Global Industrial Cyber Security Professional – GICSP
A certification for Engineers, ICS Security Professionals, and ICS Technology Specialists

www.sans.org/event/north-american-ics-scada-summit-2014

SANS ICS Resources
Control System Poster ▪ Webcasts ▪ ICS NewsBites ▪ STH Training Demo
Follow us on Twitter @SANSICS

www.sans.org/industrial-control-systems/resources/
This is not “another day in the data center” for IT professionals certification!

This is **Industrial Cyber Security**
- Engineers
- ICS Security Specialists
- OT Support Specialists

Bring your PPEs and let’s take cyber security to the plant floor!
What is the GICSP?

• The GICSP is a new certification that focuses on the **foundational knowledge** for professionals securing critical industrial infrastructure assets.

• The GISCP has been developed for engineers, control system support, and security professionals who work in environments addressed by commonly accepted standards related to control system and automation security, including ISA-99/IEC 62443 and NERC CIP.

• Holders of the GICSP will demonstrate a **globally recognized** level of competence that defines the architecture, design, management, risk and controls that assure the security of critical infrastructure.

• The GICSP is **the “bridge”** to bring together IT, engineering and cyber security professionals to achieve security for ICS from design through retirement.
What is the GICSP?

• This certification establishes a **base level** of knowledge and understanding for the diverse set of professionals who engineer, operate, secure, or support control systems and share responsibility for the security of these environments.

• This certification is applicable to control system owner/operators across all sectors, ICS vendors, integrators, and support organizations, and professionals that have access to production industrial control systems from nuclear power plant systems to building automation.

• The GICSP is expected to be adopted on a **global** basis as a gateway certification for critical infrastructure-industrial control system professionals.
Why Would Someone Want to be GICSP Certified?

To demonstrate an appreciation and understanding of the important issues involved in addressing ICS security concerns and challenges while assuring the safety and reliability of the ICS, industrial process, people, and environment.
Who Would Not Want to be GICSP Certified?

• A general IT security professional, corporate IT system analyst or resources, or an engineer that is not responsible for the administration and management of your infrastructure/plant's control system(s).

• If you possessed this certification you would not use it to represent an ability to perform any specific ICS security function, procedure, or role nor does it reflect an ability to perform work on a specific ICS technology/implementation.
GICSP Examination Highlights

• Examination – **115** items (100 scored/15 non-scored “beta” questions); time limit of **three hours**
• Test delivery is computer based and proctored by Pearson VUE at over **4000 global** testing centers
• Certification is valid for **4 years**; continuing professional education requirements are consistent with GIAC standards see [www.giac.org/renewal](http://www.giac.org/renewal)
• Certification Examination is available **November 21, 2013**
The GIAC program is accredited under the IEC/ISO/ANSI 17024 quality standard for certifying bodies and we are seeking approval for the GICSP.
GICSP & Industrial Automation and Control Systems

- **Cyber Security Certifications**
- **GICSP**
- **Standards Focused Certifications (ISA-99)**
- **Automation Certifications**

**Functional certification aligned with performing industrial cyber security**

“complimenting existing important and valuable certification efforts”
Hybrid Skill-set Needed

**Engineering & IACS (Security)**
- Industrial domain architecture
- Plant automation systems
- Industrial Cyber Security
- Risk management (with a focus on IACS)
- Process & Equipment Safety & Security
- FAT/SAT

**IT & OT Support**
- Network infrastructures
- Operating Systems
- IT infrastructure design
- Systems’ Security Lifecycle
- Information Assurance

**Cyber Security**
- Cyber Security on a conceptual level
- Cyber Security Standards
- Computer Network Defense
- Incident Response and Handling
- Root Cause Analysis

**Industry, company and professional standards**
- Sector Standards & Practices
- Most common regulations
- Most common risk management methodologies
Job Competence Profile

IT / Cyber Security

- IT Architecture
- IT Audit and Compliance
- Incident / Threat / Vulnerability Management
- Business Risk Management

Engineering

- IACS Integrity & Security
- SIS & Safeguarding
- Process Automation Systems Engineering
GICSP = Global Collaboration

The GICSP is being developed and guided by a Steering Committee of leaders from major industrial companies, advisors, and suppliers from around the world. It includes members from the following companies/organizations:

- BP, Chevron, Pacific Gas & Electric, Shell, Saudi Aramco, ABB, Emerson, Invensys, Rockwell Automation, NIPSCO, KPMG, WurldTech, ERNCIP(JRC), TNO, SANS Institute, GIAC

SME group (next to ones above):

- Yokogawa, Schneider Electric (Telvent), Cimation, Cigital, Red Tiger Security, Honeywell

The consortium of companies established collaboratively an open body of knowledge for the topic of ICS Security from which a certification framework and associated competency training programs could be established.
GICSP Subject Matter Experts

Team including experts from ICS vendors, integrators, end-users and researchers: (job titles involved)

