The GICSP: A Keystone Certification

Written by
Derek R. Harp and Bengt Gregory-Brown

August 2016

Contents

The GICSP

The Global Industrial Cyber Security Professional (GICSP) certification was conceived in the winter of 2013 because managers in multiple industries shared a growing problem. Their common challenge was delaying desired progress while rapid changes were outpacing current efforts. Technology and business forces had for years been driving IT-based technologies into industrial and automation environments (often referred to as operational technology or OT), erasing divisions that had granted a certain degree of protection and calling for security practitioners to address new and complex vulnerabilities. The demands to build integrated teams, combining automation expertise with cyber security knowledge, capable of securing the world's automation systems were growing.

The convergence of IT and OT, more than a decade old at that point, presented numerous challenges to industry, perhaps chief among them its rate of progress. Industrial control system (ICS) assets have always been large investments with life cycles of several years to decades in length. Operators of industrial equipment have historically gone through lengthy training and certification programs to ensure the safety of personnel, company resources and, in some cases, the public. The use of unauthenticated protocols and increased adoption of traditional IT infrastructure (such as TCP/IP) for controlling, monitoring, and logging of these devices, and communication between them, created new attack surfaces. This increased exposure to both malicious action and accidental misconfigurations. The trend to interconnect and interoperate was moving rapidly, while the workforce was struggling to adapt. Moreover, this rate of change was accelerating, and there was no coordinated effort to address the shortage of expertise on the horizon.

The problem was multi-faceted, extending a known technology (IP-based networking) into a second, distantly related one (industrial control/automation equipment). The skills and experiences of practitioners in either field could not fully prepare them to tackle the issues. Not only had there long been a division between IT and OT,[1] but the convergence was uncovering unanticipated design considerations. The creation of a new and interdisciplinary security resource was needed, one that could apply relevant networking tools and techniques of IT with a thorough understanding of the special considerations of OT environments.

In addition, a means to evaluate the capabilities of these resources was also called for. It was recognized that a small number of individuals worldwide had, through experience, developed relevant and valuable expertise in this area, but no standard existed to use as a measure, nor one to guide the development of additional personnel.

[1] Operational networks are deterministic. Normal network traffic can be predicted, as it consists of machine and sensor communications taking place according to scheduled operations. Information, business or general-purpose computer network traffic is non-deterministic; the amount and types of traffic shift in response to unforeseeable factors. The use of tools from the latter environment in the former introduces potential timing delays and communication errors. In the operational space, this has the documented potential to cause equipment performance issues, risking the safety of personnel, materiel and the public. Due to this and other factors, IT security personnel have often been excluded from access to OT networks.

The GICSP
(CONTINUED)

Pieces of this puzzle had been evident to business leaders in ICS customer and vendor enterprises for some time, but the establishment of a solution had not been forthcoming. Discussions among numerous parties led to a shared view of the problem and the outline of what needed to be accomplished. In particular, representatives from Shell, Chevron, Saudi Aramco, BP, Rockwell Automation, Yokogawa Industries, Emerson, ABB, Cimation and the SANS Institute came together and laid out the framework of what would become the GICSP. This group, the members of which would establish the GICSP steering committee, agreed on these objectives:

- Provide a common language spanning industries, roles and backgrounds to enable ICS security.
- Establish an essential baseline of ICS security knowledge for employer evaluation.
- Provide knowledge applicable to ICS security projects and programs.
- Provide the springboard for ICS security training programs.
- Create a standard for measuring corporate capability.
- Provide a measure to differentiate and recognize those who can join the team.
- Create tools to measure and accomplish ICS security regulatory compliance
- Create an accredited, international, cross-industry community of people developing a profession to advance the state of ICS security.

GIAC and ANSI Involvement

The Global Information Assurance Certification (GIAC) administers the GICSP. Testing (the "challenge exam") content and design undergo a rigorous process of development and ongoing review and improvement in accordance with the requirements of the American National Standards Institute (ANSI), a globally recognized standard of excellence for testing and certification.

The GICSP certification is ANSI accredited under ANSI/ISO/IEC 17024 and requires Continuing Professional Education credits every four years to renew certification holder status.

Goals of the GICSP

Each of the following sections explains one of the goals of the GICSP certification.

1. Provide a Common Language Enabling ICS Security Across Industries, Roles and Backgrounds

The basis of every multi-disciplined effort is the ability of its members to communicate with shared understanding. Because the cyber security discipline practitioners come from diverse educational and career experiences, this has been an obstacle. Electrical engineers, software programmers, network administrators, equipment operators and information system managers, to name only a handful of relevant backgrounds, use similar terms in dissimilar ways in their work. This is true both for many technical terms and for broader language use. Ensuring that the individuals working to secure control system assets would understand one another had to be the keystone component of building the new certification.

The educational purpose of a language is the acquisition and sharing of knowledge. With the communication tool of a shared terminology in hand, ICS defenders become able to advance not only their own skills but their profession as a whole by sharing their research and experience in various media. A foundation of every profession is the ability of its members to communicate with one another clearly and effectively, and the common language established by the GICSP establishes this foundation.

Certificates vs. Certifications

Certifications require holders to demonstrate specific knowledge, skills and competencies. Certification also requires ongoing work and/or training to maintain it. Failure of the holder to fulfill ongoing or updated requirements can result in revocation of rights to bear the certification. Certification eligibility requirements may include agreement to follow specific ethical or behavioral guidelines. Certification programs are ideally administered by neutral third parties rather than training providers

Certificates verify that holders have successfully completed one or more training and/or testing events. Certificates have no eligibility requirements. Certificates have no ongoing maintenance requirements or expiration dates because they verify the holder met the requirements at a single point in time. Certificates are generally issued by training providers.

2. Establish an Essential Baseline of ICS Security Knowledge for Employer Evaluation

Enterprises depending on control and automation systems rely on four pillars for their continued success and survival. Equipment, software and process are inarguably crucial to accomplish their purposes, but it is the fourth pillar, their people, that makes the rest work. This is true not only in an operational sense, of course, but in the broader task of applying the technology. Their employees and contractors may install the equipment and software, and they certainly operate and maintain them. Those same people perform the processes that define operational outcomes. The selection of components, the design of the processes and the architecture of the overall systems fall to these human resources as well. Good leaders know that having good people will see a team through places that even the best of technology won't. Further, every profession has specializations and continual growth of its field, and employers need to identify practitioners with a core set of skills relevant to their specific needs.

Fully assessing candidates for a position can be a lengthy process, and with the stakes inherent in ICS security thoroughness a must, having a litmus test to narrow the field of possibilities is valuable and expedient. The GICSP certification provides that function in requiring automation professionals and security practitioners to demonstrate both the knowledge and persistence to demonstrate competency.

