

CSSCO Whitepaper 1 – Organizational Objectives

Authors: Eric Byres and Joanne Byres

Byres Security Inc.

Lantzville BC V0R 2H0

✉ email: eric@ByresSecurity.com

🌐 web: www.ByresSecurity.com

Table of Contents

Executive Summary	1
1 Introduction.....	2
2 The Need for a Control System Security Certification Organization (CSSCO).....	3
2.1 Industries Concern.....	3
2.2 A Proposed Solution.....	3
2.3 Benefits to Industry	5
3 Goals and Objectives of a CSSCO.....	6
3.1 Do We Need Another Security Organization?	6
3.1.1 A Framework for Understanding Industrial Security Standards.....	6
3.1.2 Standards, Certification and Conformity Assessment	7
3.2 Specific Goals for a CSSCO.....	8
3.2.1 Goal #1: Development of Interim Standards	9
3.2.2 Goal #2: Creation of a Conformity Assessment Process	9
3.2.3 Goal #3: Enabling and Managing Conformity Assessment Services to Industry	10
4 Summary and Conclusions.....	11
References	12

Acknowledgements

The authors, Eric and Joann Byres would like to thank all those companies and organizations that generously supported our efforts by providing financial contributions as well as the very much appreciated advice and encouragement.

American Chemistry Council	ExxonMobil – Upstream	Southern Company
BP	Honeywell	Symantec
ChevronTexaco	Invensys	Syncrude
Emerson	ISA	TOTAL
ExxonMobil – Downstream	Shell	Yokogawa

To each and every one of you, Thanks!

Executive Summary

This whitepaper is the first in a series of three which investigates the possible formation of an independent Control System Security Certification Organization (CSSCO) to create well-engineered specifications and processes for the security testing and certification of critical control system products. It discusses why the organization is required, what it would achieve and how it relates to other organizational bodies in the area of control system security.

Over the past few years, security researchers have shown that SCADA and control systems products can have serious security vulnerabilities that can leave critical systems exposed to viruses, hackers and possibly terrorist activities from around the world. Operations-focused standards such as ISA SP-99 and NERC CIP-002-009 help the end-users ensure that their control systems are managed in a secure manner, but there are no coordinated efforts under way to establish procedures for the security testing and certification of the actual products used in these control systems. Like the weak brick in a well designed wall, this lack of product-focused security undermines the efforts of the operational security standards.

To address this short coming, industry leaders have proposed that an organization be formed to both create well-engineered specifications and processes for the testing and certification of critical control systems products and to accelerate the development of industry standards that can be used as a basis for these certifications. The focus of this certification would include all network capable products that lie between the final field elements and the security gateway that separates the control system from the business network. This would include both hardware and software components in control products, such as controllers, network switches, HMI platforms and software, programming stations.

This approach compliments existing industry security standards efforts in that it addresses developmental assurance at the product level (as compared to operational level) and is compliance focused rather than standards-creation focused. Thus the CSSCO's goals would be:

- Development of interim standards for industrial security product compliance;
- Development of processes for conformity assessment to those standards;
- Either offering conformity assessment services or accrediting other parties to offer these services.

Ensuring compliance to a standard is a very different process from creating the standard. It is a long term process to ensure that standards are followed faithfully and appropriately. As a result, it is not a trivial undertaking and can be far more complex than standards creation. A successful CSSCO launch will need to balance between completeness and expediency as it sets up the numerous processes and policies it needs to fulfill its responsibilities.

Despite the complexity of the undertaking, the rewards to industry are likely to be significant. A well designed and managed certification process for product security will likely result in reduced costs and time commitment in product selection for end users. It will also help ensure that products are more secure 'out of the box' which will result in improved process reliability and safety. For vendors the certification process will provide a single testing framework and an industry stamp of approval, resulting in faster time to market and lower development and integration costs. Finally, for the standards bodies and government agencies developing industrial security specifications, the result will be better, field-tested standards that are clearly being followed by industry.

