NICE Webinar Series

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Securing Operational Technologies and Control Systems with a Skilled Workforce

July 21, 2021

Operational Technology (OT) Cybersecurity

Keith Stouffer

Intelligent Systems Division
Engineering Laboratory
NIST
Keith.stouffer@nist.gov

Operational Technology (OT) Definition

Operational technology (OT) encompasses a broad range of programmable systems or devices that **interact with the physical environment** (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems (ICS), building management systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.

NIST OT Cybersecurity Program

Cybersecurity risk management is an important factor to ensure the safe and reliable delivery of the goods and services provided and supported by OT. The NIST OT Security Program includes multiple collaborative projects from across the NIST Information Technology Laboratory and Engineering Laboratory.

https://csrc.nist.gov/projects/operational-technology-security

TIPS & TACTICS
CONTROL SYSTEM
CYBERSECURITY

NIST CYBER

Quick steps you can take now to PROTECT your control system:

1. PUT SOMEONE IN CHARGE
2. KNOW WHAT YOU HAVE
3. ESTABLISH CYBERSECURITY RELATIONSHIPS
4. CHANGE DEFAULT PASSWORDS
5. PROTECT ASSETS FROM TAMPERING

Additional steps to MANAGE your control system cybersecurity risk:

1. TRAINING & AWARENESS
2. MANAGE USER CREDENTIALS & ACCESS
3. RESTRICT ACCESS TO THE CONTROL SYSTEM NETWORK & NETWORK ACTIVITY
4. MANAGE CYBERSECURITY VULNERABILITIES
5. IMPLEMENT APPLICATION CONTROL
6. PREPARE TO RECOVER FROM A CYBERSECURITY INCIDENT
7. IMPLEMENT & PERFORM CONTINUOUS MONITORING

NIST National Institute of Standards and Technology U.S. Department of Commerce

Example OT Cybersecurity Resources

NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security

https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

Manufacturing Extension Partnership Cybersecurity Resources

https://www.nist.gov/mep/cybersecurity-resources-manufacturers

Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide

https://csrc.nist.gov/news/2019/nistir-8183a-csf-mfg-profile-low-impact-level

Cybersecurity & Infrastructure Security Agency (CISA) ICS Cybersecurity Recommended Practices

https://us-cert.cisa.gov/ics/Recommended-Practices

Example OT Cybersecurity Training and Certifications

CISA - Some courses available at no cost

https://us-cert.cisa.gov/ics/Training-Available-Through-ICS-CERT

International Society of Automation and International Electrotechnical Commission (ISA/IEC)

https://isaeurope.com/certification/

SANS

https://www.sans.org/cyber-security-courses/?focus-area=industrial-control-systems-security

Global Information Assurance Certification (GIAC)