Goals of the GICSP
(CONTINUED)

3. Provide Knowledge Applicable to Management and Oversight of ICS Security Professionals and Programs

The best leaders recognize the abilities and limitations of their individual resources and work to achieve their team goals with those considerations in mind. Much ICS knowledge is highly specific to the equipment with which individuals have trained and worked, and learning what those individuals can do beyond the scope of that experience can be a lengthy and costly process. The wide-ranging backgrounds of personnel in the relatively immature ICS security field only complicate this further, with managers often having to compare apples and kiwis.

The GICSP, by establishing a cross-industry baseline, provides a tool to aid managers of ICS security. Whether a team member comes from an IT security background, an ICS network administration career or any other history, their holding a GICSP certification gives their employer a starting point, a grasp on what the person knows and can do. This frame of reference within which to evaluate an employee's potential role on a team is tremendously valuable and can make the difference in hiring new employees or allocating existing ones within a company.

"The need for a baseline reference on the industrial cyber security competencies for the ICS-related jobs was clear to me since our early activities in the Industrial Cybersecurity Center. All the stakeholders from the ecosystem, industrial and cyber security vendors, EPCs and system integrators, industrial organizations and critical infrastructures, consultancy companies, academia, government and public bodies, shared their real need and interest on building and testing the basic capabilities required in their teams to deal with the current industrial cyber security challenges we were all (and still are) facing. At that time, I was sharing all that feedback with the GICSP steering committee, and most of it was incorporated into the certification, resulting in an excellent acceptance of the GICSP from the Spanish-speaking market (as it is shown by the high number of certifications achieved compared to other countries in Europe, Middle East or Asia).

Now that I am working with Booz Allen Hamilton in Middle East (in UAE), I have realized that the situation is quite similar in this region, where GICSP is being well recognized and broadly required by clients for key and strategic projects and positions. Furthermore, having our team members GICSP-certified has provided us with a real advantage in the market, and the clients with the assurance that the industrial cyber security baseline capabilities are present in the team, in addition to the real experience required to execute these type of activities. Based on this, I can anticipate a big increase in the number of GICSP certifications in the UAE and the region during this next year."

—Samuel Linares, Industrial Cybersecurity Sr. Lead Technologist, Booz-Allen Hamilton, and GICSP Steering Committee Founding Member

Goals of the GICSP
(CONTINUED)

4. Provide the Basis of ICS Security Training Programs

Every control system environment is unique, composed of different equipment running different software in different configurations to address different objectives. The GICSP certification program cannot prepare or evaluate preparation for every environment one might work in. It provides the validation that an individual has the foundational knowledge and understanding upon which to build further. It also provides a template for ICS owners to build their own security training programs, which can go deeper into the specifics of their own systems. The shared knowledge and language of GICSP holders enables them to learn from material that would otherwise be incomprehensible to some.

The GICSP certification program goes further in that it provides a framework to guide other entities in designing and improving their own ICS security programs. Significant effort was invested into achieving ANSI[2] accreditation, which required multi-stage review and approval processes of both the material covered in the challenge examination and of the methods of testing. Companies seeking to develop their own security programs are strongly encouraged to incorporate the same considerations of balance and completeness when doing so.

5. Create a Standard for Measuring Corporate Capability

There are many metrics by which a company is called upon to measure itself. Many of those are purely financial- or productivity-oriented and apply to overall success of the corporate entity rather than how well it performs its specific business functions. When it comes to establishing credibility in the service marketplace, however, we look for indicators of actual ability to do a particular thing or set of things, for reasons to place our trust (and our money) in the hands of one provider over all others. Reputations, both of evidentiary record and anecdotal in nature, play a factor in these evaluations, of course, but assurances from a neutral third party that a provider's personnel have confirmed relevant skills is much desired.

"Many of today's industrial control systems rely on network architectures and infrastructures that are commingled with business enterprise systems. NexDefense endorses the GICSP certification because it helps prepare a contemporary workforce to better address cyber security challenges that can impact the ongoing safety, resiliency and operational integrity of control systems used across industry. With more than 1,000 certified practitioners to date, GICSPs around the world are already actively taking action against security risks and threats to systems that make power, move people, deliver clean water, protect national best interests and manufacture the variety of goods and services that society needs, wants and demands."

—Doug Wylie, VP of Product Strategy, NexDefense, and GICSP Steering Committee Founding Member

[2] Further information on ANSI accreditation requirements and processes can be found at www.ansi.org/Accreditation/credentialing/personnel-certification/Default.aspx

This is key to why the GICSP steering committee has always sought to establish the certification as an industry-spanning standard. Just as an IT security provider touts the Certified Information System Security (CISSP®) counts of its team members, companies whose work involves the security of ICS-using clients can and should provide data on the GICSP status of its employees engaged in that work. As the most-widely recognized metric of its kind, the GICSP being held by a company's human resources can be a valuable indicator of their abilities to work competently and effectively in this field. Lacking the certification, estimating their likely performance becomes a more time- (and potentially cost-) intensive exercise in reviewing and evaluating individual work histories. This is why some companies now emphasize the importance of GICSP certification not only internally but also to their present and potential clients.[3]

6. Create Tools to Measure and Accomplish ICS Security Regulatory Compliance

The development of safety and security regulation is primarily a reactive process. Invention and experimentation, driving factors of business growth, thrive in open and unrestricted environments, and the optimal role of regulatory restraints is that of reducing or eliminating harm done to individuals and societies by the outcomes of those activities. Regulatory safety requirements have a long-established history in many industries, limiting the freedom of businesses to choose how to dispose of their toxic by-products, for example, or mandating the physical clearances around power lines. Outside of government and military settings, security regulations are a much more recent phenomenon. Just as with physical safety, however, the preponderance of their growth has occurred in response to incidents of loss or harm. Much of this has involved malicious or accidental misuse of information systems.

Control systems increasingly connect the digital and physical worlds, so these systems often have to answer to both safety and security regulations. The amount and complexity of these regulations is rising at an accelerating pace as both governmental and industrial entities work to manage the risks created by the technological developments and the demand for individuals with expertise rises apace. Many regulations are technical in nature and highly specific as to their applicability, and both sides of the regulatory process require people who comprehend the devices and processes involved. Regulators need to understand the implications of evolving technology, as well as how business will be impacted by the documents they author. Enterprises must understand the regulations in order to implement them and maintain compliance while keeping business operations running.

Large-scale events involving the private information of millions of individuals or impacting infrastructure deemed critical to the continued operation of a nation state's society and/or economy[4] have encouraged the creation of laws intended to reduce the recurrence likelihood of similar events.[5] Entities subject to these regulations may be required to make physical changes to their work environments, modify

[3] Yokogawa press release of May 8, 2015, see Appendix D, www.yokogawa.com/pr/topics/2015/pr-topics-2015-0508-02-en.htm

[4] Q.v. Critical Infrastructure Protection, https://en.wikipedia.org/wiki/Critical_infrastructure_protection

[5] Q.v. Critical Infrastructure Protection Act of 2013, https://en.wikipedia.org/wiki/National_Cybersecurity_and_Critical_Infrastructure_Protection_Act_of_2013

operational processes, implement prescribed security or safety tools, and not only train relevant staff but prove that the training has been successfully completed. The GICSP, designed and administered by GIAC[6] as a third party, is the standard to prove exactly that. The North American Energy Reliability Council (NERC) provides one excellent example of these regulations with its Critical Infrastructure Protection (CIP) standards, which include CIP-004:

> CIP-004: Requires that personnel with authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.[7]

The European Programme for Critical Infrastructure Protection (EPCIP) is an analogous regime for the protection of critical infrastructure within the European Economic Area.[8] Both sets of standards are in ongoing development, with modifications to their definitions, scope and the stringency of the requirements taking place on a periodic basis.