- Process control engineer
- Process control network cyber security engineer
- PCD IT security engineer
- Principal security architect
- Security architect
- ICS/SCADA security manager
- Regional technical authority
- Senior ICS/SCADA security consultant
- Head of process control security
- Director of reliability & security
- Senior security engineer
- Director of technology
Collaborators
“Managing cyber risk is an issue effecting the entire energy industry ecosystem and in order to effectively implement and sustain security controls on industrial infrastructure, we’re all reliant on a complex ecosystem of people (system vendors, project engineering contractors, process operators, IT service providers and maintenance/support personnel) who require a blended set of IT/Engineering/Cyber Security competencies - a skill-pool which is unique and scarce in today’s marketplace. Developing and maintaining this workforce can be a challenge for any one organization and that is why we support this collaborative effort to establish a community developed body of knowledge and certification program for industrial cyber security. ”

Tyler Williams
Manager, PCD IT Security Solutions at Shell and Chair of the industry consortium
"Protecting industrial control and automation systems from constantly evolving cyber security threats is a very challenging task shared by all involved stakeholders. The foundation for any successful program is the people involved in developing, designing, operating and maintaining these systems. We are therefore proud to be part of the creation of the first professional certification program for industrial control system cyber security. The effort did not only result in a certification program that will advance workforce development but it is also an industry commitment to improve the security of our critical infrastructure."

Markus Braendle
Group Head of Cyber Security
ABB, Zurich, Switzerland
# Industrial Cyber Security Domains

**GICSP Certification Objectives:**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A.</strong></td>
<td>ICS Architecture</td>
</tr>
<tr>
<td><strong>B.</strong></td>
<td>ICS Security Assessments</td>
</tr>
<tr>
<td><strong>C.</strong></td>
<td>ICS Security Monitoring</td>
</tr>
<tr>
<td><strong>D.</strong></td>
<td>Configuration/Change Management</td>
</tr>
<tr>
<td><strong>E.</strong></td>
<td>Disaster Recovery and Business Continuity</td>
</tr>
<tr>
<td><strong>F.</strong></td>
<td>Incident Management</td>
</tr>
<tr>
<td><strong>G.</strong></td>
<td>ICS Security Governance and Risk Management</td>
</tr>
<tr>
<td><strong>H.</strong></td>
<td>Physical Security</td>
</tr>
<tr>
<td><strong>I.</strong></td>
<td>Industrial Control &amp; Automation Systems</td>
</tr>
<tr>
<td><strong>J.</strong></td>
<td>ICS Modules and Elements Hardening</td>
</tr>
<tr>
<td><strong>K.</strong></td>
<td>Cyber Security Essentials for ICS</td>
</tr>
<tr>
<td><strong>L.</strong></td>
<td>Access Management</td>
</tr>
</tbody>
</table>
# GICSP Objectives – Knowledge & Application of the following:

## A. ICS Architecture
1. Field device architecture (e.g., relays, PLC, switch, process unit)
2. Defense in depth (e.g., layered defense, IDS sensor placement, security system architecture, virtualization)
3. External network communications (e.g., access points into SCADA/ICS systems, VPNs, vendor/third party access points, mobile devices, secure remote access, RDP, PC Anywhere, jump servers)
4. Network protocols (e.g., DNS, DHCP, TCP/IP)
5. Network segmentation (e.g., partitioning, segregation, zones and conduits, reference architectures, network devices and services, data diodes, DMZs, test and development environments)
6. Wireless security (e.g., WIFI, wireless sensors, wireless gateways, controllers)
7. Communication medium (e.g., VSAT, RF, cell, microwave)
8. Industrial protocols (e.g., modbus, modbus TCP, DNP3, Ethernet/IP, OPC)

## B. ICS Security Assessments
1. Security assessment (e.g., risk, criticality, vulnerability, attack surface analysis, supply chain)
2. Penetration testing and exploitation
3. Security testing tools (e.g., packet sniffer, port scanner, vulnerability scanner)
4. Device testing (e.g., communication robustness, fuzzing)

## C. ICS Security Monitoring
1. Security monitoring and logging
2. Event monitoring and logging
3. Network monitoring and logging
4. Archiving

## D. Configuration/Change Management
1. Change management, baselines, equipment connections, and configuration auditing
2. Patches (preparation, approval, scheduling, remediation, mitigation)
3. Software reloads and firmware management
### E. Disaster Recovery and Business Continuity
1. System backup (e.g., security, data sanitization, disposal, redeploying, testing backups, operational procedures)
2. Site redundancy (e.g., hot site, off-site backup)
3. System restoration (e.g., full, partial, procedures, spares)

### F. Incident Management
1. Incident response (e.g., recording/reporting, forensic log analysis, containment, incident response team, root cause analysis, eradication/quarantine)
2. Incident recognition and triage (e.g., log analysis/event correlation, anomalous behavior, intrusion detection, egress monitoring, IPS)
3. Incident remediation/recovery

### G. ICS Security Governance and Risk Management
1. Security policies and procedures development (e.g., exceptions, exemptions, requirements, standards)
2. Risk management (e.g., PHA/hazop usage, risk acceptance, risk/mitigation plan, operational impact assessments)
3. Global security standards, practices, and regulations (i.e., IEC/ISA 62443, NIST 800-82, ISO 2700xx, compliance gap analysis)
4. Security life cycle management (e.g., acquisition and divestiture, procurement, commissioning [e.g., secure deployments], maintain, decommission)