https://www.giac.org/certifications/industrial-control-systems

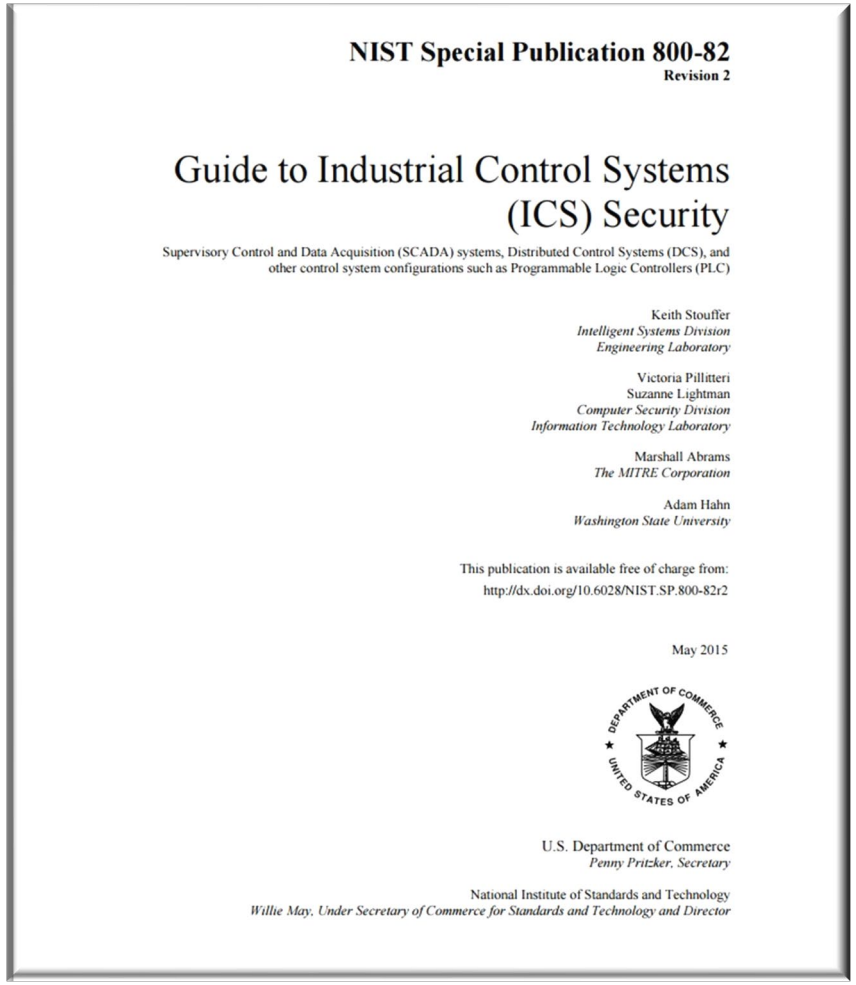
SCADAhacker

https://scadahacker.com/training.html

NIST SP 800-82

Guide to Industrial Control Systems Security

- Provides a comprehensive cybersecurity approach for securing ICS, while addressing unique performance, reliability, and safety requirements, including implementation guidance for NIST SP 800-53 controls
- Initial draft - September 2006
- Revision 1 - May 2013
- Revision 2 - May 2015
- 3,000,000+ downloads, 800+ citations, de facto worldwide standard/guideline for industrial control system cybersecurity



NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Intelligent Systems Division
Engineering Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Marshall Abrams
The MITRE Corporation

Adam Hahn
Washington State University

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

May 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

NIST SP 800-82 Update

NIST has initiated an update of SP 800-82 to incorporate lessons learned over the past several years, to provide alignment to relevant NIST guidance, to provide alignment to other relevant control system cybersecurity standards and recommended practices, and to address changes in the threat landscape. The initial public draft, which will be published as SP 800-82, Revision 3, is scheduled for late 2021/early 2022.

Proposed updates:

- Expansion in scope of SP 800-82 from ICS to control systems/OT in general
- Application of new cybersecurity capabilities in control system/OT environments
- Development of guidance specific to small and medium-sized control system/OT owners and operators
- Updates to control system/OT threats, vulnerabilities, standards, and recommended practices
- Updates to the current ICS Overlay to align with SP 800-53, Rev 5
- Removal of outdated material from the current document

Q & A

Megan Samford

Vice President,
Chief Product Security Officer,
Energy Management
Schneider Electric

in/megan-Samford-13282814

Follow me on LinkedIn

Life Is On | Schneider Electric

85% OF Critical Infrastructure

Is owned and operated by the private sector

Control Systems are the **heart and lungs** of Critical Infrastructure

>90% of the national control systems cybersecurity workforce needs are NOT being met
-CyberSeek

Big events are rare, but indirect high-frequency/low impact ones are common

MAROOCHY SHIRE
LARGE-SCALE ENVIRONMENTAL DISASTER CAUSED BY A SINGLE DISGRUNTLED PERSON
2000

DAVID BESSE NUCLEAR
SLAMMER WORM CAUSED 5 HOURS LOSS OF VISIBILITY ON SAFETY SYSTEMS
2003

STUXNET
1ST ATTACK CAUSING CYBER PHYSICAL DAMAGE AGAINST A NATION STATE
2010

SHAMOON
DEMONSTRATED LARGE DEPENDENCY ON GLOBABLE MARKETS AND COMMODITY HARDWARE
2010

GERMAN STEEL MILL
PROCESS AND CONTROL WAS DISRUPTED CAUSING PHYSICAL DAMAGE
2014

UKRAINE POWERGRID
1ST MAJOR CYBER ATTACK AGAINST THE POWERGRID
2015

WATER TREATMENT
LARGE-SCALE WATER TREATMENT OT PROCESS ALTERED AND AFFECTED RESIDENTS
2016

NOTPETYA
OVER $10 BILLION DOLLARS FOR MERCK, MAERSK, MODELEZ AND A UK FIRM
2017

MIRAI BOTNET
1ST MAJOR DDOS ATTACKS USING IOT/IP DEVICES
2017

TRISIS
1ST MAJOR ATTACK AGAINST INDUSTRIAL SAFETY SYSTEMS
2017

NORSK HYDRO
TARGETED RANSOMWARE LEVERAGING IT INFRASTRUCTURE
2019

SOLAR WINDS
WIDESCALE SUPPLYCHAIN ATTACK AFFECTING SOME COMPANIES
2020

OLDSMAR WATER
TEAM VIEWER COMPROMISED AND CONTROLS ALTERED
2021

HONDA
OPERATIONS AND SUBSIDUARIES DISRUPTED BY RANSOMWARE
2020

WHATS NEXT?