7. Create an International, Cross-industry Community of Professionals Supporting and Engaged with Advancing the Profession of ICS Security

With the great variety of educational and employment backgrounds and titles among control system defenders, steering committee members recognized that a unified defining identity was needed for professionals to make contact with one another. The common language developed by creation of the GICSP would aid in communication among certification holders, but it would not be sufficient by itself to connect those individuals in the first place. A community was needed, with GICSP certification as the entry badge not only to the group, but also to the career, with its bearers self-identifying as dedicated to improving control system security.

"Managing cyber risk is an issue affecting 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 [that require] a skill pool that 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, Industrial Cyber Security Manager, Shell, and GICSP Steering Committee Founding Member

[6] GIAC Information Security Certification - Program Overview, www.giac.org/about/program-overview

[7] NERC, CIP Compliance, www.nerc.com/pa/CI/Comp/Pages/default.aspx

[8] Communication from the Commission on a European Programme for Critical Infrastructure Protection, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN

Figure 1 illustrates the volume of GICSP certifications earned per month since 2013.

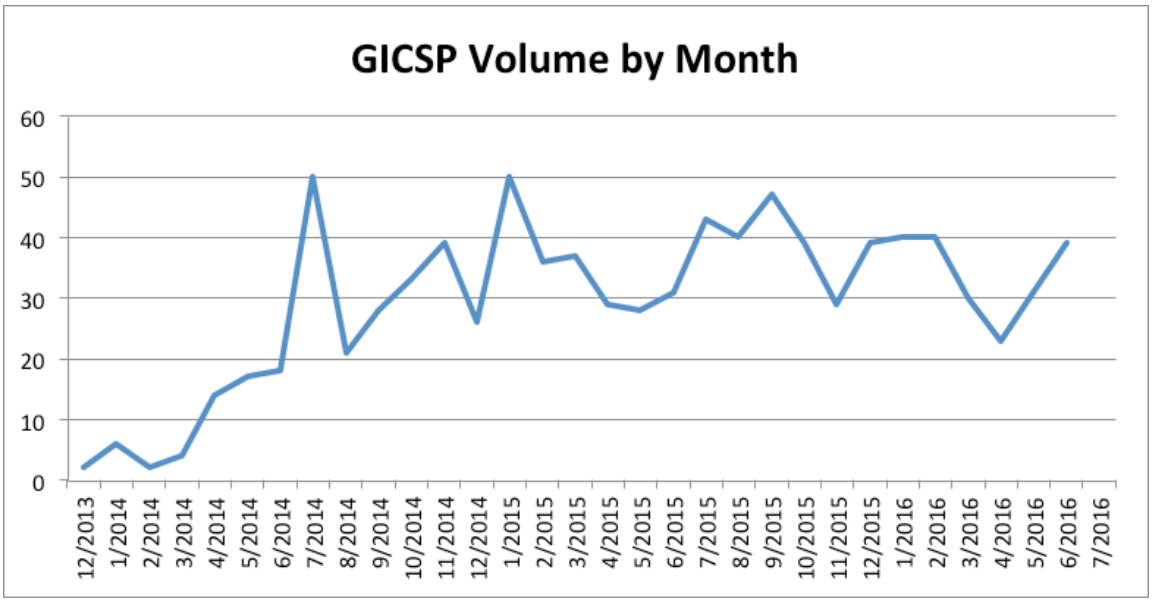


Figure 1. New GICSP Holders by Month

The examples of professions being advanced by the growth of communities of their practitioners are too numerous to mention, and the founders of the GICSP steering committee recognize the importance of this component to the ongoing growth and improvement of ICS defenders. Every community requires a minimal number of members to foster its own continued development. Early on, the steering committee set a goal of 1,000 GICSP professionals worldwide in order for this community to enter the self-supporting and self-improvement phase. That number was reached on July 25, 2016.[9] We anticipate the number of GICSP holders to accelerate as demand for resources with and recognition of the certification continue to rise.

[9] Security Certification: GICSP, www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

Goals of the GICSP
(CONTINUED)

Figure 2 illustrates the overall growth in the number of GICSP certified individuals.

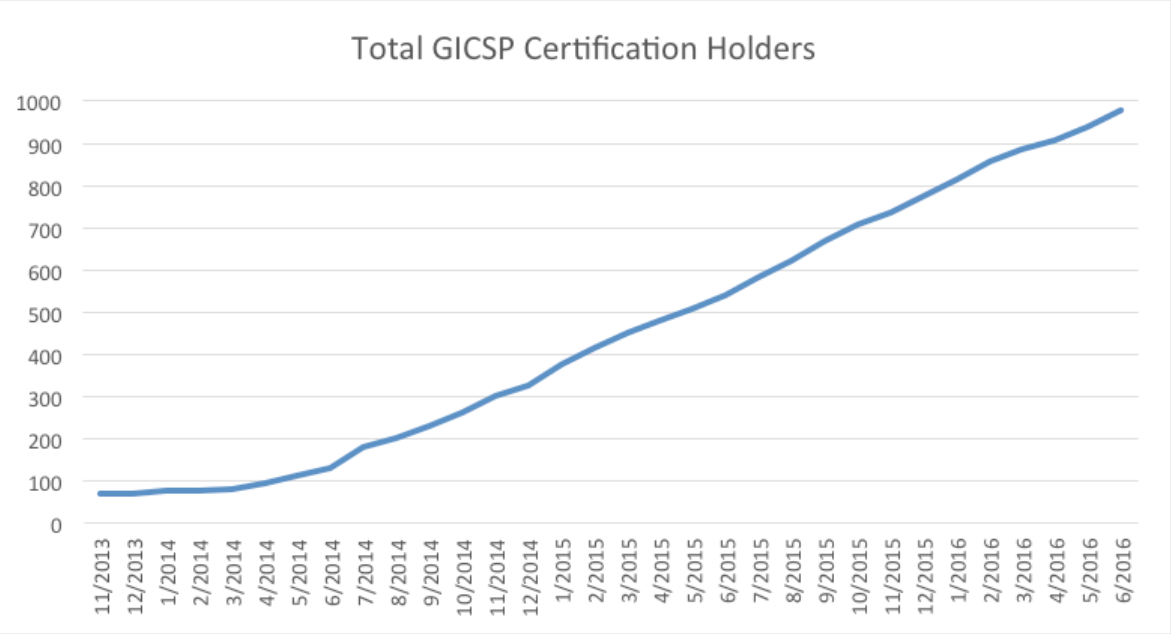


Figure 2. Total GICSP Holders

Developing the GICSP

The modelers of the GICSP drew heavily upon the learning of professional development and training programs that had gone before. A particularly notable example is that of the power industry, which underwent tremendous change in the late 20th century. The increased use of IT led to a corresponding rise in the numbers of workers directly involved in the management and operations of power generation, distribution and transmission systems. Historically these individuals came from engineering backgrounds and field work, and they were familiar with the systems over which they were given control. The rate of growth in this area of work, however, meant increasing numbers of them came from other backgrounds and had no such experience. This significantly increased the risks of human error, and called for development of a means to ensure competency of operators.