### H. Physical Security
1. Physical security (e.g., locked cabinets, locked switches, barbed wire, facility access control, surveillance, physical individual)
# GICSP Objectives – Knowledge & application of the following:

## I. Industrial Control Systems

1. Basic process control systems (e.g., RTU, PLC, DCS, SCADA, metering/telemetry, ethernet I/O, buses, Purdue (ISA 95))
2. Safety and protection systems (e.g., SIS, EMS, leak detection, FGS, BMS, vibration monitoring)
3. Critical infrastructure sector and ICS applications (e.g., chemical, waste water, water, electricity, oil and gas, manufacturing, transportation)

## J. ICS Modules and Elements Hardening

1. Antimalware implementation, updating, monitoring, and sanitization
2. End point protection including user workstations and mobile devices (e.g., anti-virus, white listing)
3. Network security/hardening (e.g., switchport security)
4. Application security (e.g., database security)
5. Removable media (e.g., USB device security, optical media, external drives)
6. OS security (unix/linux, windows, least privilege security, virtualization)
7. Embedded devices (e.g., PLCs, controllers, RTU, analyzers, meters, aggregators, security issues, default configurations, firmware)

## K. Cybersecurity Essentials for ICS

1. Attacks and incidents (e.g., man in the middle, spoofing, social engineering, denial of service, denial of view, data manipulation, session hijacking, foreign software, unauthorized access)
2. Security tenets (e.g., CIA, non-repudiation, least privilege, separation of duties)
3. Threats (e.g., nation states, general criminals, inside and outside malicious attackers, hacktivists, inside non-malicious)
4. Availability (e.g., health and safety, environmental, productivity)
5. Security awareness programs (e.g., employees/management, sensitive data identification, protecting information)
6. Cryptography (e.g., encryption, digital signatures, certificate management, PKI, public versus private key, hashing, key management, resource constraints)
GICSP Objectives – Knowledge & application of the following:

<table>
<thead>
<tr>
<th>Access Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. User access management (e.g., user accounts, service accounts, temporary</td>
</tr>
<tr>
<td>accounts, default accounts, guest accounts, account expiration, access control</td>
</tr>
<tr>
<td>list, access reconciliation)</td>
</tr>
<tr>
<td>2. Directory services (e.g., active directory, LDAP)</td>
</tr>
<tr>
<td>3. Access control models (e.g., MAC, DAC, role-based)</td>
</tr>
</tbody>
</table>

![Diagram](image)
Global Industrial Cyber Security Professional

The GICSP is the newest certification in the GIAC family and focuses on the foundational knowledge of securing critical infrastructure assets. The GICSP bridges together IT, engineering and cybersecurity to achieve security for industrial control systems from design through retirement.

This unique vendor-neutral, practitioner focused industrial control system certification is a collaborative effort between GIAC and representatives from a global industry consortium involving organizations that design, deploy, operate and/or maintain industrial automation and control system infrastructure. GICSP will assess a base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments.

GICSP will be leveraged across industries to ensure a minimum set of knowledge and capabilities that an IT, Engineer, and Security professional should know if they are in a role that could impact the cybersecurity of an ICS environment.

The GICSP will be available this fall. Pre-registration will begin in August.

Training for GICSP

- SANS ICS410 Security Essentials maps to the GISCP
- Offered in a live instructor led class or on-line, computer based training (On-site group training will be subject to instructor availability)
  - Training includes lab simulations which support real-life application of tools and techniques to support concepts tested by the GICSP
Curriculum Road Map

Advanced & Role-based ICS Training & Future Certifications:

- **HOSTED**
  - Critical Infrastructure and Control System Cybersecurity
  - Pentesting ICS and Smart Grid
  - SCADA Security

- **ICSTBD**
  - Future SANS ICS focused class TBD

Foundational Training & Certification:

- **ICS410**
  - ICS/SCADA Security Essentials
  - GIAC: GICSP

- **SEC301**
  - Intro to Information Security
  - GIAC: GISP

Security awareness & learning:

- **STH End User**
  - These 25 modules cover the broadest set of users and a wide range of cybersecurity awareness topics

- **STH Utility**
  - These 7 modules focus on cybersecurity awareness and NERC CIP training program needs for portions of the electricity industry in North America

- **STH Engineer**
  - These 14 modules focus on individuals who support engineer, or interact with automation and control systems
What Students are Saying about ICS410

• “This is a great course that distinguishes the challenges and integration points for ICS and Traditional IT security posture. The instructors provide in-depth real world knowledge and experience to the material to make it actionable within the attendees corporate environment.” Rob Oates – GDIT

• “Provides good baseline info for both IT and OT SME’s.” Daryl Haegley – DOD

• “This is a great intro course for anyone taking security seriously in an ICS environment.” Shaun Curry – SMSD
See you in the control room!