IT and OT environments have different demands. For example, they have

Security related approaches:	Information technology (IT)	Operations Technology (OT)
Security Priorities	Confidentiality, Integrity, Availability	Control, Availability, Integrity, Confidentiality
Access Control	Strict network authentication and access policies	Strict physical access but simple network device access
Cyber Criminal Motivation	Monetization	Disruption
Threat Protection	Shutdown Access	Isolate but keep operating
Maintenance	Multiple support sources, 3-5 yrs. Component life; modular, accessible components, IT staff or contracted service	Single vendor support, 15-20 yrs. component life, remote components, hidden access. No full-time dedicated IT staff.
Upgrades	Frequent patches and updates; Automatically pushed during uptime.	Carefully planned and tested; scheduled during downtime or not done at all.
Primary Players	CIO and IT	Engineers, technicians, operators and managers.

Everyone has a (NICE) role to play

Asset Owners
Operate and Maintain
Site Specific Systems

Integrators/Asset Owners
Engineer and Integrate COTS
into Site Specific Systems

Suppliers
Design and Manufacture
COTS Control Systems

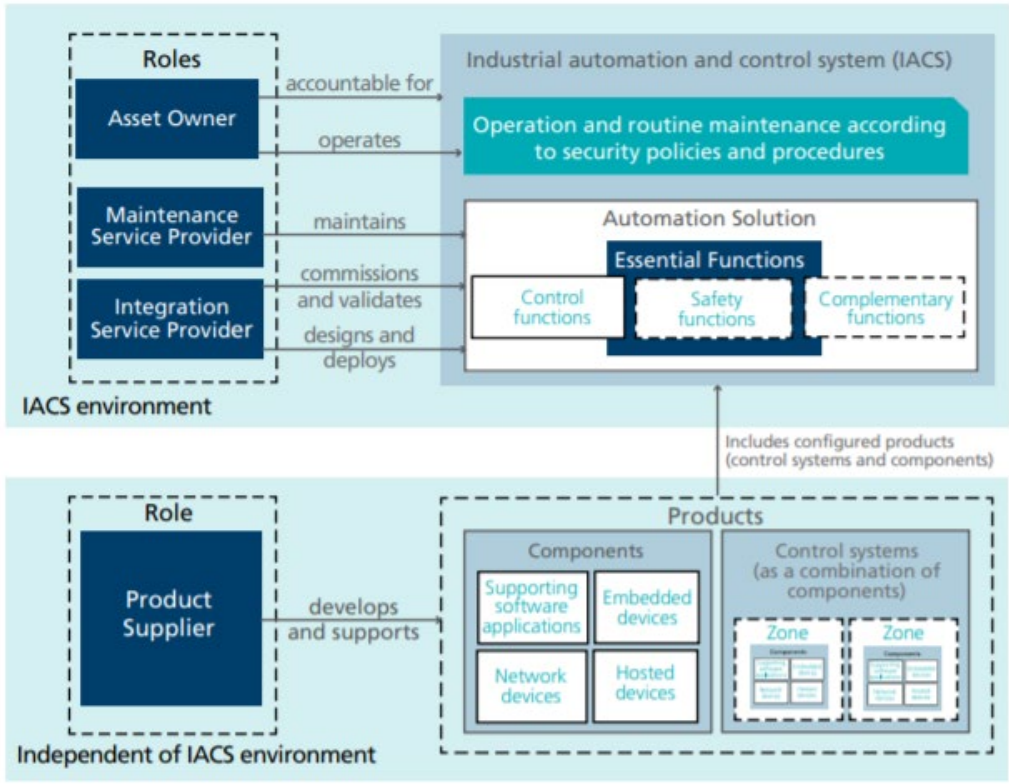
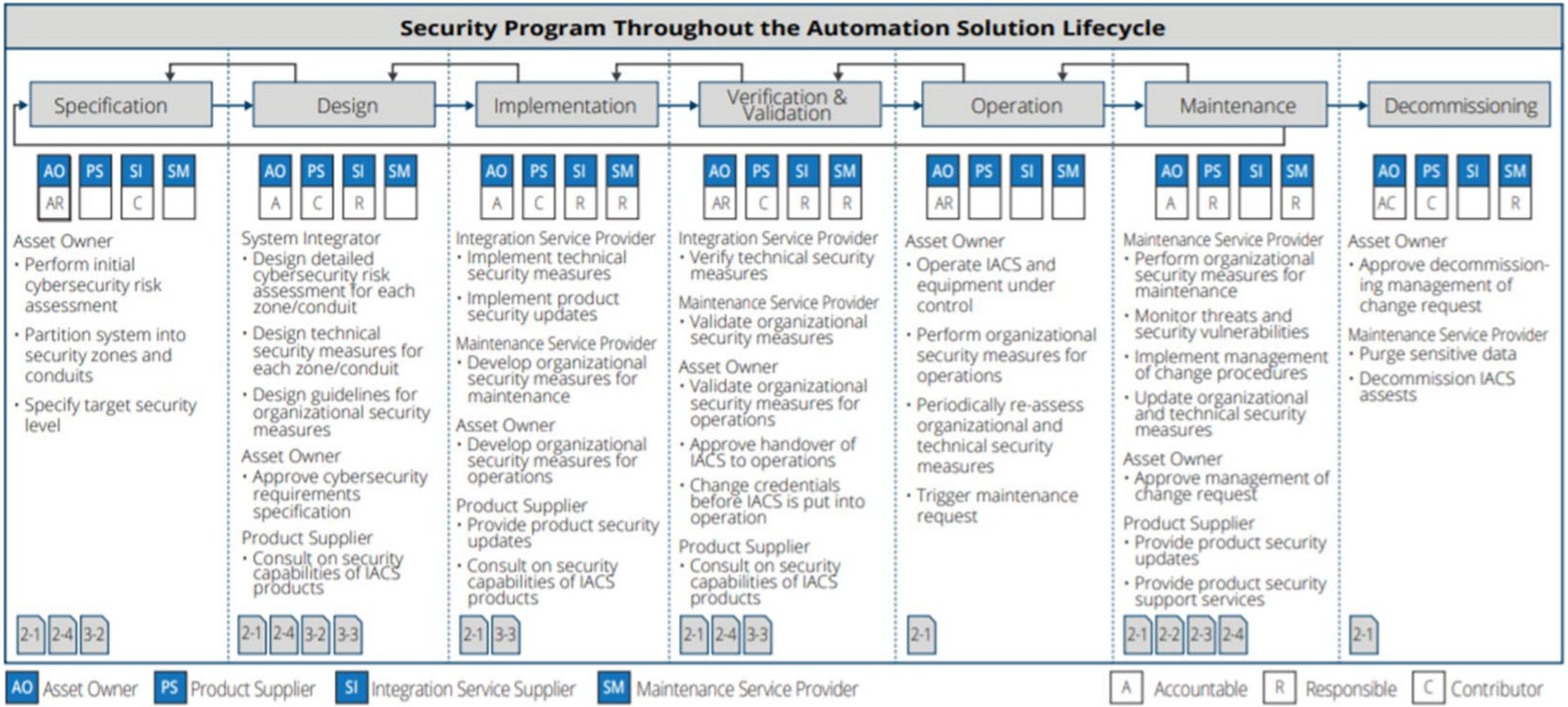


