The Mu-4000 analyzer is a security analysis platform that delivers the industry's first systematic and repeatable process to identify unknown and published vulnerabilities in any IP-based system, application or network device without requiring access to source code. The process, known as "mutate, monitor and manage," easily integrates with existing security controls. The Mu-4000 subjects the target under analysis to a virtually unlimited number of attack vectors (the "mutations"). It monitors the target and captures results in a database while managing the process in a reproducible and actionable manner. Results include detailed reports and utilities to speed fault remediation. This lifecycle approach enables the creation of security-enabled processes in all phases of product development and deployment. The extensible security analysis platform also enables organizations to integrate their own suites of attacks. The Mu-4000 analyzer is a self-contained, 2U rack-mountable appliance that is easily configured, operated and managed.

### OTHER PROTOCOLS SUPPORTED BY THE MU-4000 (partial list)

ARP	IPv6	SNMP
BGP4	ISAKMP	SNMP Traps
CDP	LDAP	SSL-TLS
DHCP	MGCP	SSDP
DNP	MODBUS	SSH
FTP	PIM-DM	Sun RPC
HTTP	PIM-SM	TCP
ICMP	POP3	TFTP
IGMP	RADIUS	TLSv1
IMAP	RTSP	UDP
IPv4	SIP	

Table-2.



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