Not Your Average Security Certification

Because the GICSP specifically measures competency with the security of control systems, it stands apart from more commonly recognized certifications such as CISSP, the GIAC Security Essentials (GSEC) and the GIAC Certified Incident Handler (GCIH). Control systems have unique design and implementation aspects, the detailing of which goes well beyond the scope of this paper. A consideration is their use in critical infrastructure and high-impact settings. Whereas security breaches in information systems may disrupt business or governmental operations and have financial effects, these same events in control system environments have the potential to result in both immediate and longer-term risks to human lives.

The first power industry program was developed through the mid-1990s and was a point-in-time evaluation; training and testing was done once and considered complete. With the dawn of the 21st century it was recognized that continuing education and certification was needed to keep operators trained on the frequently changing technology. This was implemented in 2004.[10]

The founding members of the GICSP steering committee recognized that the need for training and certification of competency in control system security did not allow for a similar development timeline. The development model of the NERC System Operator Certification program was solid, but establishment of a corollary would require a time-compressed process. Technological change was further advanced and taking place at a greater rate by 2013 than in the early 1990s, and an industrial control security professional certification program needed to be designed, developed and implemented post haste.

Further design considerations included the importance of program accreditation, the greater breadth of technologies and systems, and the needs of the many industries dependent on control systems. The steering committee took on the challenge of balancing all of this, investing significant resources in accomplishing the goals it set out for itself as quickly and efficiently as possible, and took the certification from idea to launch in one year.

[10] NERC, System Operator Certification, www.nerc.com/pa/Train/SysOpCert/Pages/default.aspx

Developing the GICSP
(CONTINUED)

Even with the certification live and in use, this group continues to work for its improvement, identifying subdomains (e.g., oil and gas, chemical processing, water, manufacturing) for additional certifications and areas requiring unique focus. Efforts are also being made to investigate the potential for simulation systems to provide "hands-on" training.

"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, and GICSP Steering Committee Member

However well the GICSP certification has accomplished the goals established for it, it should be mentioned that it continues to be updated and improved. As part of its mission to validate the skills of information security professionals,[11] GIAC periodically reviews test questions and responses in order to identify problems with wording or contents. Further, the balance of content tested upon in the challenge exam is weighed to ensure alignment with the training goals set by the steering committee. All of these efforts involve and are informed by numerous subject matter experts (SMEs), people with years of relevant experience working and often teaching in the field.

The GICSP intentionally crosses both industry and national boundaries. Many of the entities involved from the outset were, and are, global in nature, and this is reflected in the distribution of GICSP holders. Numbers have been greatest in the Americas and European nations, with interest and participation rising more recently in the Asia-Pacific (APAC) region. Figure 3 shows the distribution of GICSP holders in the United States, and Figure 4 shows the representation of GICSP holders across the globe.