Figure 4: Roles, Products, Automation Solution, and IACS

Security Lifecycles in the ISA/IEC 62443 Series *link*

Security Program Throughout the Automation Solution Lifecycle

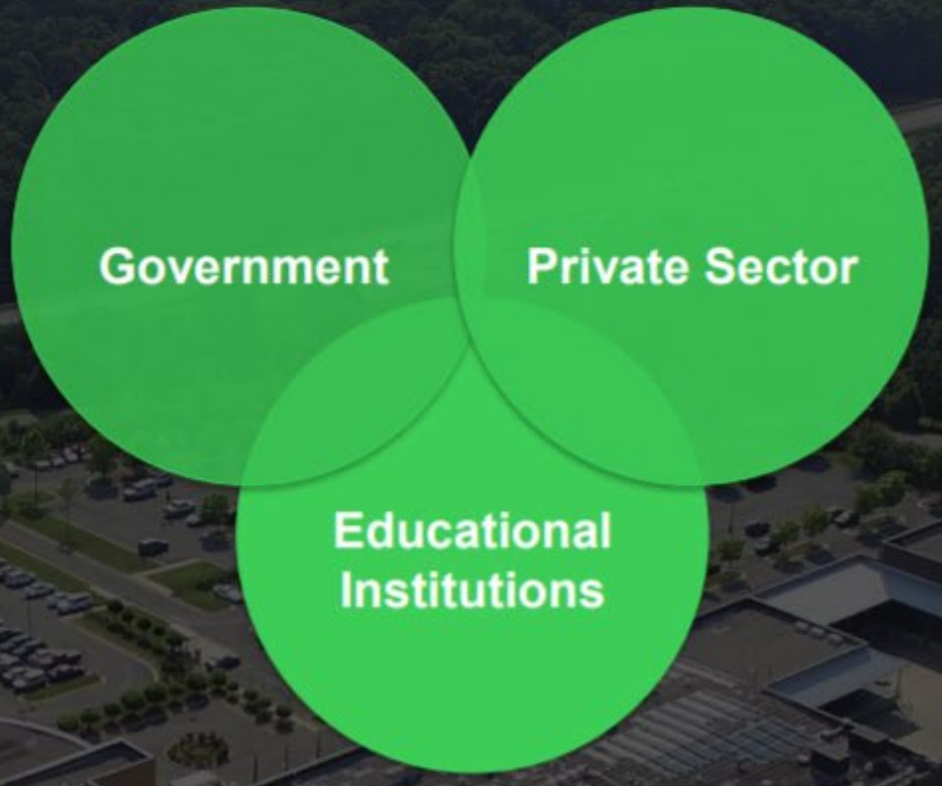


Reference: ***Security Lifecycles in the ISA/IEC 62443 Series*** *link*

The labor solution: Partnerships

A local approach to labor through partnerships between the government, private sector, and educational institutions …

… enabling rapid job skilling as well as a steady stream of qualified, talented labor in communities nationwide.