1 Introduction

This report is the first in a series of whitepapers investigating the possible formation of an independent Control System Security Certification Organization (CSSCO) to create well-engineered specifications and processes for the security testing and certification of critical control systemⁱ products. The full study is divided into three whitepapers as follows:

- **CSSCO Whitepaper #1: Organizational Objectives** – discusses why the organization is required, what it would achieve and how it would relate to other organizational bodies:
 1. Needs analysis for a Control System Security Certification organization;
 2. Objectives, goals and tasks involved in security certification of control products;
 3. Relationships and interaction with other industrial security standards bodies.
- **CSSCO Whitepaper #2: Organizational Models** – discusses how the organization could be structured and governed to achieve its maximum potential, including:
 1. Investigation of critical success factors in other industrial certification organizations;
 2. Governance, membership and voting models;
 3. A proposed path to create a third party certification process for control products.
- **CSSCO Whitepaper #3: Legal and Financial Considerations** – discusses the legal considerations as well as financial and resource requirements for the organization at startup and as it matures:
 1. An incorporation model designed to best meet the needs of industry (e.g. non-profit vs. for-profit, jurisdiction of the organization, etc.);
 2. Legal and property rights considerations;
 3. Proposed initial budget and membership fee model;
 4. Estimation of member commitment requirements in time and people;
 5. A multiyear time line and milestones for the setup and operation of the organization;

ⁱ The term “control system” is used in this paper to represent any industrial automation system including Supervisory Control and Data Acquisition (SCADA) Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Emergency Shutdown (ESD) systems and safety control systems.

2 The Need for a Control System Security Certification Organization (CSSCO)

2.1 Industries Concern

Over the past few years security researchers have shown that SCADA and control systems products often have serious security vulnerabilities that can leave critical systems exposed to viruses, hackers and possibly terrorist activities from around the world. For example, in May 2006 the US Computer Emergency Response Team (US-CERT) released a vulnerability note describing how an Inter-Control Center Communications Protocol (ICCP) Server widely used in the electrical industry for utility control center communications had a serious heap buffer overflow¹. Similarly, Sandia National Labs reported a number of incidents where critical control systems were shut down by simple network scanning tools². Even more disconcerting are the numerous Slammer Worm incidents that continue to occur against control systems years after a patch was released – according to experts at Microsoft the problem is due to the fact that end-users simply don't know they have the vulnerable Microsoft product embedded in their control system and thus never patch it.

The existence of serious security vulnerabilities in control products is not surprising. Today's automation systems were not designed with security in mind, but rather performing control simply and efficiently. The thought that someone might deliberately attack a PLC or DCS system was never part of the manufacturer's design specifications nor was it in the system development plan. To make matters worse, most control system vendors have had limited capacity to rigorously test new products for possible security flaws. As a result, the owners and operators of critical control systems have had little knowledge of the systems' robustness in the face of a cyber attack - until disaster strikes.

Adding to this problem is the fact that both control system vendors and owners have been transitioning from proprietary technologies to the less expensive technologies prevalent in the Information Technology (IT) world such as Ethernet, TCP/IP, Microsoft Windows and various web technologies. Unfortunately, many of these popular applications, protocols and operating systems have a significant number of widely known vulnerabilities. Exploitation tools, worms, and how-to papers are often readily available shortly after the announcement of a new vulnerability, so hacking many of the components of a modern SCADA system can be done with a few clicks of a mouse. Even the flaws in SCADA specific technologies have become general knowledge – detailed presentations on how to exploit SCADA vulnerabilities have been given at public conferences such as BRUM2600³, ToorCon 2005⁴ and Blackhat Federal⁵.

Control system owner/operators, equipment vendors and governments are well aware of this situation and are attempting to address it through a number of operations-focused standards such as ISA SP-99 and NERC CIP-002-009. While these efforts will help the end-users ensure that their control systems are managed in a secure manner, there are no coordinated efforts under way to establish procedures for the security testing and certification of the actual products used in these control systems. Like the weak brick in a well designed wall, this lack of product-focused security undermines the efforts of the operational security standards like ISA SP-99 and NERC CIP-002-009.