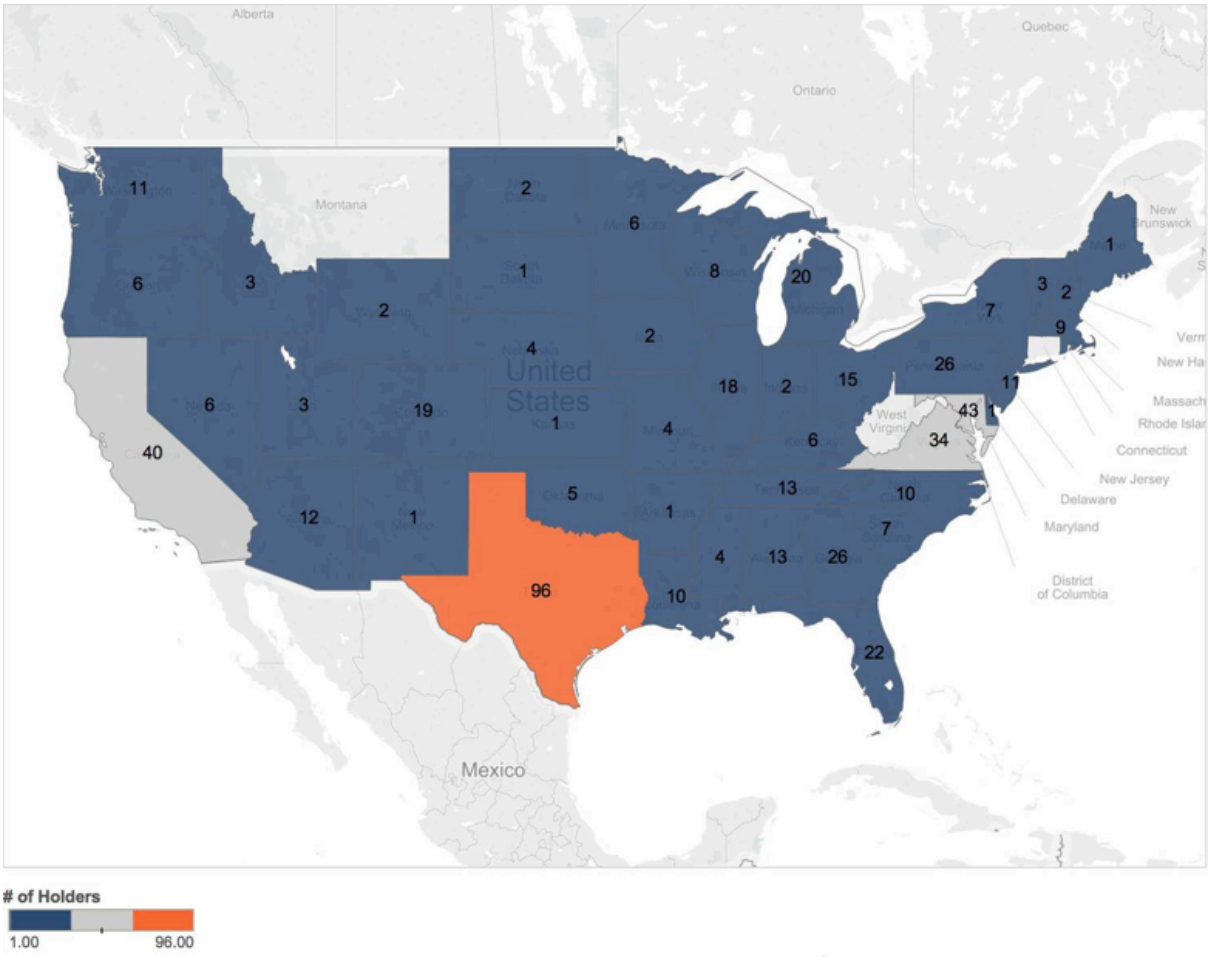


Figure 3. GICSP Holders' Geographic Distribution (USA) as of June 2016

[11] The GIAC Mission Statement, www.giac.org/about/mission

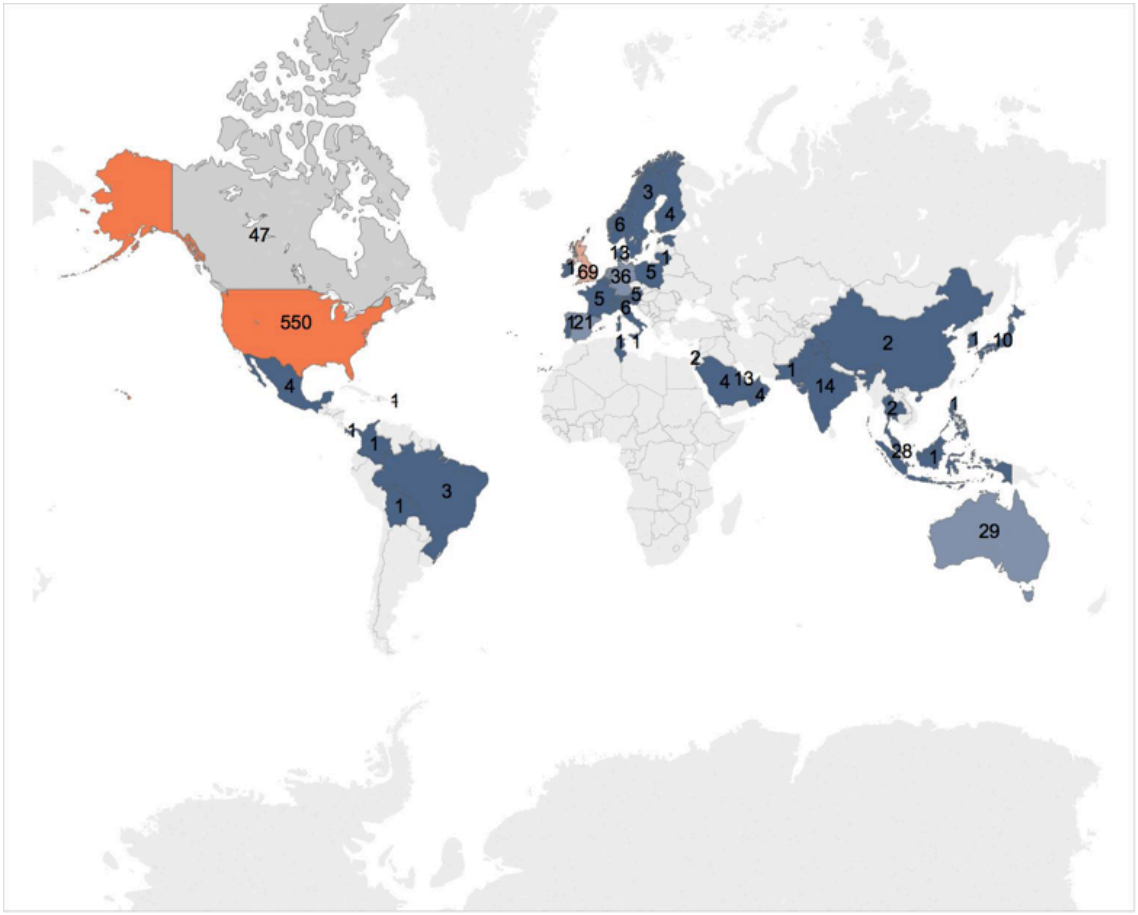


Figure 4. GICSP Holders' Geographic Distribution (Global) as of June 2016

Measuring the effect of certification on an individual career is a project launched in 2015. With the certification live for two years, the steering committee is putting resources towards its commitment to the careers of GICSP professionals and sponsoring research into the impact of this achievement. A survey, currently under development, will be administered initially in 2016 and annually thereafter. Reports will be published on findings in terms of certification impact on income, career satisfaction and job roles and titles, among other data. This will greatly supplement the tremendous amount of anecdotal information already available regarding certification value. One goal of this project is to gain better insight into GICSP penetration into different industries. Data collected from candidates taking the challenge exam indicates that the single largest group self-identified as "Other." Such a large group of unknowns unfortunately weakens the overall value of the findings. See Figure 5.

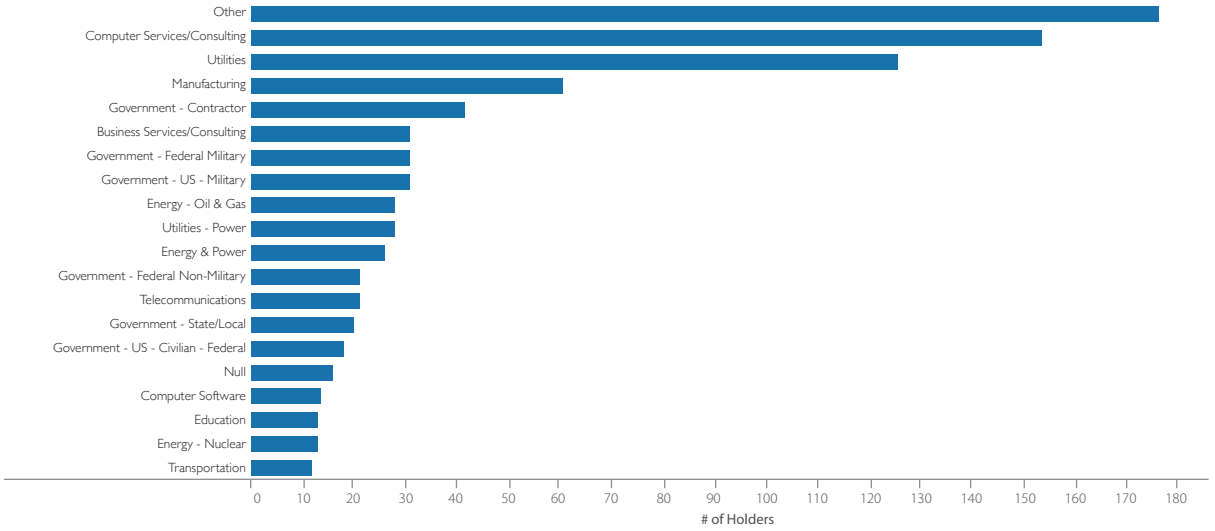


Figure 5. GICSP Holders' Distribution by Industry (Self-reported at Time of Exam) as of June 2016

Our research into the industry distribution of certification holders paints a somewhat different picture, with more than half working for service companies. Many of these are specialized consultancies supporting particular industries, such as utilities, oil and energy, and industrial automation. How many individuals reported that they worked in the industries that they service versus how many have moved in the interim from those employers to an external company servicing that same industry is a question not currently answerable, but other research supports the argument that movement of labor into consultancies is ongoing.[12] See Figure 6 for a picture of the industries in which GICSP professionals are employed.

[12] "SANS 2016 State of ICS Security Survey," www.sans.org/reading-room/whitepapers/analyst/2016-state-ics-security-survey-37067

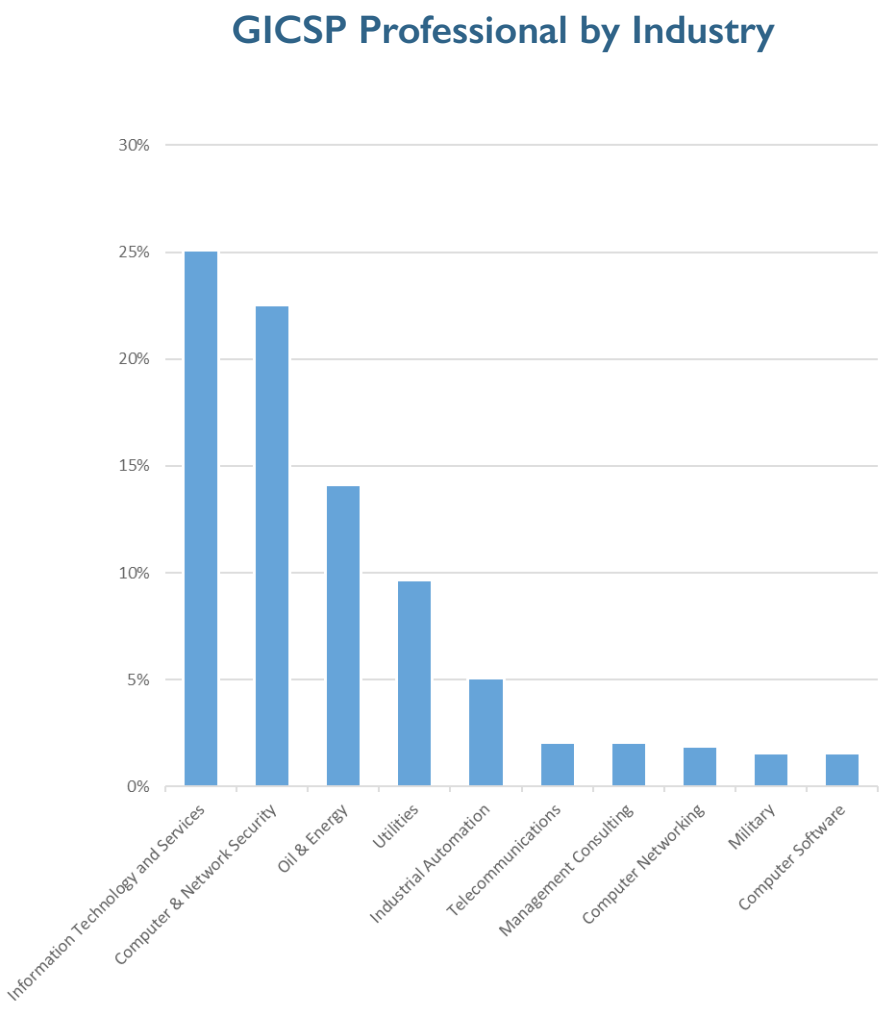


Figure 6. GICSP Holders' Distribution by Industry (Self-reported at Time of Exam)

Looking Forward

An indicator of the growing recognition of the importance of GICSP certification is the appearance of new control system security training offerings. The SANS Institute was one of the founding organizations and continues to be the largest provider of control system security education worldwide. Its ICS/SCADA Security Essentials course, specifically intended to prepare aspiring GICSP holders for the challenge exam, was the first publicly available class designed for this purpose and continues to be updated as the certification matures. No specific training is required for the exam, however, and several other groups now offer ICS security training as well. Some of these offer GICSP-preparatory training, while others prepare students for their own control system security-related certificates. Many organizations, such as the NIST National Initiative for Cybersecurity Education (NICE)[13] and the National Security Agency (NSA) National Centers of Excellence,[14] while sharing the goal of educating the work force protecting our critical infrastructure, are broader in their missions than the GICSP steering committee. Additional certificate programs of note are administered by the International Society of Automation (ISA),[15] the European Union Agency for Network and Information Security (ENISA)[16] and the Information Assurance Certification Review Board (IACRB).[17]

The GICSP steering committee still has several goals to achieve. Subdomain certifications, mentioned previously, are in current development, as is next-level certification for those with higher degrees of mastery in the field. The GICSP is a crucial cornerstone in building the workforce of control system security professionals that is so clearly in demand, but it is only the first step. Moving forward will continue to require dedication to this larger goal and involvement of industry leaders worldwide for the foreseeable future. It is also anticipated that those coming up through the GICSP program, whether with years of experience in this area or whose entry point to their careers is achieving the certification, will contribute to the future growth and development of this important program.

[13] NIC National Initiative for Cybersecurity Education, http://csrc.nist.gov/nice/index.htm

[14] National Security Agency/Central Security Service, www.nsa.gov/academia/index.shtml

[15] The International Society of Automation, Certificate Programs, www.isa.org/isa-certification/certificate-programs

[16] European Union Agency for Network and Information Security, www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals

[17] Information Assurance Certification Review Board, www.iacertification.org/cssa_certified_scada_security_architect.html

Appendix A: Certification Basics

GICSP Global Industral Cyber Security Professional

This certification will be leveraged across industries to ensure a minimum set of knowledge and capabilities that IT, engineer and security professionals should know if they are in a role that could impact the cyber security of an ICS environment.

1
The Test
- 115 questions, 100 scored
- Open book
- 3-hour exam

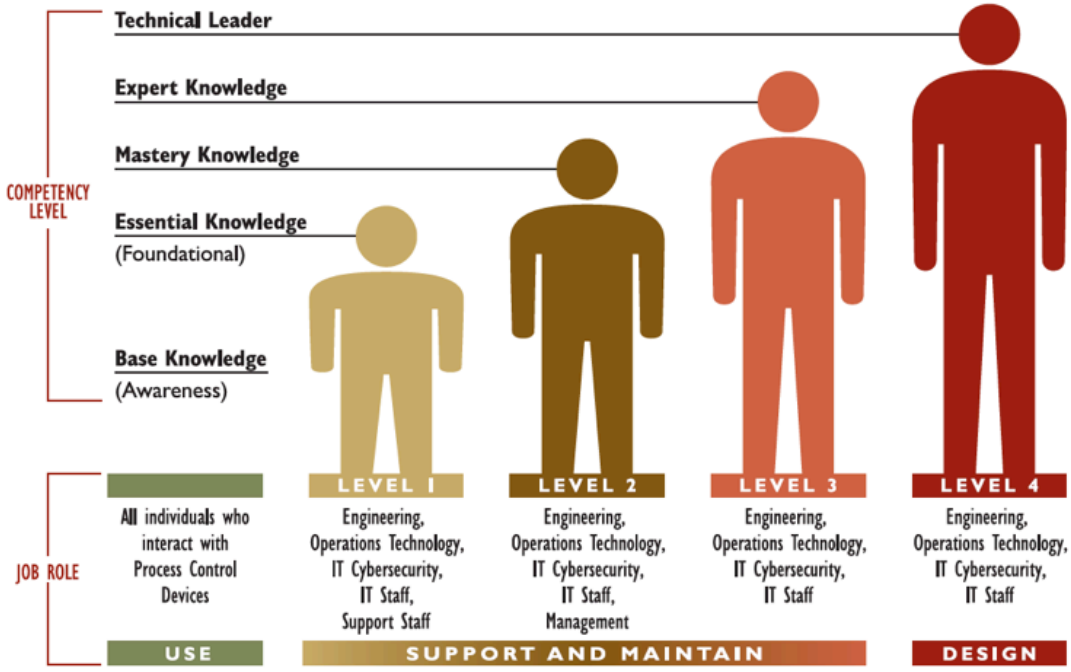
2
Scheduling
- 2 practice tests
- Available 7–10 days after ICS 410
- Available immediately for challenge
- Available at Pearson Vue
- Must take within 120 days

3
Scheduling
- Renewal every 4 years
- Test re-take or
- CMU Certification Maintenance Units

The graphic above appears in the SANS ICS410: ICS/SCADA Security Essentials course, which prepares students for the GICSP exam. It contains information regarding the GICSP Challenge Exam, including test format, exam eligibility requirements and certification upkeep requirements.

Appendix B: ICS Job Roles

ICS-Related Job Role Mapping



The graphic above originally appeared in a SANS workforce consensus initiative developed with input and review from many ICS asset owners and operators across multiple industries. It suggests one way to model the intersection of job roles, competency levels and security functions.

Appendix C: ICS Competency Objectives

GICSP Certification Objectives[18]

1. Access Management - access control models
   Knowledge of access control models (e.g., MAC, DAC, role-based)
2. Access Management - directory services
   Knowledge of directory services (e.g., active directory, LDAP)
3. Access Management - user access management
   Knowledge of user access management (e.g., user accounts, service accounts, temporary accounts, default accounts, guest accounts, account expiration, access control list, access reconciliation)
4. Configuration/Change Management - change management, baselines, equipment connections and auditing
   Knowledge of change management, baselines, equipment connections and configuration auditing
5. Configuration/Change Management - distribution and installation of patches
   Knowledge of distribution and installation of patches
6. Configuration/Change Management - software reloads and firmware management
   Knowledge of software reloads and firmware management
7. Cybersecurity Essentials for ICS - attacks and incidents
   Knowledge of attacks and incidents (e.g., man in the middle, spoofing, social engineering, denial of service, denial of view, data manipulating, session hijacking, foreign software, unauthorized access)
8. Cybersecurity Essentials for ICS - availability
   Knowledge of availability (e.g., health and safety, environmental, productivity)
9. Cybersecurity Essentials for ICS - cryptographics
   Knowledge of cryptographics (e.g., encryption, digital signatures, certificate management, PKI, public versus private key, hashing, key management, resource constraints)
10. Cybersecurity Essentials for ICS - security awareness programs
    Knowledge of security awareness programs (employees/management)
11. Cybersecurity Essentials for ICS - security tenets
    Knowledge of security tenets (e.g., CIA, non-repudiation, least privilege, separation of duties)
12. Cybersecurity Essentials for ICS - threats
    Knowledge of threats (e.g., nation states, general criminals, inside and outside malicious attackers, hacktivists, inside non-malicious)

[18] Global Industrial Cyber Security Professional Certification Description, www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

Appendix C: ICS Competency Objectives
(CONTINUED)

13. **Disaster Recovery and Business Continuity - system backup**
    Knowledge of system backup (e.g., security, data sanitization, disposal, redeploying, testing backups, operational procedures)

14. **Disaster Recovery and Business Continuity - system restoration**
    Knowledge of system restoration (e.g., full, partial, procedures, spares)

15. **ICS Architecture - communication medium**
    Knowledge of communication medium (e.g., VSAT, RF, cell, microwave)

16. **ICS Architecture - defense in depth**
    Knowledge of defense in depth (e.g., layered defense, IDS sensor placement, security system architecture, virtualization)

17. **ICS Architecture - external network communications**
    Knowledge of external network communications (e.g., access points into SCADA/ICS systems, VPNs, vendor/third-party access points, mobile devices)

18. **ICS Architecture - field device architecture**
    Knowledge of field device architecture (e.g., relays, PLC, switch, process unit)

19. **ICS Architecture - industrial protocols**
    Knowledge of industrial protocols (e.g., modbus, modbus TCP, DNP3, Ethernet/IP, OPC)

20. **ICS Architecture - network protocols**
    Knowledge of network protocols (e.g., DNS, DHCP, TCP/IP)

21. **ICS Architecture - network segmentation**
    Network segmentation (e.g., partitioning, segregation, zones and conduits, reference architectures, network devices and services, data diodes, DMZs)

22. **ICS Architecture - wireless security**
    Wireless security (e.g., WIFI, wireless sensors, wireless gateways, controllers)

23. **ICS Modules and Elements Hardening - anti-malware implementation, updating, monitoring and sanitization**
    Knowledge of anti-malware implementation, updating, monitoring and sanitization

24. **ICS Modules and Elements Hardening - application security**
    Knowledge of application security (e.g., database security)

25. **ICS Modules and Elements Hardening - embedded devices**
    Knowledge of embedded device (e.g., PLCs, controllers, RTU, analyzers, meters, aggregators, security issues, default configurations)

Appendix C: ICS Competency Objectives
(CONTINUED)

26. **ICS Modules and Elements Hardening - endpoint protection including user workstations and mobile dev**
    Knowledge of endpoint protection, including user workstations and mobile devices (e.g., anti-virus, white listing)

27. **ICS Modules and Elements Hardening - network security/hardening**
    Knowledge of network security/hardening (e.g., switchport security)

28. **ICS Modules and Elements Hardening - OS security**
    Knowledge of OS security (Unix/Linux, windows, least privilege security, virtualization)

29. **ICS Modules and Elements Hardening - removable media**
    Knowledge of removable media (e.g., USB device security, optical media, external drives)

30. **ICS Security Assessments - device testing**
    Knowledge of device testing (e.g., communication robustness, fuzzing)