Life Is On | Schneider Electric

Q & A

Idaho State University

Foundations of Industrial Cybersecurity Education and Training

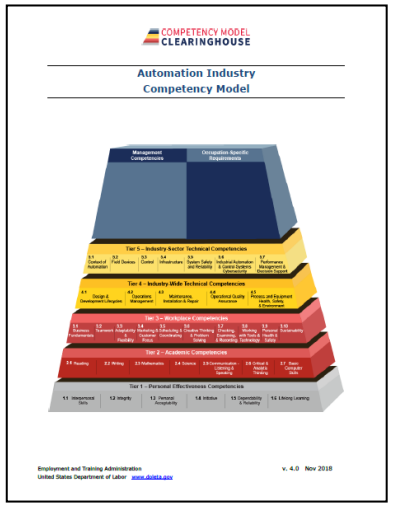
Sean McBride

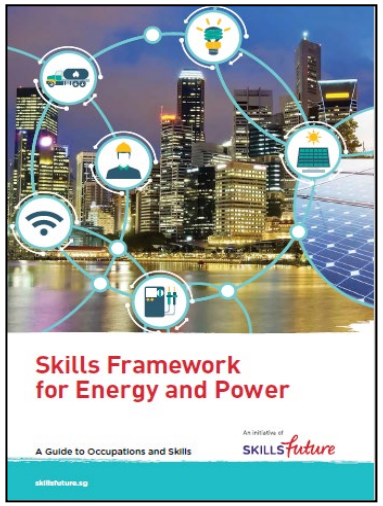
ROAR

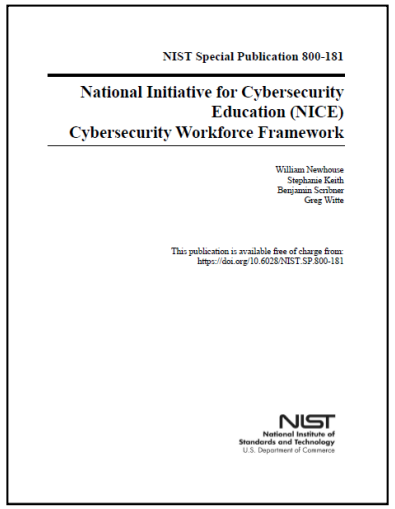
Key Differences

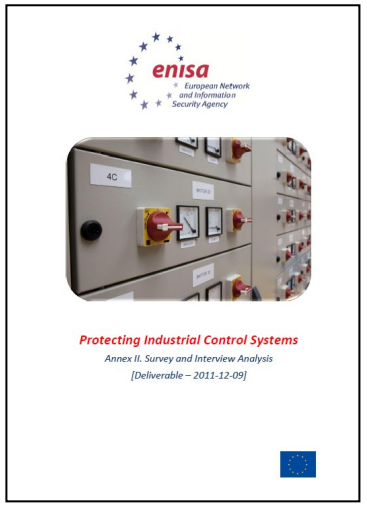
	IT	OT
Being controlled	Data	Physics
Measurement	Bits & bytes	Temp pressure, level, flow
Lifecycle	System lifecycle	Plant lifecycle
Consequences	Competitive disadvantage Embarrassment Financial loss	Product damage Loss of life Environmental release
Desired system characteristics	Confidentiality Integrity Availability	Safety Reliability Controllability
Educational background	Computer Science Information Systems Cybersecurity	On the job Career & Technical Education Electrical Engineering
Reporting chain	ISO CISO CIO	Shift Supervisor Plant Manager COO
Managerial Accounting	Cost center	Profit center

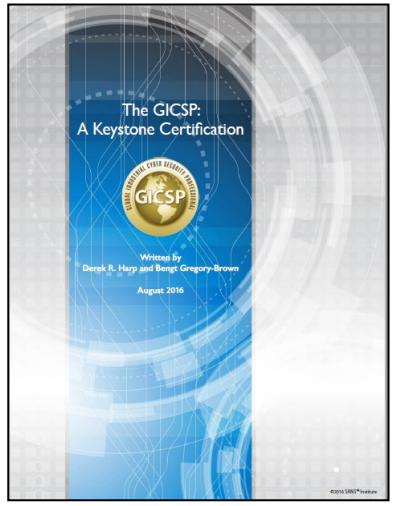
Searching for a standard

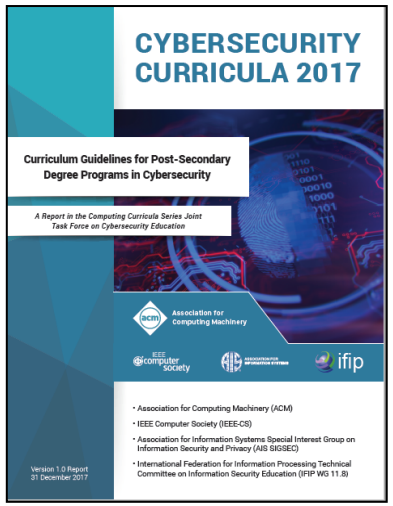


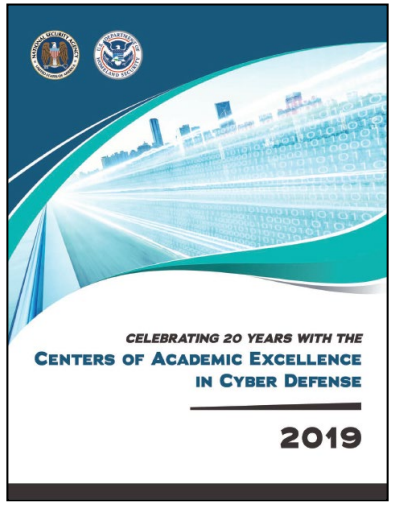












What would we expect of a standard?

- Address industrial cyber
- Clearly differentiate industrial
- Consensus-based
- Qualified participants
- Publicly available
- Includes work roles
- Includes tasks
- Includes knowledge
- Includes sector-specific content
- Evidence of empirical validation

Current Results

KEY ROLES OF THE TEAM

MANAGER
Direct and oversee industrial cybersecurity program.

ENGINEER
Design safe and secure industrial systems.

ANALYST
Synthesize threat and vulnerability information.

TECHNICIAN
Assure security and safety of ICS operations.

RESEARCHER
Identify new vulnerabilities to achieve kinetic consequences.

