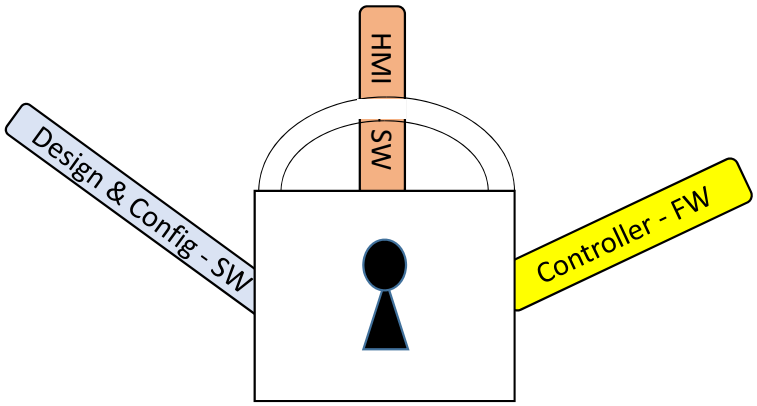
LA-UR-14-24320
Approved for public release; distribution is unlimited.

Title:	Control Systems - Software/Firmware Security
Author(s):	Frost, Sandra L.
Intended for:	DOE Control System Security, 2014-06-12 (Los Alamos, New Mexico, United States)
Issued:	2015-02-25 (rev.1)