In the absence of any product security standards, end users are developing their own security specifications, often with little technical understanding of how to properly evaluate a product's security. Those companies that do have the knowledge for proper evaluation are expending significant resources to do so, and are creating conflicting requirements that ultimately make compliance difficult for the vendors.

2.2 A Proposed Solution

Industry leaders from a number of major control system operators and manufacturers, have proposed that an organization be formed to create a set of well-engineered specifications and processes for the testing and certification of critical control systems products. The mission of this organization would be to:

- Facilitate the independent testing and certification of control system products to a defined set of control system security standards;
- Use existing control system security industry standards where available, develop interim standards where they don't already exist, and adopt new standards when they become available;
- Accelerate the development of industry standards that can be used to certify that control systems products meet a common set of security requirements.

As shown in Figure 1, the targets of evaluation (TOE) would include all network capable products that lie between the final field elements and the security gateway that separates the control system from the business networkⁱⁱ. This would include both hardware and software components in control products, such as controllers, network switches, HMI platforms and software, programming stations and the like. Equipment that falls outside of the control domain, such as office systems, would not be included.

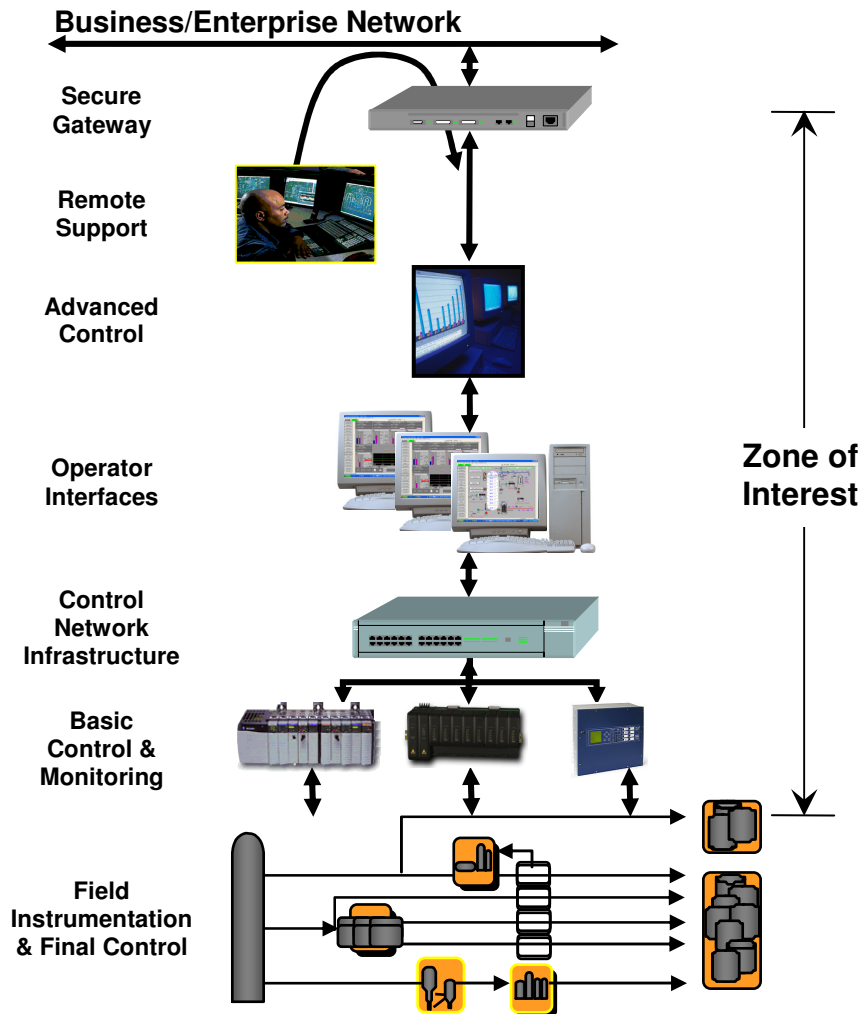


Figure 1: Zone of Interest for the CSSCO

ⁱⁱ As advanced communications protocols migrate into the actual field devices, it is likely that the TOE will also include these as well.

It is envisioned that the program would be similar in concept to the internationally accepted IEC 61508 standards paired with the TÜV certification for Safety Instrumented Systems, allowing control system vendors to be able to offer products that are certified to meet a standard set of minimum security requirements. In addition, the organization would work closely with existing standards groups, supplying them with both the draft documents that can be formulated as standards and the supporting research to enable informed decisions on security standards.

2.3 Benefits to Industry

Over the years, well managed certification programs across a broad spectrum of industries have provided clear advantages to their participants. Programs like the TÜV certification for Safety Instrumented Systems and the Fieldbus Foundation's device interoperability certificates have had significant positive impact in the industrial control arena, while the USB Implementers Forum's certification efforts have brought home computer users one of first communications technologies that operates almost flawlessly, regardless of the product involved. Worldwide, there are tens of thousands of certifications programs across all industries that exist because certification creates tangible benefits for the product user, the product manufacturer, standards bodies and society as a whole.

These benefits can be both tangible and intangible. As noted by the Open Group, a not-for-profit' consortium that manages IT certification programs, the typical benefits of certification programs include:

- *Increased probability that the whole (or system or solution) will operate as expected*
- *Improved interoperability of components by assuring common interpretation of specifications*
- *Facilitated improvements in specifications as the process uncovers ambiguities in standards*
- *Facilitated improvements in implementations as the process uncovers ambiguities in products*
- *Accelerated convergence between the specifications and implementations as the process uncovers ambiguities in the specification and errors in interpretation built into products*
- *Improved supplier confidence in parts they provide can itself be a differentiator⁶*

More specific to the controls industry, this proposed security certification process will result in significantly reduced costs and time commitment in product selection and acceptance for end users. It will also help ensure that products are more secure 'out of the box' which, as a result, will offer improved process reliability and safety. For vendors the certification process will provide a single testing framework and an industry stamp of approval, resulting in faster time to market and lower development and integration costs. Finally, for the standards bodies and government agencies developing industrial security specifications, the result will be better, field-tested standards that are clearly being followed by industry.

3 Goals and Objectives of a CSSCO

3.1 Do We Need Another Security Organization?

People active in the SCADA and process industries often comment that there is already an overabundance of groups creating “standards” for industrial security. For example, the Sandia Center for SCADA Security website lists eleven different organizations currently creating SCADA security standards⁷. So isn’t product certification for security something that is already covered by one of these groups? As it turns out, the answer is NO for several reasons that we will outline below.

3.1.1 A Framework for Understanding Industrial Security Standards

It is well known in industry that establishing the security of a system is not a single event or process. As noted security expert Dr. Hans Daniel points out, any product or system undergoes a lifecycle starting from the initial concept and design and finally ending with the decommissioning. Each stage is likely to consist of many processes and related activities, with security assurance increments being gained with every successful activity. This lifecycle process has been formally recognized in a number of standards including the International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) standard 15288⁸ which defines five lifecycle stages as shown in Figure 2. This can be simplified into the three major user and provider concerns that can be addressed by standards and methods⁹:

1. Development of new products and systems
2. Integration of products into operational systems
3. Operating a specific system in a facility and personnel context

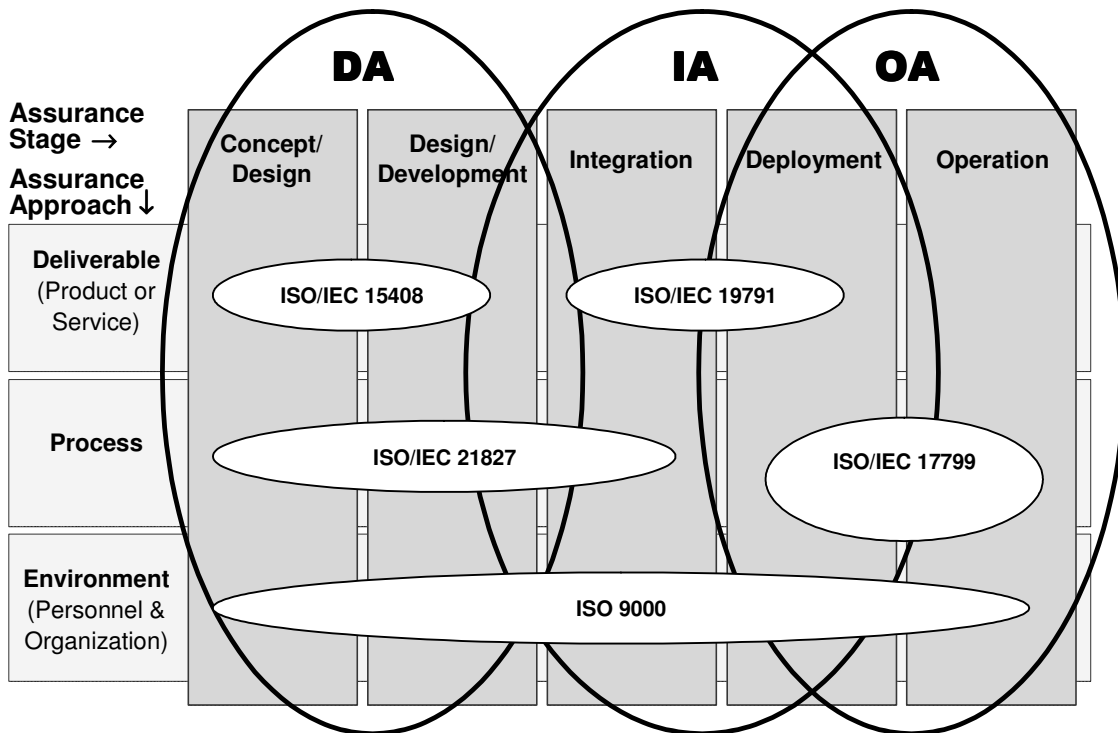


Figure 2: Security Assurance Stages in a System Life Cycle (courtesy of Dr. Hans Daniel)

Obviously each one of these stages are likely to require different standards or processes – for example, the security requirements for a software designer creating a new control product will be very different from what the system owner should do when actually using the system in an operating plant. The software designer may need to follow defined methodologies for software validation while the user may be required to deploy appropriate password policies in the plant. Yet both are critical for a secure system and, as any user of mainstream office software has learned, failures at any point in the lifecycle can jeopardize the security of the entire system.

As a result, industry needs well-defined methods and standards associated with Developmental Assurance (DA), Integration Assurance (IA) and Operational Assurance (OA). No one standard can do it all. This is already well understood by the IT world, where standards like ISO/IEC 15408 (Common Criteria) for have been created for developmental assurance, as compared to ISO/IEC 17799 for operational assurance.

There are also different approaches that one may take to obtain a level of security assurance. For example, higher levels of assurance are gained by the product while lower levels of assurance are provided by evaluating the environment it was created in. For example, standards like ISO 9000 (and the product vendor's reputation) provide an "environmental" assurance, while ISO/IEC 17799 specifies processes to be followed for security and ISO/IEC 15408 offer methodologies on how to actually evaluate a specific product for security. Thus the actual approach to creating assurance must also be considered in any industry standard.

So the real question is not "are there too many standards?", but rather which standards overlap with others and which parts of the life cycle are missing from all the efforts. It turns out that nearly all of the existing control system security standards programs focus on operational assurance using a "process" approach and that developmental assurance at the product level is missing.

The two exceptions to this are the Process Control Security Requirements Forum's "System Protection Profile for Industrial Control Systems" (SPP-ICS) and American Gas Association's AGA-12. The first is best described as a meta-standard that outlines the overall security requirements for a system. It provides an excellent starting point for product standards but is very general in its approach and can be extremely costly to follow in its entirety. The second standard defines a specific encryption technology for SCADA systems and does not address any other aspect of security. Thus both need additional standards to offer a true product security standard.

So despite the proliferation of organizations involved in setting standards for industrial control systems today, there is a significant gap in product-focused security certification standards or methodologies for control systems. Filling this gap until such time as another standards body can step into the role needs to be one of the primary goals of the CSSCO.

3.1.2 Standards, Certification and Conformity Assessment

It is important to understand that certification is not the same as a standard. A standard sets the rules while certification provides a specific assessment for whether a particular company, product, or individual conforms to those rules. For example, in the safety instrumented systems world IEC 61508 is the international standard for electrical and electronic safety related systems, while groups like TUV and the 61508 Association actually perform the assessment and certification. Most standards setting bodies like IEC and ISO make it very clear that they do not conduct certification as stated in this quote from the ISO website, "*ISO itself does not carry out conformity assessment activities.*"¹⁰

Those standards that lack a well defined certification process often cause considerable difficulty for end users. An example of this is the infamous EIA/TIA-232 (ITU-V.24) standard that was more renowned for its incompatibility between vendors than its usefulness.

Certification is just one possible type of Conformity Assessment (CA), which is officially defined¹¹ as "*activity that provides demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.*" As both ISO and the 61508 Association explains, that activity can have a number of processes and outcomes such as testing, inspection, examination and certification. The product, process, system, etc. is referred to as the object of assessment and the CA may be performed by:

3.2.1 *Goal #1: Development of Interim Standards*

For many certification organizations, the task is simply to ensure conformity with the established standards through a series of well defined conformity assessment activities. In the case of the proposed CSSCO things are a bit more complicated – as outlined in section 3.1.1, there are no appropriate product security standards in existence and none are expected in the next two to three years. Thus, in addition to acting as a certification body, the CSSCO will need to develop interim product security standards until such time as the various standards bodies can address this area.

The creation of interim “standards” can be accomplished in several sub phases. First the CSSCO will need to convene a small group of industry experts to create a set basic product security requirements. This can be based on both industry needs analysis and existing documents such as the PCSRF’s “System Protection Profile for Industrial Control Systems” (SPP-ICS)” and ISO/IEC 15408 (Common Criteria). This will then be converted to standards-like language and used as the target for the subsequent development of a process for conformity assessment. Finally, the results of the actual conformance activities (Goal #2 and #3) will be fed back to the back to this phase to allow refinement of the interim standard.

At the same time as the interim standards are being developed, a working group to assist industry standards bodies such as the IEC, IEEE, ISA, and ANSI should be formedⁱⁱⁱ. This would provide the various standards bodies with both well-developed draft documents that can be formulated as official standards and the supporting research to enable informed decisions on security standards. By supporting these largely volunteer-based bodies with professionally developed materials, we believe that the overall standards-development process can be accelerated.

3.2.2 *Goal #2: Creation of a Conformity Assessment Process*

The goal of creating a conformity assessment process for industry is the primary focus of the CSSCO and in this case, involves developing a certification program for control product security compliance. The steps to achieve this target are fairly well known in the certification industry and can be divided into three core management elements:

- Specification Creation and Management
- Trademark Creation and Management
- Test Definition and Certification Management

Each of the above elements is critical to the long term success of the program and require significant effort in the initial stages of the CSSCO formation. For example, the development of the following processes (and associated documents) is a possible starting point:

- **Formal goals and Objectives** – the mission of this organization, the priority targets and what is beyond scope for the group (both short term and long term).
- **Membership Structure and Operations** – membership selection, decision making processes and definition of organizational structures.
- **Legal** – agreed upon process and documents for legal considerations such as anti-trust provisions, intellectual policy management and confidentiality.
- **Certification Process** – the policies to be followed in the creation and operation of the program including everything a vendor needs to know to achieve and maintain certification and procedures to address whatever might go wrong during the certification process.

ⁱⁱⁱ For example, ISA-SP99 is in the process of forming a working group to create “ISA 99.00.04 – Specific Security Requirements for Industrial Automation and Control Systems”. Whether this document focuses on requirements for end users or vendors (or both) is still under debate as of September 2006. Regardless, it would welcome assistance from outside advisory bodies like the CSSCO.

- **Trademark Licensing Management** – the processes and agreements for vendors to use the “certification test” trademarks and enforcement of the trademark against
- **Conformance Requirements** – defines what a conforming product must do to be certified and provides mapping between products and specifications.
- **Operational Guidelines** – processes and manuals for quality control and audit procedures.

Thus this goal will likely consume the bulk of the organizations resources, both in the initial stages and over the long term. Getting this stage off to a good start will likely determine the success of the body as a whole.

3.2.3 Goal #3: Enabling and Managing Conformity Assessment Services to Industry

The final goal of the CSSCO will be to ensure that the services to do the certification testing of the products are available to the industry through a process that ensures impartiality, confidentiality, and predictability at all times. It will do this by being the Certification Authority for the program, a task that includes:

- Processing registrations for certification
- Auditing each certification submission, including any required test results
- Assessing whether a product submitted for certification meets the conformance requirements
- Maintaining a register of products that have been successfully certified
- Providing guidance to suppliers throughout the process
- Monitoring and administering vendor reporting of problems encountered during testing and vendor requests for interpretations of the specification.

It is not necessary for the CSSCO to do the actual certification testing itself. In fact, considering the high capital costs and manpower requirements for testing services, it is probably better for the CSSCO to certify independent for profit testing organizations like TUV or UL to provide this service. These organizations could then pay a licence fee to the CSSCO based on either their certification as an approved test house or on each of the product tests they conduct. Regardless, it is important to realize that this “outsourcing” adds its own requirements and obligations. Certification and compliance verification of the external testers is essential, as is policing of the test market so that vendors are treated consistently and fairly. Finally, enforcement of the certification testing process is critical to ensure respect for the CSSCO program over the long term.

4 Summary and Conclusions

Industry experience has shown us that assurance of conformity to a standard is a very different process from creating the standard. Instead it is the critical next step to ensure that standards are followed faithfully and appropriately. By their very nature, all standards are ambiguous or incomplete in some way and without a central authority that adjudicates conformity, compliance will be inconsistent from vendor to vendor and of limited use to the end user. Thus over the long term the primary focus of the CSSCO will be to provide that conformity assurance for control system products to specific security standards. Over the short term the CSSCO may also need to help create those standards.

Conformity assurance through a certification process is not a trivial undertaking. There are multiple processes to be defined, numerous legal considerations to be addressed and a considerable number of policy and procedural documents to be created. The quality of these steps will determine the success of the CSSCO over the long run, so it is critical that they are conducted with care. At the same time, most end users sponsoring this study have noted that time is of the essence in getting a control product certification program operating, so it is equally critical that these steps are conducted quickly. Thus a successful CSSCO launch will need to balance between completeness and expediency. In the next in this series of whitepapers we will look at possible models for the organization and the steps necessary to get it from a concept to functional organization.

References

-
- ¹ Vulnerability Note VU#190617: LiveData ICCP Server heap buffer, US Computer Emergency Response Team, May 16, 2006, <http://www.kb.cert.org/vuls/id/190617>
- ² David P. Duggan, Michael Berg, John Dillinger and Jason Stamp; "Penetration Testing of Industrial Control Systems", *Sandia National Laboratories*, March 7, 2005
- ³ "We have your water supply, and printers' – *Bruncon report*", *The Register*, October 20, 2003
- ⁴ <http://www.toorcon.org/2005/conference.html?id=16>
- ⁵ <http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf>
- ⁶ "Business Scenario: Certification", *The Open Group*, January 23, 2004
- ⁷ <http://www.sandia.gov/scada/standards.htm>
- ⁸ http://www.15288.com/about_15288.htm
- ⁹ Hans W. Daniel; "Security For Industrial Process Measurement And Control", IEC TC65CWG10 Presentation, Vancouver BC, March 2006
- ¹⁰ <http://www.iso.org/iso/en/comms-markets/conformity/iso+conformity.html>
- ¹¹ ISO/IEC 17000:2004 " Conformity assessment - Vocabulary and general principles"
- ¹² http://www.iso.org/iso/en/comms-markets/conformity/iso+conformity-02.html#P27_5684
- ¹³ <http://www.61508.org/ca.htm>