Current Results

Industrial and Cybersecurity Knowledge Domains

Industrial Knowledge

- Industrial operations
- Instrumentation and control
- Equipment
- Communications
- Safety
- Regulation

+

Cybersecurity Knowledge

- Data
- Software
- Component
- Connection
- System
- Human, organizational and societal

Idaho State University

Current Results

Industrial knowledge domain content:

Industrial operations and processes: industry sectors, professional roles and responsibilities in industrial environments, engineering diagrams, process types, plant lifecycle.

Instrumentation and control: sensing elements, control devices, programmable control devices, control paradigms, programming methods, process variables, data acquisition, supervisory control, alarms, engineering laptops/workstations, data historians.

Equipment under control: motors/generators, pumps, valves, relays, generators, transformers, breakers, variable frequency drives.

Industrial communications: reference architectures, industrial communications protocols, fieldbuses.

Safety: electrical safety, personal protective equipment, safety/hazards assessment, safety instrumented systems, lock-out tag-out, safe work procedures, common failure modes for equipment under control.

Regulation and guidance: presidential/executive orders, NIST SP 800-82 R2, IEC 62443, NERC CIP.

Common weaknesses: indefensible architectures, unauthenticated protocols, unpatched and outdated hardware/firmware/software, lack of training and awareness among ICS-related personnel, transient devices, third-party access.

Defensive technologies and approaches: firewalls, data diodes, independent sensing and backhaul, ICS network monitoring, cyber-informed engineering, cyber process hazards assessment, cyber-physical fail-safes, awareness and training for ICS-related personnel.

ROAR

Idaho State University

WHAT DOES YOUR INDUSTRIAL CYBERSECURITY TEAM **NEED TO DO?**

MANAGER

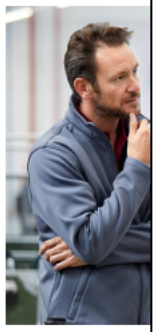
An Industrial Cyb
cybersecurity for
continuously wit

MANAGER PRIM

- Prioritize effort
- Understand re
- Obtain and ma
- Build the team
- Run and impro

Qualifications and

- Master of Busine
- Project Manage
- Information syst
- Licensed Profes
- Industrial cyber



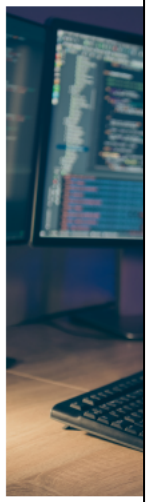
Building An Industrial Cybe

RESEARCHER

The Industrial Cybersecurity Researcher works to increase detailed knowledge about ways an industrial cyber-
protected. The r
and often works
standards for cla

RESEARCHER

- Describes and
- Designs and c
- Discovers vuln
- Develops adve
- Recommends
- Documents ar



Building An Industrial Cyb

ANALYST

The Industrial Cybersecurity Analyst works among enterprise cybersecurity personnel to contextualiz
environment
options, and
perspective

ANALYST P

- Stays abrea
relevant to
- Dissects ar
- Collects in
- Synthesize
- Analyzes th
consequen
environme
- Produces a
- Proposes r

Building An Industrial

TECHNICIAN

The Industrial Cybersecurity Technician works among plant operations personnel to assure safety, reliabi
monitoring, t

TECHNICIAN

- Maintains I
security pu
- Reviews ar
- Updates IC
during stop
- Maintains b
- Maintains a
environme
- Securely im
equipment

Building An Industrial

ENGINEER

The Industrial Cybersecurity engineer works within the engineering department to design and create systems, processes and procedures that maintain the safety, reliability, controllability and security of industrial systems in the face of intentional and incidental cyber events. Interfaces with Chief Information Security Officer, plant managers and industrial cybersecurity technicians.

ENGINEER PRIMARY TASKS

- Direct creation of industrial systems inventory and model for cybersecurity purposes
- Design physical failsafes to counteract potential cybersabotage
- Advise development and operation of security operations center relative to the industrial environment
- Recommend security techniques, technologies, and approaches for adoption in industrial environment
- Create cybersecurity inspection and test procedures for industrial systems
- Review industrial system engineering plans and documentation for cybersecurity concerns
- Review proposed cybersecurity policies and procedures related to industrial environments; and equipment and software based on cybersecurity criteria
- Optimize industrial system designs for security effectiveness and efficiency.

Qualifications and Certifications

- Master of Science in Electrical, Mechanical, or Computer Engineering
- Licensed Professional Engineer
- Industrial automation
- Information systems security.