31. **ICS Security Assessments - penetration testing and exploitation**
    Knowledge of penetration testing and exploitation

32. **ICS Security Assessments - security assessments**
    Knowledge of security assessment (e.g., risk, criticality, vulnerability, attack surface analysis, supply chain)

33. **ICS Security Assessments - security tools**
    Security testing tools (e.g., packet sniffer, port scanner, vulnerability scanner)

34. **ICS Security Governance and Risk Management - risk management**
    Knowledge of risk management (e.g., PHA/hazop usage, risk acceptance, risk/mitigation plan)

35. **ICS Security Governance and Risk Management - security life cycle management**
    Knowledge of security life cycle management (e.g., acquisition and divestiture, procurement, commissioning secure deployments, maintenance, decommissioning)

36. **ICS Security Governance and Risk Management - security policies and procedures development**
    Knowledge of security policies and procedures development (e.g., exceptions, exemptions, requirements, standards)

37. **ICS Security Monitoring - archiving**
    Knowledge of archiving

38. **ICS Security Monitoring - event monitoring and logging**
    Knowledge of event monitoring and logging

39. **ICS Security Monitoring - network monitoring and logging**
    Knowledge of network monitoring and logging

Appendix C: ICS Competency Objectives
(CONTINUED)

40. **ICS Security Monitoring - security monitoring and logging**
    Knowledge of security monitoring and logging

41. **Incident Management - incident recognition and triage**
    Incident recognition and triage (e.g., log analysis/event correlation, anomalous behavior, intrusion detection, egress monitoring, IPS)

42. **Incident Management - incident remediation/recovery**
    Knowledge of incident remediation/recovery

43. **Incident Management - incident response**
    Knowledge of incident response (e.g., recording/reporting, forensic log analysis, containment, incident response team, root cause analysis, eradication/quarantine)

44. **Industrial Control Systems - basic process control systems**
    Knowledge of basic process control systems (e.g., RTU, PLC, DCS, SCADA, metering/telemetry, Ethernet I/O, buses, Purdue (ISA 95))

45. **Industrial Control Systems - critical infrastructure sector**
    Knowledge of critical infrastructure sector (e.g., chemical, waste water, water, electricity, oil and gas, manufacturing, transportation)

46. **Industrial Control Systems - safety and protection systems**
    Knowledge of safety and protection systems (e.g., SIS, EMS, leak detection, FGS, BMS, vibration monitoring)

47. **Physical Security**
    Knowledge of physical security

Appendix D: Yokogawa Press Release[19]

Press Release

May 8, 2015

Yokogawa Promotes GICSP Training to Enhance Plant Safety

Yokogawa Electric Corporation announces that, as of the end of fiscal year 2014, 14 of its employees have obtained certification as Global Industrial Cyber Security Professionals (GICSP). This is a relatively new professional qualification, first introduced in November 2013, and Yokogawa has been one of the leading companies within the industrial automation industry in obtaining certification for its employees. This attests to the high-level industrial cyber security expertise of its workforce and is in line with the company's longstanding commitment to bringing its customers safety and asset excellence.

The GICSP certification exam is offered under the auspices of Global Information Assurance Certification (GIAC), a leader in the cyber security certification field. The GICSP is the only credential of its kind that addresses the specific cyber security issues that are encountered in the industrial control systems (ICS) field. This vendor-neutral certification is aimed at IT, engineering, and security professionals working in every industry. It assesses and validates that professionals have the skills, knowledge, and capabilities needed to be in a role where they will exercise responsibility for the cyber security of an ICS.

An increasing number of Yokogawa's major customers are now requiring the assignment of at least one GICSP qualified professional to each project. This is clear evidence of the industry's strong recognition of and support for this professional qualification.

Commenting on the GICSP, Shailendra Shete, head of the Global Engineering Business Division, says, **"I believe it will be difficult for Yokogawa to make headway in expanding its security business if we do not emphasize the GICSP. Employees who get this certification will be conversant with the latest technologies and be at the forefront of efforts to provide such services to the industry. I think that they will be able to help Yokogawa take and maintain a leading position in the provision of security services."**

Yokogawa is continually striving to optimize control systems security for its customers by developing highly secure systems and instruments and providing operational support services. Even before launching its GICSP initiative, Yokogawa had developed its own security training program to ensure that its employees would be able to provide the security solutions needed by customers. Yokogawa will continue its efforts to increase the number of GICSP certified professionals at each of its Group companies around the world. This will help to strengthen the company's position as a leader in the ICS field, and will build on our long history in network security and our global reach. Our continual aim is to make sure that our customers can operate their plants safely.

[19] Yokogawa Press Release, www.yokogawa.com/us/news/press-releases/2015/yokogawa-promotes-gicsp-training-to-enhance-plant-safety.htm

Appendix E: GICSP Steering Committee Founding Members

Member	Firm
Soliman Almadi	Saudi Aramco
Michael Assante	SANS ICS
Markus Braendle	ABB
Scott Cassity	GIAC
Ed Crawford	Chevron
Derek Harp	SANS ICS
Ian Henderson	BP
Charles Hosner	KPMG
Auke Huistra	Shell
Hideaki Kobayashi	CSSC Japan
Nate Kube	GE CyberSecurity
Samuel Linares	BAH
Lee Neitzel	Wurldtech, a GE company (Previously Emerson)
Jamey Sample	E&Y (Previously PG&E)
Tyler Williams	Shell
Doug Wylie	NexDefense (Previously Rockwell Automation)

Authors

Derek Harp

Director—ICS & SCADA Security

Derek Harp is currently the Director for ICS Global Programs at SANS and the GICSP Steering Committee Chair. He is responsible for organizing events, resources and initiatives that educate and enable increased collaboration within the entire ICS security community. Mr. Harp has served as a founder, CEO or advisor of early-stage companies for the past 18 years with a focus on cybersecurity. Derek is also a co-founder and a board member of NexDefense, Inc., a company focused on the security technology needs of ICS asset owners. Previously, he was the CEO and co-founder of LogiKeep, Inc., where he was the co-inventor of Intellishield™, a pioneer IT security product that was subsequently acquired. Mr. Harp is a former U.S. Navy officer with experience in combat information management, communications security and intelligence.

Bengt Gregory-Brown

Principal Analyst at Sable Lion

Bengt is principal analyst at Sable Lion Ventures, LLC, a accelerator focused on emerging cyber security solutions. He brings 20 years of experience in management of IT and infrastructure projects, enterprise security governance, digital systems security risk analysis, regulatory compliance and policy conformance for companies, including Liebert Systems, American Electric Power, Xerox and Nationwide.

Bengt was also a co-founder and director of LogiKeep, Inc. and was instrumental in the crafting of its premier IT security product, Intellishield™. Additionally, he has managed IP development and protection strategies from executing ideation sessions through patent process administration, and he is a co-inventor of multiple issued patents. Current clients include NexDefense, Inc. and the SANS Institute.