Control Systems - Software/Firmware Security

Sandy Frost/LANL



LA-UR-14-24320

Outline

- Motivation
- Standards
- Vendors
- LANL
- Next Steps

ICS-CERT 2013 Vulnerabilities

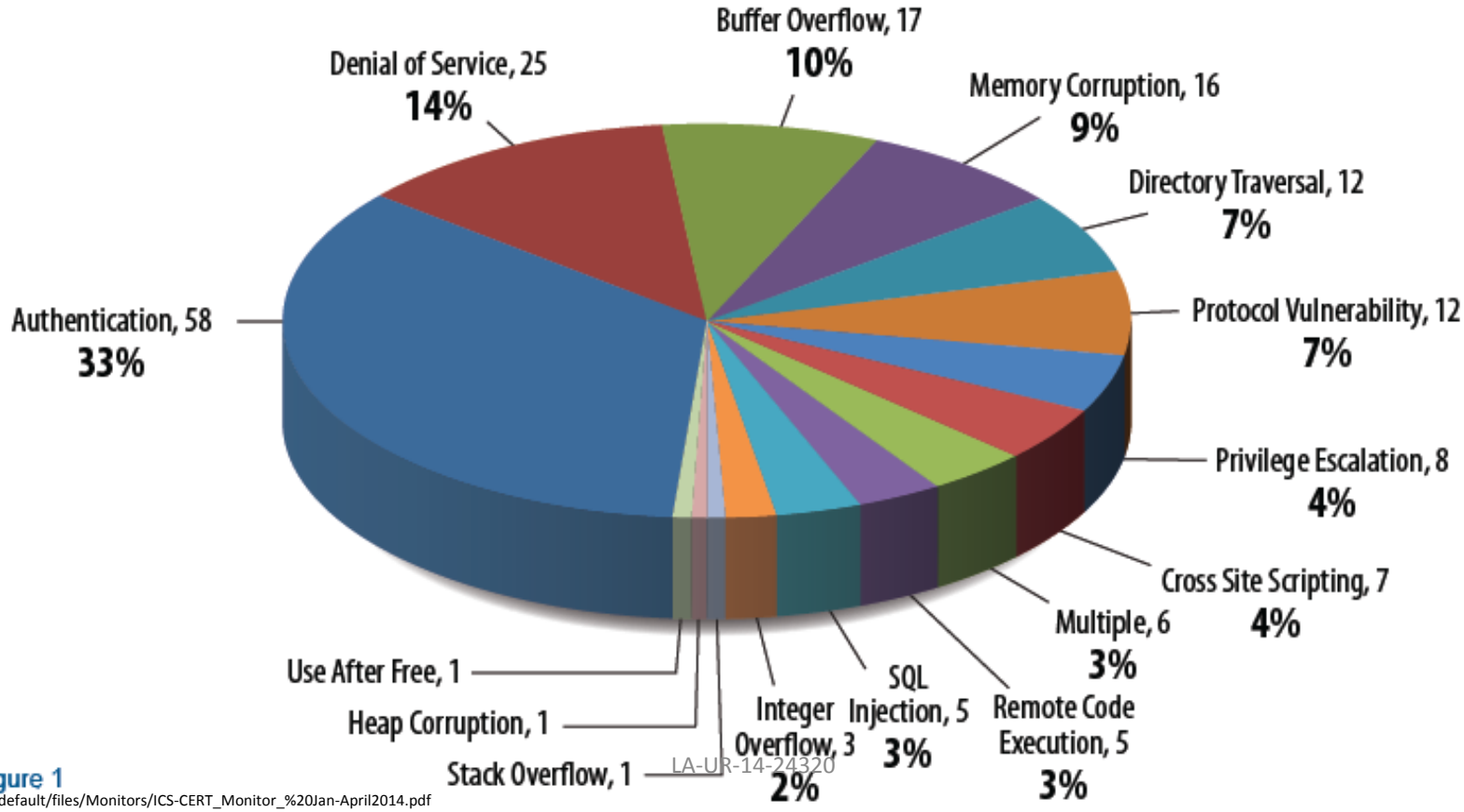


Figure 1

http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf

ICS-CERT 2013 Vulnerabilities

- Total: 181 vulnerabilities
- 87% - remotely exploitable

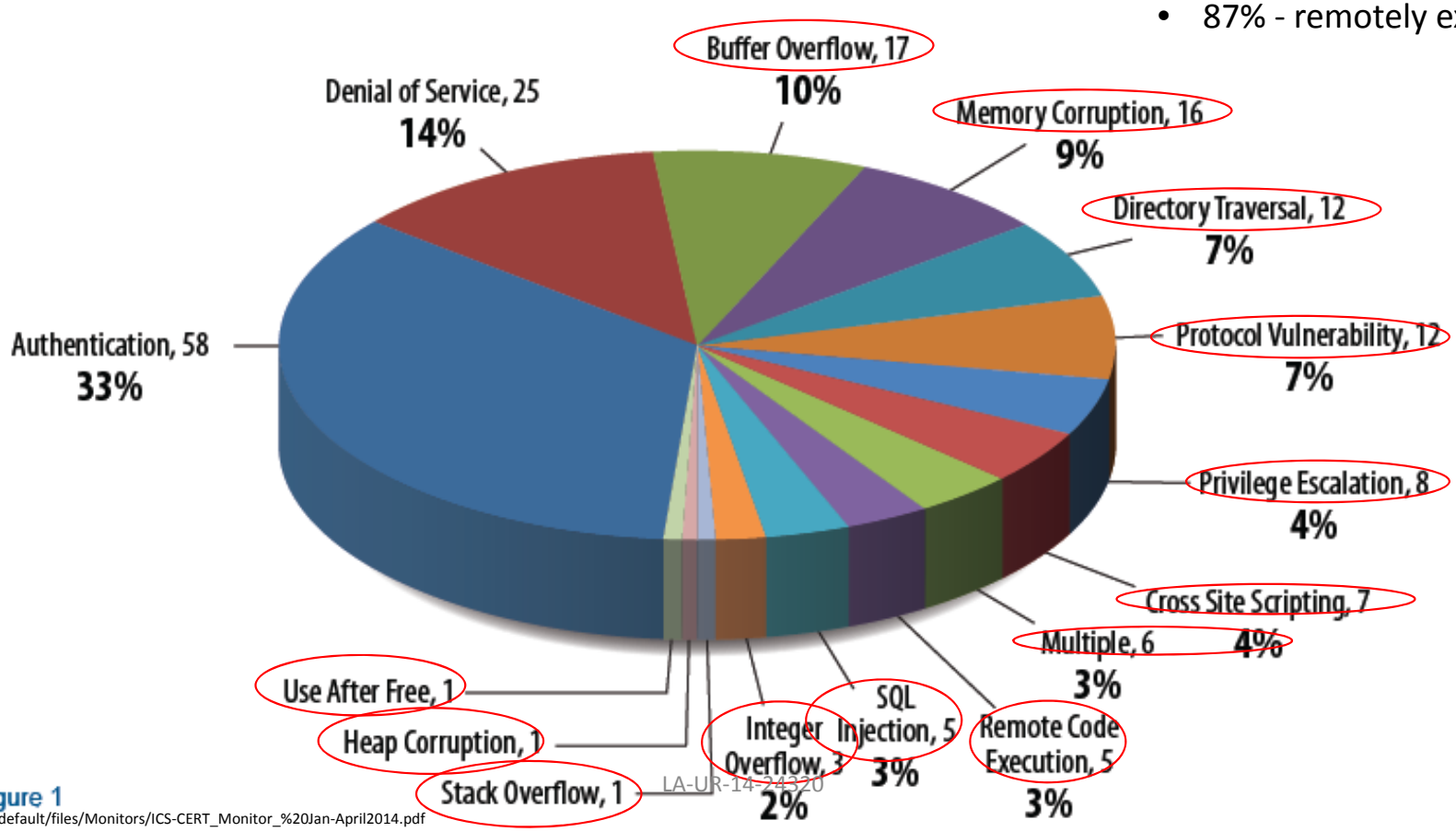


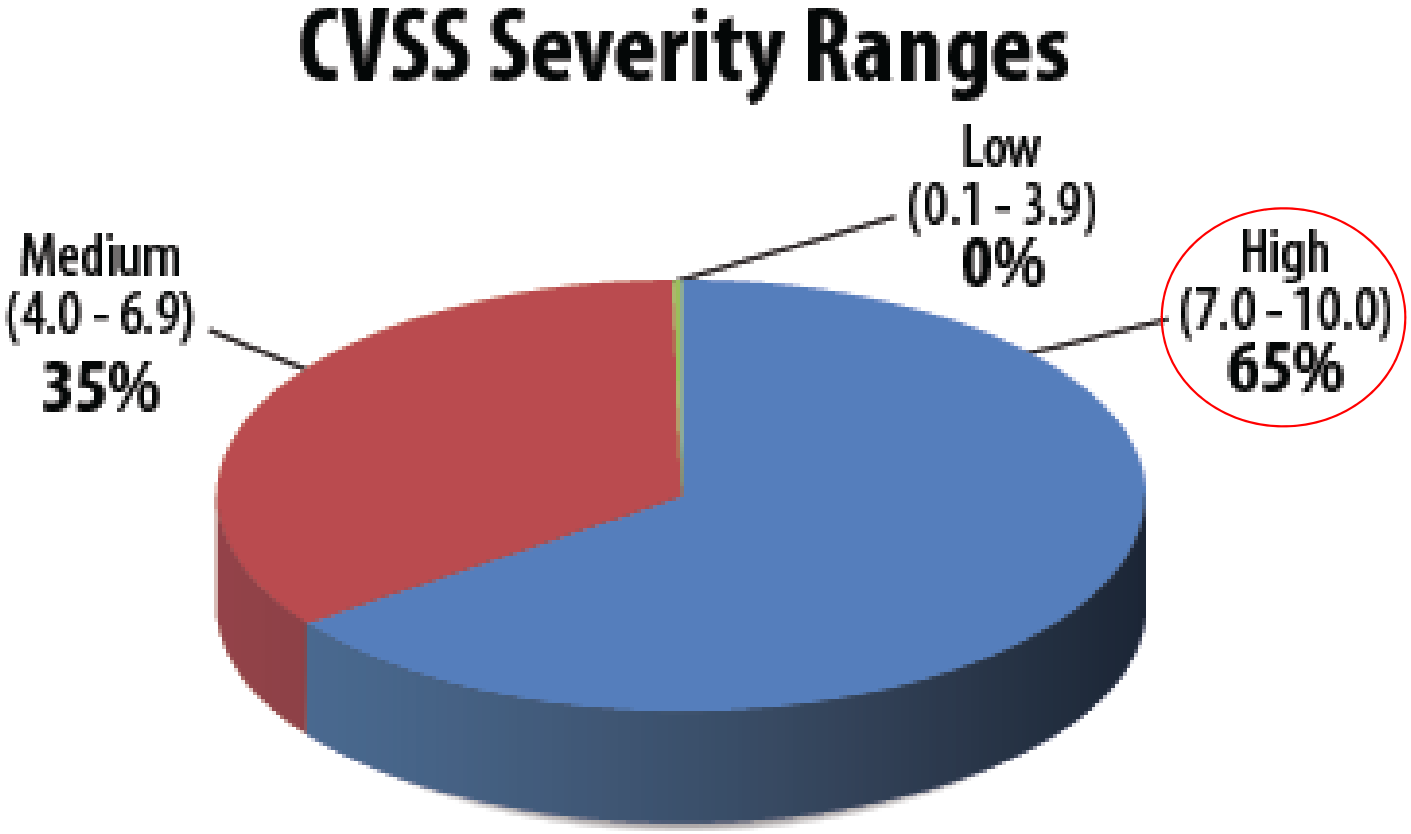
Figure 1

http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf

RECAP OF VUNERABILITIES IN 2013

As previously reported in the 2013 Year in Review, ICS-CERT received 181 vulnerability reports from researchers and ICS vendors throughout the year. Of those, 177 were determined to be true vulnerabilities that involved coordination, testing, and analysis across 52 vendors. The majority of these or 87 percent were exploitable remotely while the other 13 percent required local access to exploit the vulnerabilities. A fundamental recommendation for mitigating remotely exploitable vulnerabilities is to minimize network exposure and configure ICSs behind firewalls so they aren't directly accessible and exploitable from the Internet. Equally important is patching and updating ICS devices as soon as practically possible, understanding that patches and upgrades must be properly tested by each asset owner/operator before being implemented in operational environments. The following chart depicts the different types of vulnerabilities reported and coordinated in 2013.

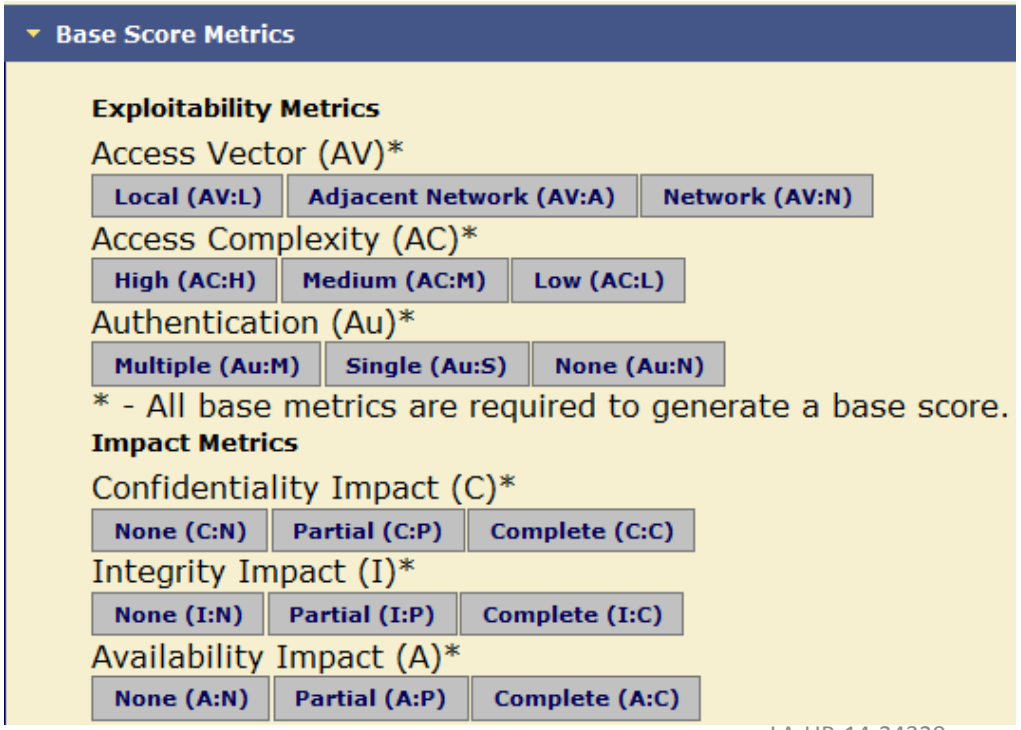
http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf



http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf

What is CVSS (Common Vulnerability Scoring System)?

- Vulnerability scoring system to rate IT vulnerabilities



Example:
CVSS base score of 10.0:
AV:N/AC:L/Au:N/C:C/I:C/A:C

AV:N
- Access Vector = Network

AC:L
- Access Complexity = Low

Au:N
- Authentication = None

C:C
- Confidentiality Impact = Complete

I:C
- Integrity Impact = Complete

A:C
- Availability Impact = Complete

http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2

https://ics-cert.us-cert.gov/alerts

https://ics-cert.us-cert.gov/alerts

ICS-CERT Alerts - 2014

ICS-ALERT/ <Follow up>	CVSS v2 Base Score	CVE	Name	Vulnerability Type	Remotely Exploitable	Impact
14-155-01A			Daktronics Vanguard Default Credentials (Update A)	Default credentials	Yes	Modification of sign text
14-99-01E	6.4	AV:N/AC:L/Au:N/C:P/I:P/A:N	Situational Awareness Alert for OpenSSL Vulnerability (Update E)	Heartbleed SSL key exposure Input data not properly validated	Yes	Private/encrypted information exposure
14-015-01 14-016-01	7.8	AV:N/AC:L:Au:N/C:N/I:N/A:C	Ecava IntegraXor Buffer Overflow Vulnerability	Buffer Overflow	Yes	DoS

https://ics-cert.us-cert.gov/alerts

ICS-CERT Alerts - 2013

ICS-ALERT/ <Follow up>	CVSS v2 Base Score	CVE	Name/ <Product>	Vulnerability Type	Remotely Exploitable	Impact
13-304-01			Nordex NC2 – Cross-Site Scripting Vulnerability	XSS	Yes	Possible Remote Code Execution
13-259-01 14-051-02	9.3	AV:N/AC:M/Au:N/ C:C/I:C/A:C	Mitsubishi Electric Automation MC-WorX Suite Unsecure ActiveX Control	Insecure ActiveX control	Yes	Possible Remote Code Execution
13-256-01 ICSA-13-295-01	5.8	AV:N/AC:M/Au:N/ C:N/I:P/A:P	WellinTech KingView ActiveX Vulnerabilities	ActiveX, KChartXY	Yes	Overwrite arbitrary files
				Traverse outside of restricted path		
				ActiveX, SuperGrid	Yes	Overwrite arbitrary files, establish persistence on computer
13-164-01			Medical Devices Hard-Coded Passwords	Hard-coded password	Yes, device dependent	Critical settings/device firmware modification
13-091-01 ICSA-13-140-01	9.3	AV:n/AC:M/Au:N/ C:C/I:C/A:C	Mitsubishi Electric Automation MX Buffer Overflow Vulnerability	Buffer Overflow	Yes	Possible Remote Code Execution
13-091-02			Clorius Controls ICS SCADA Information Disclosure	Information Disclosure	Yes	Loss of Confidentiality
13-016-01A ICSA-13-077-01B	10.0	AV:N/AC:L/Au:N/ C:C/I:C/A:C	Schneider Electric Product Vulnerabilities (Update A)/ BMX NOE 0110	Unauthenticated SOAP/HTTP interface	Yes	Remote code execution
			Modicon M340	TCP connection resource exhaustion	Yes	DoS
			Magelis XBT	HMI 6001/TCP hard coded credentials	Yes	Loss of integrity
	8.5	AV:N/AC:M/Au:S/ C:C/I:C/A:C	Modicon M340	XSF	Yes	Unauthorized access
13-016-02			Offline Brute-Force Password Tool Targeting Siemens S7	Exploit Tool: Credentials Brute Force Credentials Brute Force		Possible capture of current credentials for device
13-009-01 ICSA-13-225-01	6.3	AV:N/AC:M/Au:S/ C:N/I:C/A:N	Advantech WebAccess Cross-Site Scripting	XSS	Yes	Execute unauthorized code; bypass protection mechanisms; read application data
13-004-01/ ICSA-13-067-01	7.8	AV:N/AC:L/Au:N/ C:C/I:N/A:N	Advantech Studio DirectPR Traversal	Directory Traversal	Yes	Data Leakage

Metasploit for HMI – SCADA Modules

Exploit	Module Name	Disclosed	Reference - CVE	Reference - ICS	Target	Platform	Remote Access	Enumerator	DOS	Buffer Overflow	Integer Overflow
SCADA 3S CoDeSys Gateway Server Directory Traversal	codesys_gateway_server_traversal	2-Feb-13	CVE-2012-4705	ICSA-13-050-01-a	Windows Universal S3 CoDeSyS < 2.3.9.27	Windows	1				
Modbus Unit ID and Station ID Enumerator	modbus_findunitid	28-Oct-12						1	1		
7-Technologies IGSS 9 IGSSdataServer.exe DoS	igss9_dataserver	20-Dec-11	CVE-2011-4050	ICSA-11-335-01					1		
SCADA 3S CoDeSys CmpWebServer Stack Buffer Overflow	codesys_web_server	2-Dec-11	CVE-2011-5007	ICS-ALERT-11-336-01	CoDeSys	Windows				1	
Modbus Version Scanner	modbusdetect	1-Nov-11									
TeeChart Professional ActiveX Control Trusted Integer Dereference	exploit/windows/browser/teechart_pro	11-Aug-11			Windows XP, 7	Windows					1
DATAC RealWin SCADA Server 2 On_FC_CONNECT_FCS_a_FILE Buffer Overflow	realwin_on_fc_binfile_a	21-Mar-11	CVE-2011-1563	ICSA-11-110-01	Universal	Windows				1	
RealWin SCADA Server DATAC Login Buffer Overflow	realwin_on_fcs_login	21-Mar-11	CVE-2011-1563	ICSA-11-110-01	Universal	Windows				1	
Interactive Graphical SCADA System Remote Command Injection	igss_exec_17	21-Mar-11	CVE-2011-1566		Windows	Windows	1				
DATAC RealWin SCADA Server SCPC_TXTEVENT Buffer Overflow	realwin_scpc_txtevent	18-Nov-10	CVE-2010-4142		Universal	Windows				1	
DATAC RealWin SCADA Server SCPC_INITIALIZE_RF Buffer Overflow	realwin_scpc_initialize_rf	15-Oct-10	CVE-2010-4142	ICSA-10-313-01	Universal	Windows				1	
DATAC RealWin SCADA Server SCPC_INITIALIZE Buffer Overflow	realwin_scpc_initialize	15-Oct-10	CVE-2010-4142	ICSA-10-313-01	Universal	Windows				1	
BACnet OPC Client Buffer Overflow	bacnet_csv	16-Sep-10		ICSA-10-264-01.pdf	Windows XP, 2K	Windows				1	
DATAC RealWin SCADA Server Buffer Overflow	realwin	26-Sep-08	CVE-2008-4322		Universal	Windows				1	
CitectSCADA/CitectFacilities ODBC Buffer Overflow	citect_scada_odbc	11-Jun-08	CVE-2008-2639		Citect32 CiExceptionMailer.dll, Debug	Windows				1	

http://www.rapid7.com/db/modules/, 10/18/2010

Metasploit for PLC – Privately Developed

- General Electric D20
  - D20tftpbd – D20ME asynchronous command line
    - No authentication
  - D20pass – D20ME credential recovery
    - No authentication, retrieves/displays account usernames/passwords from device configuration
  - D20_tftp_overflow – D20ME TFTP server buffer overflow DoS
    - Buffer overflow causes DoS
- Koyo/DirectLOGIC ECOM
  - Koyo_login- PLC password brute force
    - Reconnaissance, modify ladder logic to affect process integrity/availability
- Rockwell Automation ControlLogix
  - Multi_cip_command – EtherNet/IP CIP commands
    - No authentication
    - Insecure protocol allows "stop CPU" command, reboot controller, crash PLC CPU/Ethernet Controller etc. affect process integrity/availability
- Schneider Electric Modicon Quantum
  - Modicon_command – remote start/stop command
    - No authentication
  - Modicon_password_recovery – password recovery
    - Hard coded backdoor account allows retrieval of account information
  - Modicon_stux_transfer
    - No authentication, send/receive PLC ladder logic

Metasploit Exploit Module Released For PLC SCADA Devices

Digital Bond and Rapid7 partner to move additional Project Basecamp PLC exploits to the Metasploit Framework

http://www.digitalbond.com/tools/basecamp/metasploit-modules/
http://www.darkreading.com/metasploit-exploit-module-released-for-plc-scada-devices/d/d-id/1136949?

Common Cybersecurity Vulnerabilities in Industrial Control Systems

May 2011

Homeland Security

Control Systems Security Program

National Cyber Security Division

http://ics-cert.us-cert.gov/sites/default/files/documents/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf, previous 2009 version (2004-8)

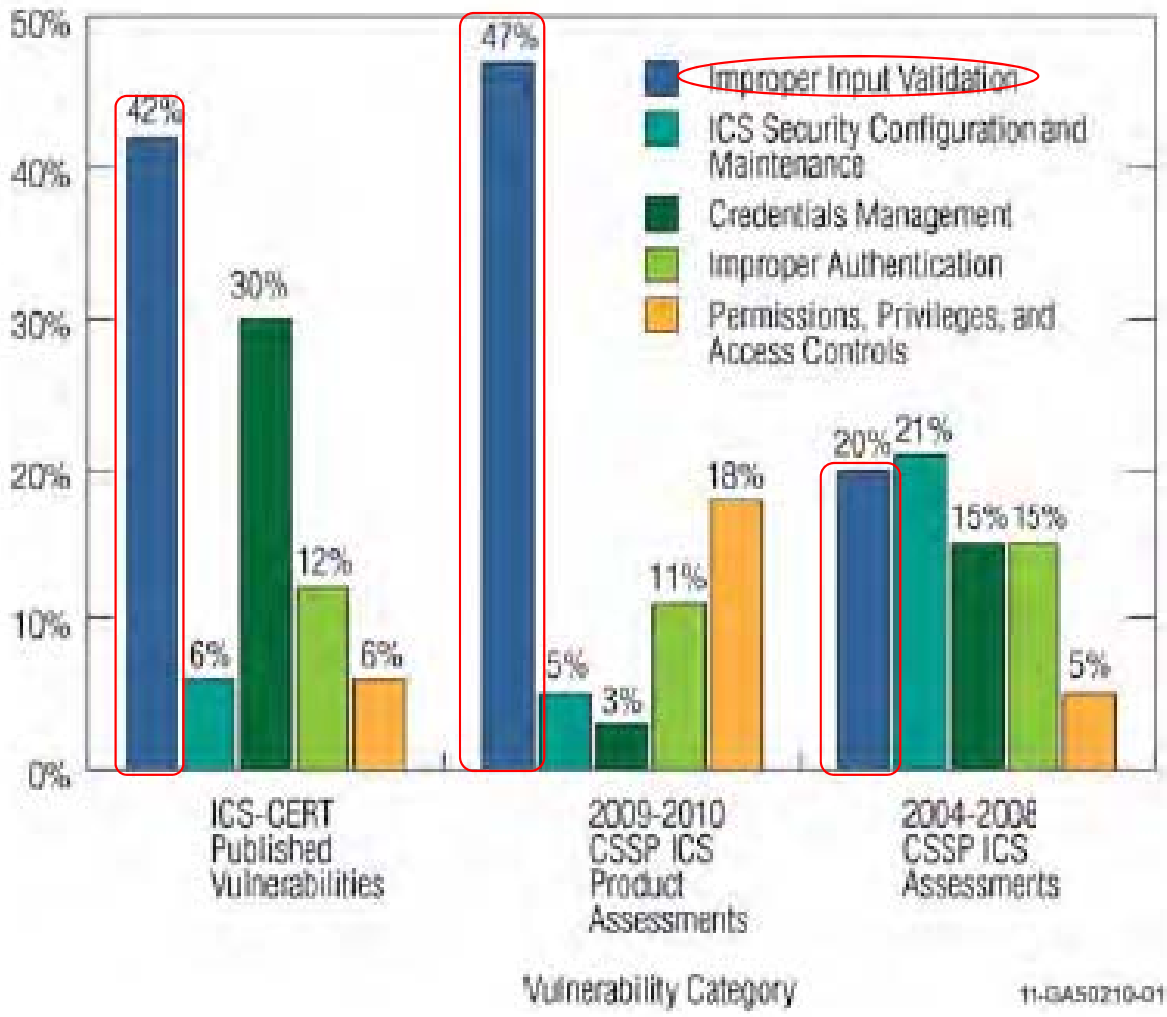
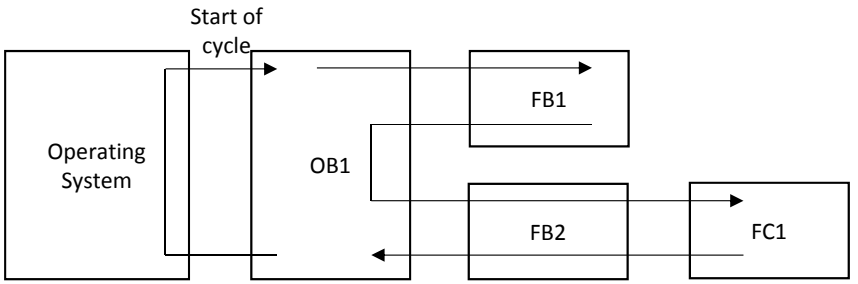


Figure EX-1. Comparison of ICS software security weaknesses.

http://ics-cert.us-cert.gov/sites/default/files/documents/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

Stuxnet – PLC Data Types



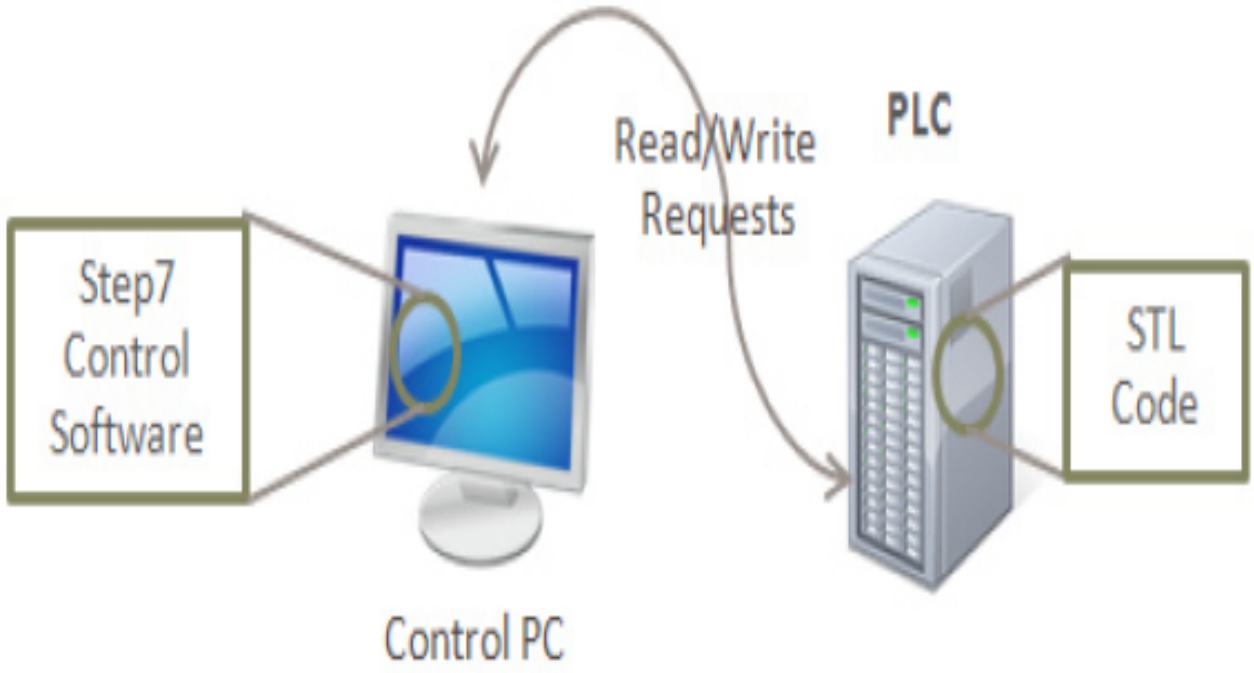
- Data Blocks (DB)
  - Contain program-specific data (e.g. numbers, structures)
- System Data Blocks (SDB)
  - PLC configuration information
  - Created depending on the number/type of hardware modules connected to the PLCs
- Organization Blocks (OB)
  - A type of program block in a Siemens PLC that interfaces the PLC operating system to the user program. Stuxnet examples:
    - OB1 – entry-point of the PLC program. It's executed cyclically without specific time requirements
    - OB35 – standard watchdog OB, executed every 100ms
- Function Blocks (FB)
  - Standard code blocks
  - Contain code that is executed by the PLC
- Functions (FC)
  - Contain program routines for frequently used functions

```
FUNCTION_BLOCK FB20
VAR_INPUT
ENDVAL:              INT;
END_VAR
VAR_IN_OUT
IQ1 :          REAL;
END_VAR
VAR
INDEX:               INT;
END_VAR

BEGIN
CONTROL:=FALSE;
FOR INDEX:= 1 TO ENDVALUE DO
    IQ1:= IQ1 * 2;
    IF IQ1 >10000 THEN
            CONTROL = TRUE
    END_IF
END_FOR;
END_FUNCTION_BLOCK
```

http://www.infoplc.net/files/descargas/siemens/infoplc_net_sitrain_12_obs.pdf,
http://www.automation.siemens.com/doconweb/pdf/SINUMERIK_SINAMICS_02_2012_E/S7P.pdf?p=1
http://www.toolingu.com/definition-430330-177320-organization-block.html

PLC and Step7



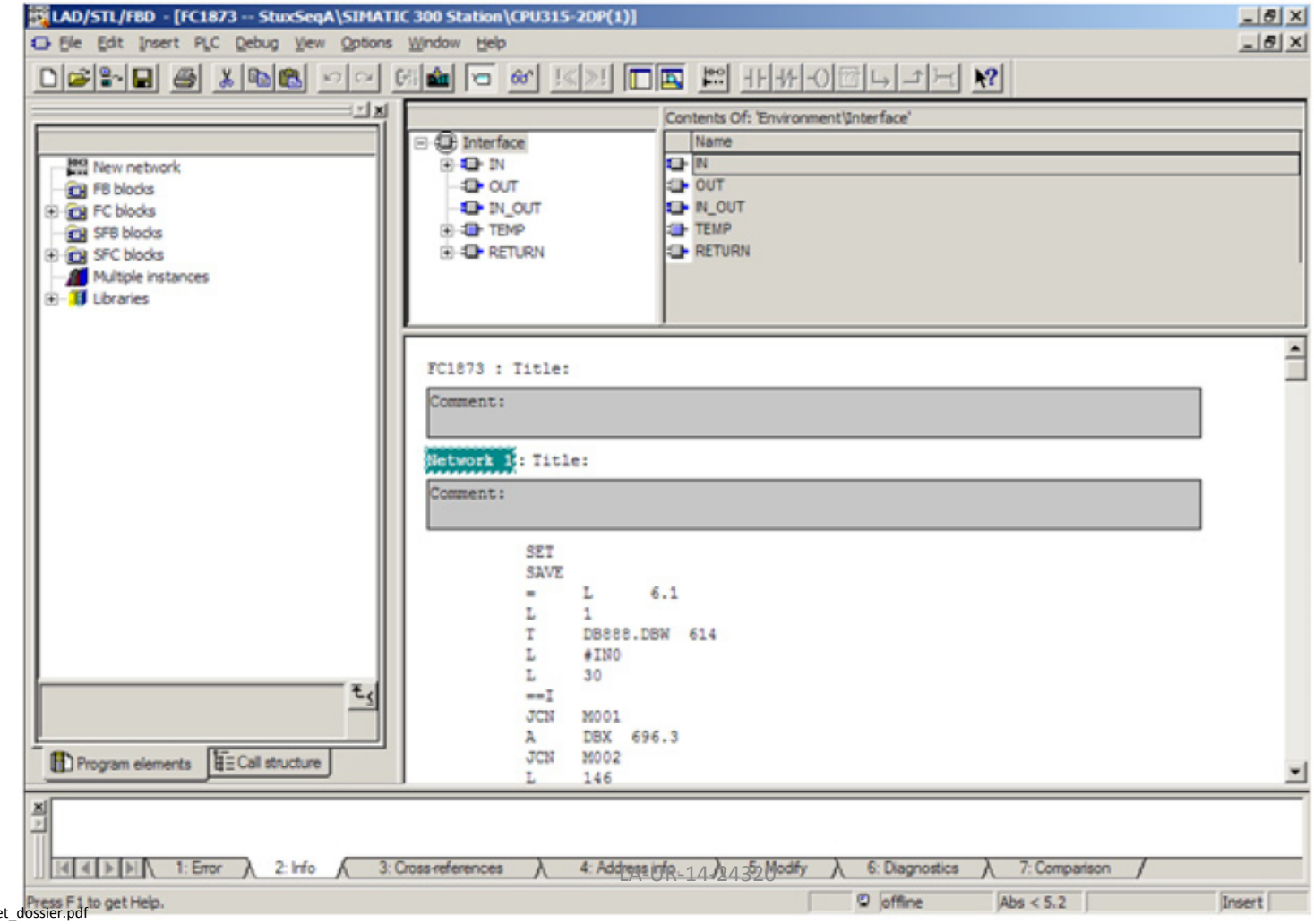
www.symantec.com/.../w32_stuxnet_dossier.pdf

STL = Statement List, ~assembly; SCL = Structured Control Language – high-level textual programming language, ~Pascal

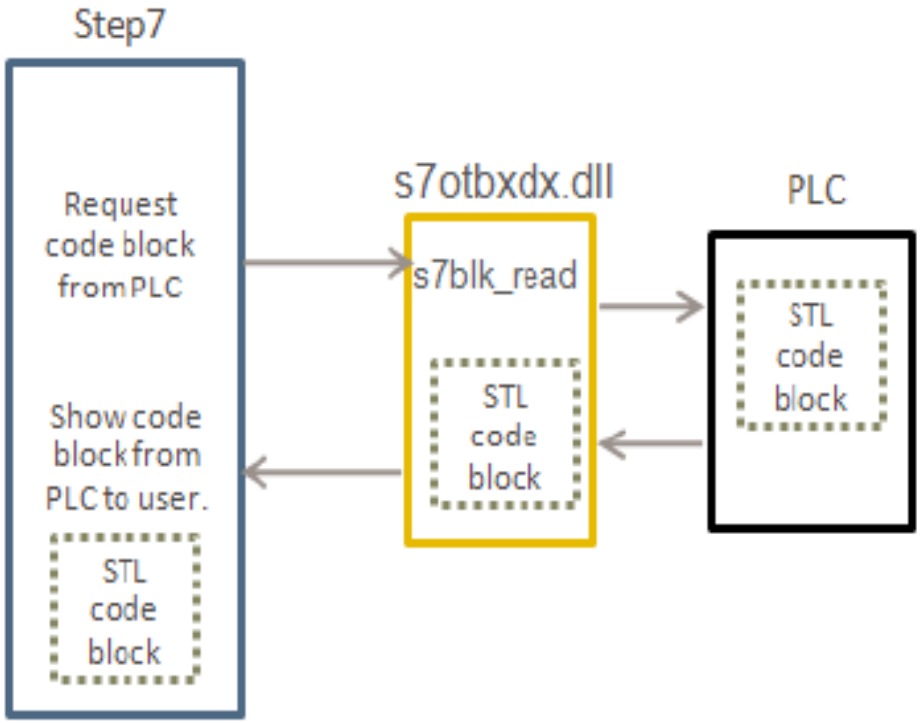
Figure 21 shows a portion of Stuxnet's malicious code in the Step7 STL editor. The beginning of the MC7 code for one of Stuxnet's Function Code (FC) blocks is visible. The code shown is from the disassembled block FC1873.

Figure 21

Stuxnet code in the Step7 STL editor

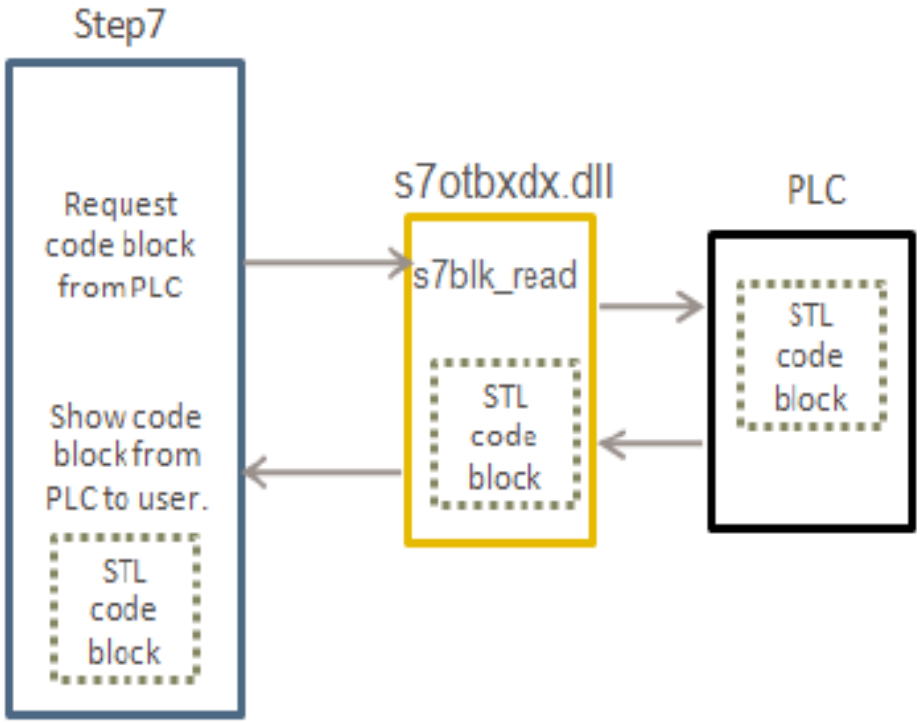


Step7 and PCL communicating via s7otbxdx.dll

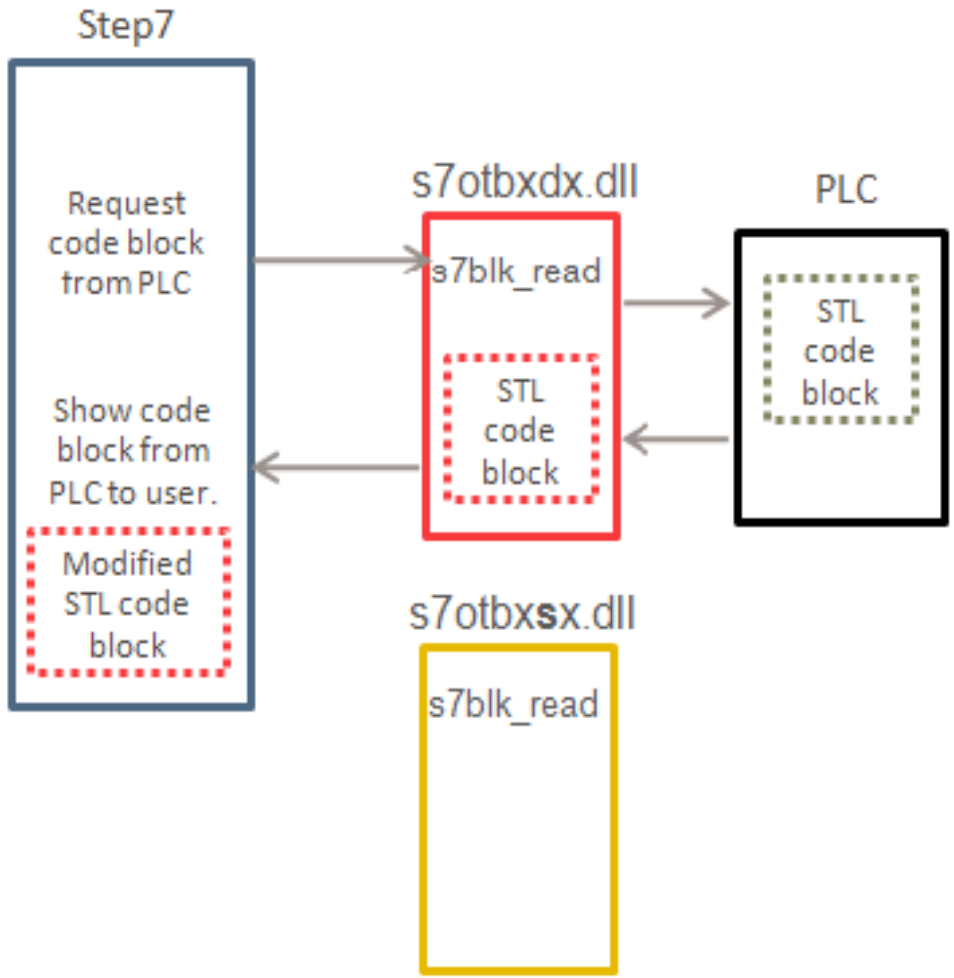


www.symantec.com/.../w32_stuxnet_dossier.pdf

Step7 and PCL communicating via s7otbxdx.dll



Communication with malicious version of s7otbxdx.dll



www.symantec.com/.../w32_stuxnet_dossier.pdf

Figure 24

OB1 before and after infection

OB1/OB35 infection

Stuxnet uses a simple code-prepending infection technique to infect Organization Blocks. For example, the following sequence of actions is performed when OB1 is infected:

- Increase the size of the original block.
- Write malicious code to the beginning of the block.
- Insert the original OB1 code after the malicious code.

Figure 24 illustrates OB1 before and after infection.

Langner explains what the rogue DLL does by referencing its decompiled code. Basically, the code ensures that it is running on a valid PLC target (making various probes of specific words in memory, checking CPU type and Control Process type, and *identifying individual targeted controllers*). If it has acquired a target, it injects code directly into the PLC's Ladder Logic (LL). This is the code that directly impacts a physical process.

www.symantec.com/.../w32_stuxnet_dossier.pdf
http://www.informit.com/articles/article.aspx?p=1636983

Outline

- Motivation
- Standards
- Vendors
- LANL
- Next Steps

Security and Privacy Controls for
Federal Information Systems
and Organizations

NIST 800-53 Revision 4: Gap Areas Addressed

- Application security
- Supply chain risk
- Security assurance and trustworthy systems
- Insider threat
- Mobile and cloud computing technologies
- Advanced persistent threat
- Tailoring guidance and overlays
- Privacy

http://nova.issa.org/wp-content/uploads/2013/06/Ron_Ross_ISSA-NOVA-06-20-2013.pdf
http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf
http://web.cecs.pdx.edu/~hook/cs491sp08/AssuranceSp08.ppt

Significant Updates to Security Controls

- Development processes, standards, and tools.
- Developer security architecture and design.
- Developer configuration management.
- Developer security testing.
- Developer-provided training.
- Supply chain protection.

http://nova.issa.org/wp-content/uploads/2013/06/Ron_Ross_ISSA-NOVA-06-20-2013.pdf

Assurance Related Controls for Different Baselines

TABLE E-1: ASSURANCE-RELATED CONTROLS FOR LOW-IMPACT SYSTEMS[99]

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-3, AT-4	PE	PE-1, PE-6, PE-8
AU	AU-1, AU-6	PL	PL-1, PL-2, PL-4
CA	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-4, CM-8	RA	RA-1, RA-3, RA-5
CP	CP-1, CP-3, CP-4	SA	SA-1, SA-2, SA-3, SA-4, SA-4 (10), SA-5, SA-9
IA	IA-1	SC	SC-1, SC-39
IR	IR-1, IR-2, IR-5	SI	SI-1, SI-4, SI-5
MA	MA-1		

TABLE E-2: ASSURANCE-RELATED CONTROLS FOR MODERATE-IMPACT SYSTEMS

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, **AT-2 (2)**, AT-3, AT-4	PE	PE-1, PE-6, **PE-6 (1)**, PE-8
AU	AU-1, AU-6, **AU-6 (1)**, **AU-6 (3)**, **AU-7**, **AU-7 (1)**	PL	PL-1, PL-2, **PL-2 (3)**, PL-4, **PL-4 (1)**, **PL-8**
CA	CA-1, CA-2, **CA-2 (1)**, CA-3, CA-5, CA-6, CA-7, **CA-7 (1)**, CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, **CM-2 (1)**, **CM-2 (3)**, **CM-2 (7)**, **CM-3**, **CM-3 (2)**, CM-4, CM-8, **CM-8 (1)**, **CM-8 (3)**, **CM-8 (5)**	RA	RA-1, RA-3, RA-5, **RA-5 (1)**, **RA-5 (2)**, **RA-5 (5)**
CP	CP-1, CP-3, CP-4, **CP-4 (1)**	SA	SA-1, SA-2, SA-3, SA-4, **SA-4 (1)**, **SA-4 (2)**, **SA-4 (9)**, SA-4 (10), SA-5, **SA-8**, SA-9, **SA-9 (2)**, **SA-10**, **SA-11**
IA	IA-1	SC	SC-1, **SC-2**, SC-39
IR	IR-1, IR-2, **IR-3**, **IR-3 (2)**, IR-5	SI	SI-1, SI-4, **SI-4 (2)**, **SI-4 (4)**, **SI-4 (5)**, SI-5, **SI-7**, **SI-7 (1)**, **SI-7 (7)**, **SI-10**, **SI-16**
MA	MA-1		

TABLE E-3: ASSURANCE-RELATED CONTROLS FOR HIGH-IMPACT SYSTEMS[103]

ID	CONTROLS	ID	CONTROLS
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-2 (2), AT-3, AT-4	PE	PE-1, PE-6, PE-6 (1), **PE-6 (4)**, PE-8
AU	AU-1, AU-6, AU-6 (1), AU-6 (3), **AU-6 (5)**, **AU-6 (6)**, AU-7, AU-7 (1), **AU-10**	PL	PL-1, PL-2, PL-2 (3), PL-4, PL-4 (1), PL-8
CA	CA-1, CA-2, CA-2 (1), **CA-2 (2)**, CA-3, CA-5, CA-6, CA-7, CA-7 (1), **CA-8**, CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-2 (1), **CM-2 (2)**, CM-2 (3), CM-2 (7), CM-3, **CM-3 (1)**, CM-3 (2), CM-4, **CM-4 (1)**, CM-8, CM-8 (1), **CM-8 (2)**, CM-8 (3), **CM-8 (4)**, CM-8 (5)	RA	RA-1, RA-3, RA-5, RA-5 (1), RA-5 (2), **RA-5 (4)**, RA-5 (5)
CP	CP-1, CP-3, **CP-3 (1)**, CP-4, CP-4 (1), **CP-4 (2)**	SA	SA-1, SA-2, SA-3, SA-4, SA-4 (1), SA-4 (2), SA-4 (9), SA-4 (10), SA-5, SA-8, SA-9, SA-9 (2), SA-10, SA-11, **SA-12**, **SA-15**, **SA-16**, **SA-17**
IA	IA-1	SC	SC-1, SC-2, **SC-3**, **SC-7 (18)**, **SC-7 (21)**, **SC-24**, SC-39
IR	IR-1, IR-2, **IR-2 (1)**, **IR-2 (2)**, IR-3, IR-3 (2), IR-5, **IR-5 (1)**	SI	SI-1, SI-4, SI-4 (2), SI-4 (4), SI-4 (5), SI-5, **SI-5 (1)**, **SI-6**, SI-7, SI-7 (1), **SI-7 (2)**, **SI-7 (5)**, SI-7 (7), **SI-7 (14)**, SI-10, SI-16
MA	MA-1		

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST 800-160

- Describe best practices for security engineering.
- Show how security engineering can be integrated into the traditional systems engineering process.
- Demonstrate linkage from system and security engineering processes to information security and risk management processes.

http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

Security

A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protection measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach [CNSSI 4009].

Note 1: The CNSSI 4009 definition focuses on security as an organizational enterprise objective.

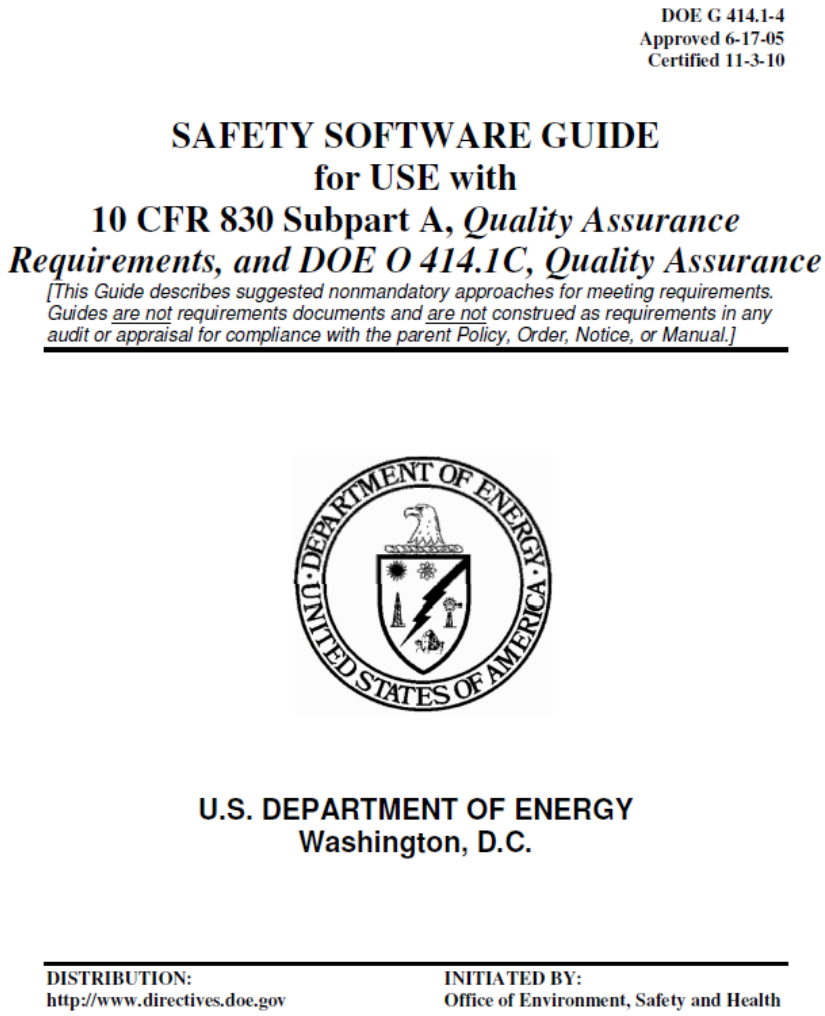
Note 2: The engineering perspective views security as a complex quality factor that is composed of multiple quality sub-factors. The most prevalent sub-factors are confidentiality, integrity, and availability. Additionally, the integrity sub-factor can be further divided into hardware, software, data, and communications integrity. Other security-relevant quality sub-factors include, but are not limited to, privacy and non-repudiation. There are also quality sub-factors that generally have been considered only by the system safety engineering, such as continuity, resiliency, and fault-tolerance, that are now being assessed in terms of susceptibility to malicious intent and the resultant impact on the mission/business; all motivated by mission assurance concerns that span the entire spectrum of incidental and accidental misuse through to attack by an advanced persistent threat.

The systems security engineering perspective ensures that all security-relevant quality sub-factors are satisfied by the engineered system and that the system achieves mission/business security objectives such as that defined by CNSSI 4009.

http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

DOE G 414.1-4 Revision

- Include
  - Digital instrumentation, Control and Automation System software
    - E.g. Controllers (e.g. PLC), smart transmitters
    - Firmware and embedded systems
  - Security controls
  - Software security assurance
  - Non-safety software



DOE G 414.1-4
Approved 6-17-05
Certified 11-3-10

SAFETY SOFTWARE GUIDE
for USE with
10 CFR 830 Subpart A, *Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*

[This Guide describes suggested nonmandatory approaches for meeting requirements. Guides are not requirements documents and are not construed as requirements in any audit or appraisal for compliance with the parent Policy, Order, Notice, or Manual.]

U.S. DEPARTMENT OF ENERGY
Washington, D.C.

DISTRIBUTION: http://www.directives.doe.gov

INITIATED BY: Office of Environment, Safety and Health

http://energy.gov/sites/prod/files/hss/Enforcement%20and%20Oversight/Enforcement/docs/guides/DOE_Guide_414_1_4.pdf

Safety Software

http://www.nrc.gov/about-nrc/regulatory/research/digital/key-issues/cyber-security.html

U.S. NUCLEAR REGULATORY COMMISSION

January 2010

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 5.71

(New Regulatory Guide)

CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES

U.S. NUCLEAR REGULATORY COMMISSION

July 2011
Revision 3

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.152

(Draft was issued as DG-1249, dated June 2010)

CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

NUREG-0800

U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

BRANCH TECHNICAL POSITION 7-14

GUIDANCE ON SOFTWARE REVIEWS FOR DIGITAL COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-01

Task Working Group #1:
Cyber Security

Interim Staff Guidance

http://www.nrc.gov/reading-rm/doc-collections/reg-guides/
http://pbadupws.nrc.gov/docs/ML0706/ML070670183.pdf
http://pbadupws.nrc.gov/docs/ML0729/ML072980159.pdf

Outline

- Motivation
- Standards
- Vendors
- LANL
- Next Steps

ICS Vendor Security Strategies – Security Development Lifecycle (Dale Peterson/Digital Bond)

A major difference in ICS vendor's security strategies is how much effort they are putting on security throughout the product lifecycle, or their Security Development Lifecycle (SDL). Put another way, how secure is their own code from common programming mistakes that lead to exploitable vulnerabilities.

Microsoft popularized the SDL after having security issues with worms early in the previous decade. Some vendors have highly leveraged Microsoft and others experience to integrate threat modeling, security requirements, fuzz testing, third party assessments and a variety of other security development procedures into the product development process.

Others have done very little to add security into the development process.

…

So you should be asking your vendors about their development process. What are the elements in their security development lifecycle? Can you see their threat models? Fuzz testing and other security QA testing results? How security is integrated into the requirements? What are there secure coding standards? How are there engineers trained on those standards and how to they insure those standards are met?

You do not need to be a security expert or even review these documents in great detail. A couple of hours of interview and inspection is plenty. It often is as simple as can the vendor show you the SDL and its results from a project? It is an easy answer and item to provide if there was an SDL and it was followed. If it is not there is a lot of hemming and hawing and struggle to create documentation after the fact.

http://www.digitalbond.com/blog/2011/01/19/ics-vendor-security-strategies-%E2%80%93-part-iv-security-development-lifecycle/

Vendor Questions

- What standard(s)/guidelines are you using?
- Do you have a secure software/firmware development life cycle (concept to delivery), where there is a security requirement that is defined and analyzed for each phase?
- How do you secure firmware in comparison with your software (e.g. Engineering Workstation verification tool prior to Controller download, access control for firmware update, downloads only to a specific Controller serial number, digital signature)?
- How are your securing your databases?
- How are you promoting a culture of security in their organization (e.g. training)?
- How do you monitor the threat landscape (e.g. OWASP Top Ten, CWE/SANS Top 25 Most Dangerous Software Errors, CVE/CWE, WASC Threat Classification v2.0)?
- How do you notify customers of security vulnerabilities?
- What type of patch/upgrade testing do you do?

BAS HMI Software

AUTOMATEDLOGIC
1150 Roberts Boulevard
Kennesaw, Georgia 30144
770/429-3000
Fax 770/429-3001
www.automatedlogic.com

Memorandum: **WebCTRL® Security**

Date: June 3, 2013

The WebCTRL Server application provides a very high level of security, making unauthorized access extremely unlikely. This memorandum briefly outlines design, security, configuration, and implementation aspects of your WebCTRL Building Automation System Server application.

- WebCTRL web server engine:
  - The WebCTRL Server application uses its own built-in web server engine based on a locked-down version of Apache Tomcat. This greatly reduces the chance of an undiscovered Apache Tomcat vulnerability.
  - The WebCTRL Server application does NOT use Microsoft's IIS web server.
  - The web server renders only WebCTRL pages. It cannot be used as a general-purpose web server to render pages from other systems on the building network.
  - All database queries use a single internal interface that protects against common SQL injection attacks. As of v6.0, this includes Write to Database alarm actions.
  - As of v6.0, the WebCTRL Server application no longer uses Java Applets or Java Web Start which have been the source of Java vulnerabilities to desktop computers. While we no longer use Java, we do recommend that customers keep their Java Runtime Environment up to date at all times.
  - Any add-on application not provided by Automated Logic should be carefully reviewed for source and content before using with the WebCTRL Server application.

- WebCTRL communications:
  - The WebCTRL Server application uses the ports and protocols listed in the following table. In the **Use** column, **Client/Server** is communication between the end user's computer and the

WebCTRL White Paper Section	Security Control - Automated Logic	NIST 800-53r4 Control	NIST 800-53r4 Control Name
Web Server Engine			
	The WebCTRL Server application uses its own built-in web server engine based on a locked down version of ApachTomcat. This greatly reduces the chance of an undiscovered Apache Tomcat vulnerability. [1]	AC-4	Information Flow Enforcement
		CM-2	Baseline Configuration
		CM-6	Configuration Settings
		SA-4	Acquisition Process
		SA-20	Customized Development of Critical Components
		SI-4	Information System Monitoring
	The WebCTRL Server application does NOT use Microsoft's IIS web server. [2]	SA-8	Security Engineering Principles
		SA-13	Trustworthiness
...		SA-17	Developer Security Architecture and Design
	purpose web server to render pages from other systems on the building network.	SI-10	Information Input Validation
	All database queries use a single internal interface that protects against common SQL injection attacks. As of v6.0, this includes Write to Database alarm actions. [3, 4]	SI-10	Information Input Validation
		SI-15	Information Output Filtering
		SC-5	DoS Protection
	As of v6.0, the WebCTRL Server application no longer uses Java Applets or Java Web Start which have been the source of Java vulnerabilities to desktop computers. While we no longer use Java, we do recommend that customers keep their Java Runtime Environment up to date at all times. [2]	SA-8	Security Engineering Principles
		SA-13	Trustworthiness
		SA-17	Developer Security Architecture and Design
	Any add-on application not provided by Automated Logic should be carefully reviewed for source and content before using with the WebCTRL Server application.	SA-8	Security Engineering Principles
		SA-13	Trustworthiness
		SA-17	Developer Security Architecture and Design
Communications			
	Windows file sharing, or other applications that can increase the vulnerability of the system. The Diagnostic Telnet port listed above is a password-protected text-only UI that is limited to WebCTRL Server application functions. This is ONLY used for Tech Support purposes and should be firewalled.	AC-2	Account Management

NIST 800-53r4 Control	NIST 800-53r4 Name	#
CM-7	Least Functionality	6
AC-2	Account Management	4
AC-3	Access Enforcement	4
AC-6	Least Privilege	4
IA-5	Authenticator Management	4
SA-8	Security Engineering Principles	4
SA-13	Trustworthiness	4
SA-17	Developer Security Architecture and Design	4
SC-8	Transmission Confidentiality and Integrity	4
SC-12	Cryptographic Key Establishment andManagement	4
SC-13	Cryptographic Protection	4
IA-2	Identification and Authentication (Organizational Users)	3
SC-7	Boundary Protection	3
SC-23	Session Authenticity	3
AC-4	Information Flow Enforcement	2
AU-3	Content of Audit Records	2
CM-6	Configuration Settings	2
SI-10	Information Input Validation	2
AC-17	Remote Access	1
CM-2	Baseline Configuration	1
CP-11	Alternate Communications Protocols	1
RA-5	Vulnerability Scanning	1
SA-4	Acquisition Process	1
SA-20	Customized Development of Critical Components	1
SC-5	Denial of Service Protection	1
SC-32	Information System Partitioning	1
SI-4	Information System Monitoring	1
SI-15	Information Output Filtering	1

NIST 800-53r4 Family	NIST 800-53r4 Name	#
SC	System and Communications Protection	20
AC	Access Control	15
SA	Security Assessment and Authorization	14
CM	Configuration Management	9
IA	Identification and Authentication	7
SI	System and Information Integrity	4
AU	Audit and Accountability	2
CP	Contingency Planning	1
RA	Risk Assessment	1

A1-Injection

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2-Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

A3-Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A4-Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

A5-Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

...

OWASP	OWASP Top 10 - 2013	NIST 800-53r4 Control	NIST 800-53r4 Name
A1	Injection	SI-10	Information Input Validation
A2	Broken Authentication and Session Management	SC-23	Session Authenticity
A3	Cross-Site Scripting (XSS)	SI-10	Information Input Validation
		SC-18	Mobile Code
A4	Insecure Direct Object References	AC-3	Access Enforcement
		SI-10	Information Input Validation
A5	Security Misconfiguration	AC-3	Access Enforcement
		AC-4	Information Flow Enforcement
		SI-10	Information Input Validation
		SI-11	Error Handling
		SC-8	Transmission Confidentiality and Integrity
		SC-18	Mobile Code
A6	Sensitive Data Exposure	AC-4	Information Flow Enforcement
		SC-4	Information in Shared Resources
		SC-8	Transmission Confidentiality and Integrity
		SC-12	Cryptographic Key Establishment and Management
		SC-13	Cryptographic Protection
		SC-23	Session Authenticity
		SC-28	Proteciton of Information at Rest
A7	Missing Function Level Access Control	AC-3	Access Enforcement
A8	Cross-Site Request Forgery (CSRF)	SC-23	Session Authenticity
A9	Using Known Vulnerable Components	SC-5	DoS Protection
A10	Unvalidated Redirects and Forwards	SI-10	Information Input Validation

OWASP	OWASP Top 10 - 2013	NIST 800-53r4 Control	NIST 800-53r4 Name
A1	Injection	SI-10	Information Input Validation
A2	Broken Authentication and Session Management	SC-23	Session Authenticity
A3	Cross-Site Scripting (XSS)	SI-10	Information Input Validation
		SC-18	Mobile Code
A4	Insecure Direct Object References	AC-3	Access Enforcement
		SI-10	Information Input Validation
A5	Security Misconfiguration	AC-3	Access Enforcement
		AC-4	Information Flow Enforcement
		SI-10	Information Input Validation
		SI-11	Error Handling
		SC-8	Transmission Confidentiality and Integrity
		SC-18	Mobile Code
A6	Sensitive Data Exposure	AC-4	Information Flow Enforcement
		SC-4	Information in Shared Resources
		SC-8	Transmission Confidentiality and Integrity
		SC-12	Cryptographic Key Establishment and Management
		SC-13	Cryptographic Protection
		SC-23	Session Authenticity
		SC-28	Proteciton of Information at Rest
A7	Missing Function Level Access Control	AC-3	Access Enforcement
A8	Cross-Site Request Forgery (CSRF)	SC-23	Session Authenticity
A9	Using Known Vulnerable Components	SC-5	DoS Protection
A10	Unvalidated Redirects and Forwards	SI-10	Information Input Validation

NIST 800-53r4 Control	NIST 800-53r4 Name	#
SI-10	Information Input Validation	5
AC-3	Access Enforcement	3
SC-23	Session Authenticity	3
AC-4	Information Flow Enforcement	2
SC-18	Mobile Code	2
SC-8	Transmission Confidentiality and Integrity	2
SC-12	Cryptographic Key Establishment and Management	1
SC-13	Cryptographic Protection	1
SC-28	Protection of Information at Rest	1
SC-4	Information in Shared Resources	1
SC-5	Denial of Service Protection	1
SI-11	Error Handling	1

NIST 800-53r4 Control	NIST 800-53r4 Name	#
SC	System and Communications Protection	12
SI	System and Information Integrity	6
AC	Access Control	5

COMPARE: HMI vs. IT Web App

WebCTRL				OWASP Top 10		
NIST 800-53r4 Control	**NIST 800-53r4 Name**	**#**		**NIST 800-53r4 Control**	**NIST 800-53r4 Name**	**#**
CM-7	Least Functionality	6		SI-10	Information Input Validation	5
AC-2	Account Management	4		AC-3	Access Enforcement	3
AC-3	Access Enforcement	4		SC-23	Session Authenticity	3
AC-6	Least Privilege	4				
IA-5	Authenticator Management	4				
SA-8	Security Engineering Principles	4				
SA-13	Trustworthiness	4				
SA-17	Developer Security Architecture and Design	4				
SC-8	Transmission Confidentiality and Integrity	4				
SC-12	Cryptographic Key Establishment andManagement	4				
SC-13	Cryptographic Protection	4				
NIST 800-53r4 Family	**NIST 800-53r4 Name**	**#**		**NIST 800-53r4 Family**	**NIST 800-53r4 Name**	**#**
SC	System and Communications Protection	20		SC	System and Communications Protection	12
AC	Access Control	15		SI	System and Information Integrity	6
SA	Security Assessment and Authorization	14		AC	Access Control	5

SANS “Critical Security Controls v5”

Critical Security Controls - Version 5

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Access Control
8: Data Recovery Capability
9: Security Skills Assessment and Appropriate Training to Fill Gaps
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11: Limitation and Control of Network Ports, Protocols, and Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense
14: Maintenance, Monitoring, and Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Protection
18: Incident Response and Management
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises

Critical Security Control: 6

‹ Critical Control 5 Critical Control 7 ›

Application Software Security

Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Why Is This Control Critical?

Attacks often take advantage of vulnerabilities found in web-based and other application software. Vulnerabilities can be present for many reasons, including coding mistakes, logic errors, incomplete requirements, and failure to test for unusual or unexpected conditions. Examples of specific errors include: the failure to check the size of user input; failure to filter out unneeded but potentially malicious character sequences from input streams; failure to initialize and clear variables; and poor memory management allowing flaws in one part of the software to affect unrelated (and more security critical) portions. There is a flood of public and private information about such vulnerabilities available to

ID #	Description	Category
CSC 6-1 (NEW)	For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.	Quick Win

NERC CIP Standard Mapping to the Critical Security Controls - Draft

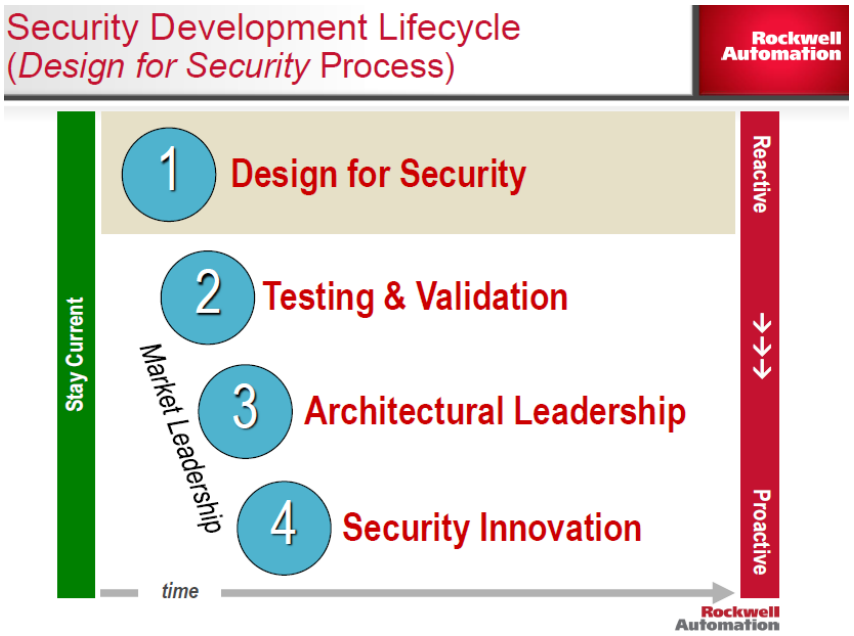
For any feedback or suggestions on this poster, please contact :

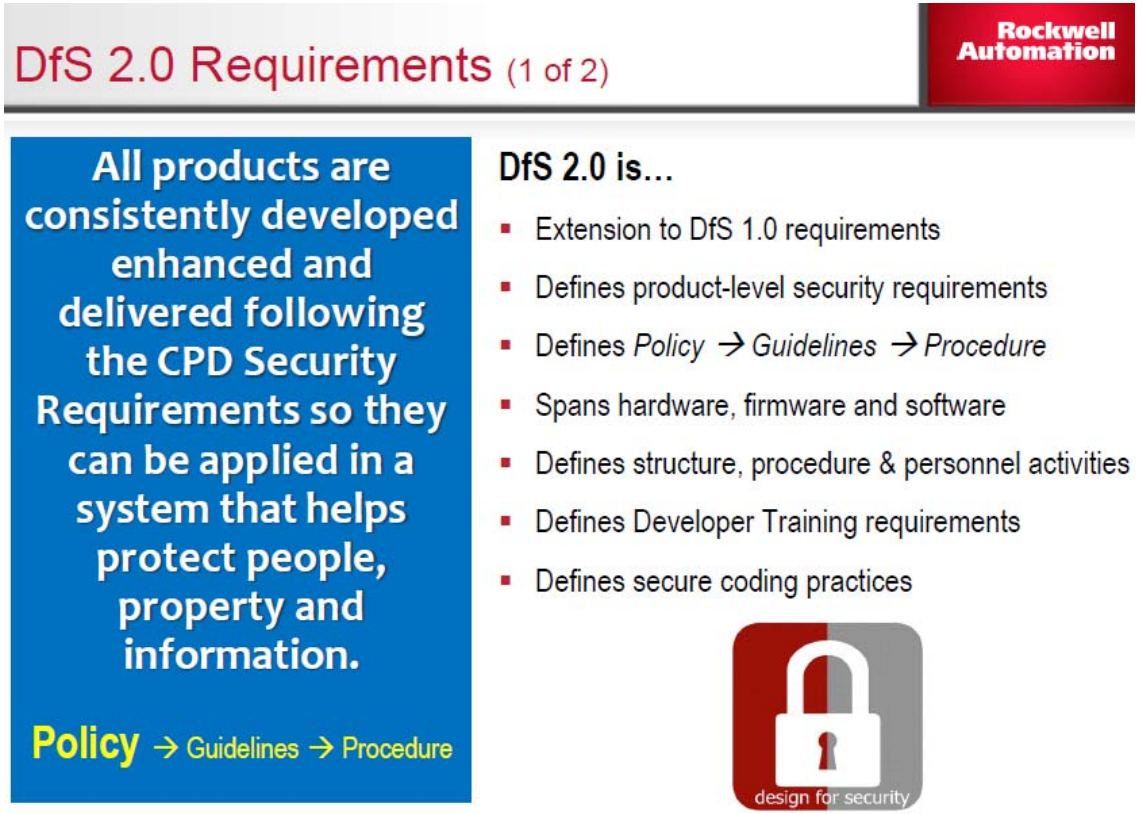
CIP@securingthehuman.org
www.securingthehuman.org/utility

NERC CIP Version 3	NERC CIP Version 4	NERC CIP Version 5	Critical Security Controls
CIP-002-3 Critical Cyber Asset Identification	CIP-002-4 Critical Cyber Asset Identification	CIP-002-5 BES Cyber System Categorization	
: Risk-Based Assessment Methodology (RBAM) to id Critical sets (CA)	Attachment 1: Critical Asset Criteria added to determine criticality. No more RBAM. Sub-requirements R1.1 and R1.2 now N/A	R1: Attachment 1 CIP-002-5 incorporates the "Bright Line Criteria" to classify BES Assets as Low, Medium, or High. Called BES Cyber Systems consolidating CAs and CCAs	Control 1: Inventory of Authorized and Unauthorized Device Control 2: Inventory of Authorized and Unauthorized Software Control 4: Continuous Vulnerability Assessment and Remediation
: Apply RBAM to ID Critical Assets	N/A	R2: BES Cyber System Lists must be reviewed and approved every 15 calendar months	
: Identify Critical Cyber Assets (CCA)	New R2		

http://www.sans.org/critical-security-controls/
https://www.sans.org/media/critical-security-controls/nerc-cip-mapping-sans20-csc.pdf

“Yes, we have one!”





“Design for Security”
https://www.rockwellautomation.com/resources/downloads/rockwellautomation/pdf/events/pnc-13/sessions/industrial-security-perspectives.pdf
https://www.rockwellautomation.com/resources/downloads/rockwellautomation/pdf/events/pnc-13/sessions/industrial-security-perspectives.pdf

Rockwell Software & Firmware

Rockwell Software Product Directory

1 Design & Configuration

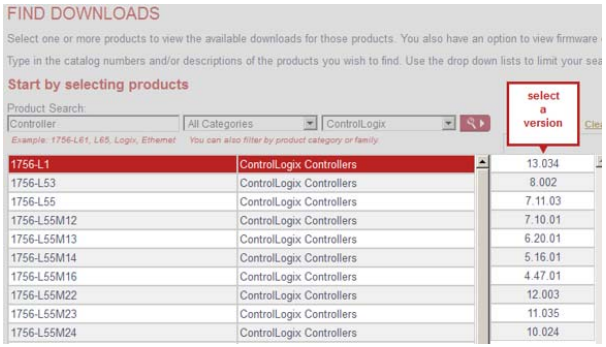
(e.g. Ladder Logic)

- Arena
- FactoryTalk AssetCentre
- RSLinx®
- RSLogix
- RSLogix Emulate
- RSNetWorx
- Studio 5000

2 HMI

- FactoryTalk View
- FactoryTalk ViewPoint
- RSView32

3 Firmware



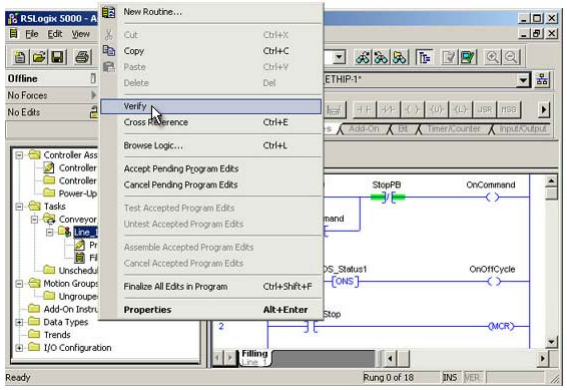
http://www.rockwellautomation.com/rockwellsoftware/products/overview.page
http://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?famID=2&keyword=Controller&crumb=112

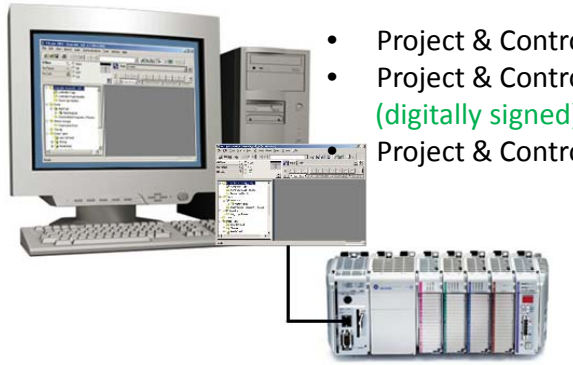
Rockwell Automation – Firmware “Verify”

RSLogix 5000 How Do I?

Media clips and tutorials organized under the topics: Get Started, Get Connected, and My First Project that show a u use the software to complete common tasks.

- Get Started
- Get Connected
- My First Project
  - Create a New Project
  - Modify the Main Task
  - Modify the Main Program
  - Modify the Main Routine
  - Configure an Input Module
  - Configure an Output Module
  - Create a Tag
  - Create a User-Defined Data Type
  - Enter Ladder Diagram Routine Logic
  - Reference a Tag in a Routine
  - Verify a Project
  - Download a Project
  - Go Online
  - Change a Controller's Mode
  - Monitor & Edit Data Online





- Project & Controller slot #
- Project & Controller firmware revision (digitally signed)
- Project & Controller serial #

http://www.rockwellautomation.com/resources/downloads/rockwellautomation/multimedia/solutions/integrated-architecture/StartPageMedia/MediaPlayer.html?media=P11-Verify.swf&mediaLang=ENU&defaultMediaLang=ENU
http://www.rockwellautomation.com/resources/downloads/rockwellautomation/multimedia/solutions/integrated-architecture/StartPageMedia/MediaPlayer.html?media=P15-DownloadProject.swf&mediaLang=ENU&defaultMediaLang=ENU

Rockwell Automation - Add-On Instructions

- Custom instructions that you design and create
- Encapsulate commonly used functions or device controls
- High integrity – 32-bit signature values seals the instruction to prevent modification and provide high integrity

Instruction Signature

The instruction signature, available for both standard and safety controllers, lets you quickly determine if the Add-On Instruction has been modified. Each Add-On Instruction has its own instruction signature on the Add-On Instruction definition. The instruction signature is required when an Add-On Instruction is used in SIL 3 safety-related functions, and may be required for regulated industries. Use it when your application calls for a higher level of integrity.

Once generated, the instruction signature seals the Add-On Instruction, preventing it from being edited until the signature is removed. This includes rung comments, tag descriptions, and any instruction documentation that was created. When an instruction is sealed, you can perform only these actions:

- Copy the instruction signature
- Create or copy a signature history entry
- Create instances of the Add-On Instruction
- Download the instruction
- Remove the instruction signature
- Print reports

http://literature.rockwellautomation.com/idc/groups/literature/documents/pm/1756-pm010_-en-p.pdf

Rockwell Automation Support Center

Search Knowledgebase | Explore Forums | Submit Questions | Chat Live | Find My Stuff | Get Help

54102 - Industrial Security Advisory Index

Access Level: Everyone
Date Created: 07/30/2008 01:26 PM
Last Updated: 03/27/2014 09:20 AM

Industrial security continues to rapidly become an essential consideration in the design and operation of contemporary controls systems. Rockwell Automation recognizes the importance of security for industrial control applications. Employing good security measures in a control system can help protect amongst other things personal safety, critical assets, intellectual property and key proprietary data. It remains an integral aspect to the Rockwell Automation controls philosophy to deliver and evolve comprehensive security solutions that meet customer needs while also providing an appropriate level of support and services that help fulfill our customer's security goals and requirements.

This Industrial Security Advisory Index contains direct pointers to specific industrial security content held in Rockwell Automation's Knowledgebase and public website. The materials contained herein and hereby referenced are intended to inform, educate, and assist our customers about industrial security as it relates to Rockwell Automation products and systems.

Rockwell Automation Security Notices & Alerts:

- 54103 - Firmware Upgrade Security Notice: Comment on DHS Communication (Control Systems Vulnerability)
- 57729 - Potential Security Vulnerabilities in ControlLogix 1756-ENBT/A EtherNet/IP Bridge
- 58964 - ControlLogix 1756-ENBT/A EtherNet/IP Bridge Firmware Upgrade Process
- 65980 - Password Security Vulnerability in MicroLogix™ Controllers
- 65982 - Client Software Authentication Security Vulnerability in MicroLogix™ Controllers
- 66678 - Password Security Vulnerability in PLC5® and SLC™ 5/0x Controllers
- 66684 - Client Software Authentication Security Vulnerability in PLC5® and SLC™ 5/0x Controllers

54103 - Firmware Upgrade Security Notice: Comment on DHS Communication (Control Systems Vulnerability in Multiple Sectors)

Access Level: Everyone
Date Created: 07/30/2008 01:32 PM
Last Updated: 02/19/2013 11:27 AM

Rockwell Automation recognizes the importance of information and control system security to our customers. We are committed to working with government agencies and standards development organizations to develop solutions targeted to help our customers improve their overall system security strategy.

As part of this effort, the Idaho National Laboratory (INL) Control Systems Security Program, under contract to the Department of Homeland Security (DHS), identified a potential security concern within the firmware upgrade process used in control systems deployed in Critical Infrastructure and Key Resources (CIKR). DHS has confirmed that the firmware upgrade process can be intentionally manipulated in a manner that has potential to render the device inoperable and cause a disruption to the process and/or system operation.

Rockwell Automation has been working in partnership with DHS to identify potential short-term and long-term mitigation strategies.

As a result, Rockwell Automation is implementing a policy to digitally sign most firmware images and require contemporary devices to validate this signature before applying a firmware upgrade. Over time, many contemporary Rockwell Automation products will include this signature validation mechanism to help ensure firmware integrity and authenticity.

The following Rockwell Automation products currently authenticate firmware using digital signatures:

- ControlLogix 1756-L72, L73, L74, L75 Programmable Automation Controllers
- Virtual firmware of the 1789 SoftLogix PC based controllers

For other devices, to help reduce the likelihood of the upgrade process being exploited and help reduce associated security risk, Rockwell Automation and DHS recommend the following short-term mitigation strategies (Note: multiple strategies can be employed simultaneously):

1. Disable where possible the capability to perform remote firmware upgrades over a network to a controller by placing the controller key switch into RUN mode. This prevents the Allen-Bradley brand controllers from accepting firmware upgrades.

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/54102
https://rockwellautomation.custhelp.com/app/answers/detail/a_id/54103

Outline

- Motivation
- Standards
- Vendors
- LANL
- Next Steps

What is LANL doing for Control Systems?

- Participating in DOE G 414.1-4 Revision
- Kristi's "Secure Coding" initiative
  - LANL Secure Coding Day – Control System speaker
- Quality & Performance Assurance Audit – Control system SW/FW
- Control System
  - Security Plan – included "SW Quality Management" reference for SW/FW
  - Annual Control System Workshop – LANL talk

Outline

- Motivation
- Standards
- Vendors
- LANL
- Next Steps

Next Steps

- Add Control Systems to Kristi's plan
  - Initial Phase
    - Awareness, education, building/maturing basic services and prototyping with a small team
  - Institutional Phase
    - Scale team to LANL, make resources available to all developers, enforce secure coding practices
- Mindset – "Adapt to this evolving discipline"