HIRING GUIDANCE

- ☐ **Most important role on the industrial cybersecurity team and may require skilled recruitment.**
- ☐ Requires 5 or more years of engineering experience in each of industrial automation, information technology, and cybersecurity.
- ☐ Demonstrates expert level familiarity with industrial safety and cybersecurity events including detailed root-cause analysis.
- ☐ Deep engineering experience and expertise and is capable of considering the mindset of a well-resourced adversary.
- ☐ Demonstrates proficiency in systems thinking and systems design, including production of policies, diagrams, drawings, and specifications.
- ☐ *For Team: One or two per facility or per type of facility.*

Building An Industrial Cybersecurity Workforce: A Manager's Guide 8

ROAR

Idaho State University

Mission

To provide world-class leadership in
infusing tomorrow's engineering professionals with critical cybersecurity competencies

Degree in
Engineering Technology

- Instrumentation
- Electrical
- Mechanical
- Nuclear Operations
- Diesel Power
- Robotics

+

Courses in
Industrial Cybersecurity

- IT-OT Fundamentals
- Networking
- Security Design for CPS
- Risk Management for CPS
- Network Security for CPS
- Critical Infrastructure Defense

+

Courses in
Operations Management

- Ops & Production Mgmt
- Project Management
- Organizational Behavior
- Informatics & Analytics
- Information Assurance
- Business Statistics

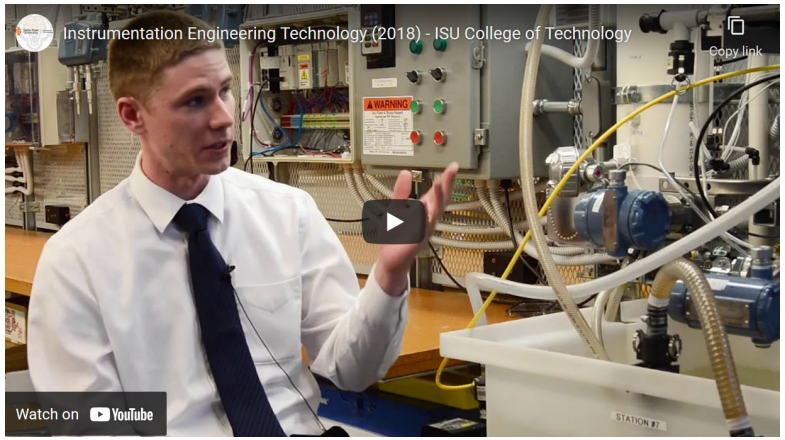
ROAR

Idaho State University

Incoming Programs

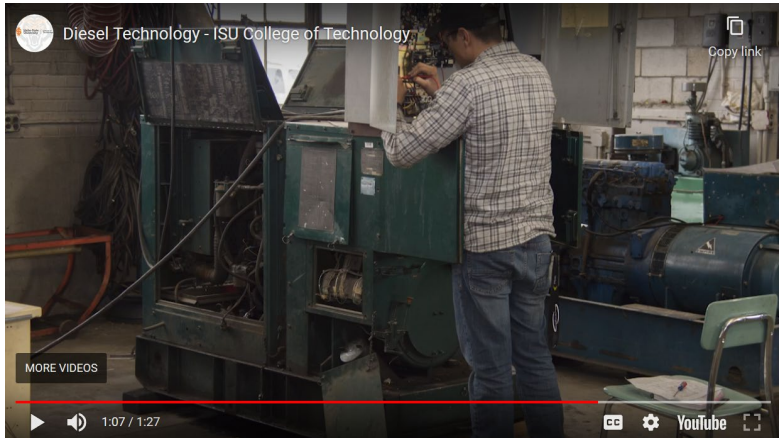
Mechanical Engineering Tech

Electrical Engineering Tech



Instrumentation Engineering Tech

Information Technology Systems



Diesel Power Systems

Nuclear Operations

ROAR


INOVAR ON Campbell Scientific
Varian Clear Water Paper
Wunderlich-Malec
Chevron
Heinz

https://inl.gov/icscop/

Q & A

Thank You for Joining Us!

Upcoming Webinar: The Information Technology Workforce and Skills for the Future

When: September 15, 2021 from 2-3PM ET

Register: https://nist-secure.webex.com/nist-secure/onstage/g.php?MTID=e4b2fb325e45250e24dadb39090f5a91c

nist.gov/nice/webinars

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION