

CSSCO Whitepaper 2 – Organizational Models

**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.....	3
2 Critical Success Factors in Certification Organizations.....	4
2.1 Clear Definition of the Value Proposition for Stakeholders.....	4
2.2 Brand Management and Trust	4
2.3 Ensuring Technical Relevance	5
2.4 “Do Not Reinvent the Wheel”	7
3 Membership, Governance, and Voting Models.....	8
3.1 Membership.....	8
3.2 Governance Structure and Voting Models	8
3.2.1 Size and Composition of the Executive Board.....	9
3.2.2 Technical Steering Committee	9
3.2.3 Voting.....	10
3.2.4 Staffing.....	10
4 Processes for Creating Product Certifications	11
4.1 Conformity Assessment and Certification Processes	11
4.2 A Possible Path to Create Third Party Certification	12
5 Conclusions.....	16
References	17

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 second 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 the critical success factors in other industrial certification organizations and how the organization could be structured and governed to achieve its maximum potential.

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.

While this sounds simple, it turns out that creating a functional organization for compliance assurance and certification of the security of control system products is not a trivial process. Fortunately, hundreds of thousands of similar organizations have been created over the past twenty five years, so the path forward has already been established by many others before us. Thus the first step in designing a new organization is to look at what other similar organizations have learned during their creation and evolution. The study identified four critical success factors:

- Clear Definition of the Value Proposition for Stakeholders
- Brand Management and Trust
- Ensuring Technical Relevance
- Not Reinventing Processes, Guidelines and Policies

Next membership and member classes or types were investigated. If the interest and support shown in the initial CSSCO study is any indication, then the bulk membership will come from major end-by users, followed by equipment vendors. In all, we see five types of members:

- Control equipment end users
- Security and control equipment vendors
- Consultants and testing houses
- Government Agencies
- Associate Members

Since the CSSCO will be dealing with security issues that can be sensitive to both corporate and national wellbeing, some mechanism to prevent undesirable organizations or individuals from joining is desirable. This need for control of membership needs to be balanced against possible anti-trust issues.

Based on the membership types we then looked at possible models for governance and voting and propose a simple model based on a two-tier governance system with an Executive Board and a Technical Steering Committee. The board would consist of ten seats elected from the full members of the CSSCO and distributed among the member types as follows:

- Control equipment end users – 4 Board Seats
- Security and control equipment vendors – 4 Board Seats

- Consultants and testing houses – 1 Board Seat
- Government Agencies (Rotated between countries) – 1 Board Seat

The Technical Steering Committee would also be elected from the CSSCO membership and would have between 8 and 12 seats.

Finally processes for creating product certifications were looked at. It was determined that either *Self-Certification with Verification* or *Third Party Testing* would be the best possible alternatives. The latter is clearly the preferred route, but is the most expensive to set up and to administer over the long term. The CSSCO will need to determine the level of resources it is likely to have at its disposal and the level of expense that the industry is willing to bear. It may be necessary to start with the less desirable *Self-Certification with Verification* model and then evolve to the full *Third Party Testing* over a number of years. Regardless of which model is selected, we have laid out a possible 7-step path for the CSSCO to achieve its immediate objectives.

In summary, it is important that the CSSCO clearly define and articulate its goals and objectives early on in its formation. The process of setting up and operating the CSSCO will require considerable resources. While financial support is one obvious aspect, technical support will be equally important and member organizations must be willing to provide access to their own experts to facilitate the efficient flow of information for the purpose of satisfying the organization objectives. Finally it is important that the CSSCO take advantage of the past experiences of other organizations, the experts in the field and the proven strategies of successful certification organizations so as to be as efficient as possible.

1 Introduction

This report is the second 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 Critical Success Factors in Certification Organizations

Before setting out to design a new organization for providing certification, it is critical to look at what other similar organizations have learned during their creation and evolution. Thus in this section, we will attempt to determine what the factors are that make one certification body an unqualified success, while another similar group fails to gain acceptance in industry and eventually disappears without meeting its objectives.

It turns out that this is a complicated question to answer. Through our research we uncovered over one hundred so-called “critical” success factors. For example, each of the organizational executives we interviewed offered very different reasons why their entity had been successful and others had not been. Clearly, distilling all these possible success factors down to those that are both relevant and under the influence of the founding members of the CSSCO is vital.

There are several reasons for this surplus of “success factors”. First, as we pointed out in White Paper #1, a certification body like the one proposed for the CSSCO is not a simple entity with a single focus but must address a number of goals and objectives to be successful overall. Second, different players in the certification process will clearly have different ideas of what success is. For example, for the vendor community a successful outcome of the certification process might be “improved customer satisfaction and reduced legal exposure”, while for the customer it could be “reduced procurement costs and improved product functionality”. This possible divergence of the definition of success for different stakeholders leads us to our first and most critical success factor, which we will discuss below.

2.1 Clear Definition of the Value Proposition for Stakeholders

Throughout our interviews with key executives in industrial certification bodies (both successful and unsuccessful), discussions with organizational and legal consultants and reviews of published literature^{1 2}, the one factor that was repeatedly cited was the need for clear definition of the value proposition for key stakeholders in the early stages of the organizations formation. There are several reasons for this. First, as we explain in Whitepaper #3, both the creation and operation of a certification entity is not an inexpensive proposition. Even the cost of the actual testing and certification process for individual products can be costly. Relatively simple certifications like those accredited by the Fieldbus Foundation typically cost \$5,000 to \$10,000 per device tested, while complex certifications such as those for IEC-15408 (Common Criteria) can run into the millions of dollars. Thus all the potential stakeholders in a certification effort need to have a clear definition of the specific value of certification for their organization. This can not be a “feel good” value proposition (such as “for the betterment of the industry”), but must be a clear statement of tangible benefits. Ideally it should also include corresponding calculations of the financial return on investment for both the formation of the organization and the costs of the certification process. Without this information, it is unlikely that most companies’ senior management will be willing to commit both the financial and manpower resources needed to make the CSSC a success over the long term.

The second function of this definition process is to clearly determine where potential conflicts in the objectives of different stakeholders might lie. A significant number of certification organizations have failed when the goals of the different stakeholders were not reconciled early in the formation process. Lack of disclosure of the intended objectives of key participants may also leave those members exposed to anti-trust actions³ (anti-trust issues are discussed in more detail in Whitepaper #3). Finally, potential new members of the organization, as well as adopters of the process or the certification, results will likely base their decision to participate heavily on the stated reasons for the organization’s existence. If these are not well defined in the very early stages of formation, many companies will hesitate to be participants.

2.2 Brand Management and Trust

Most individuals new to the certification process assume that the most important component of the certification process is getting the technical aspects of the assessment correct. While this is certainly important, most experts list technology a distant third or fourth as compared to the issues of brand management⁴. For example, Andrew Updegrave, a noted expert on the formation of standard setting and certification consortia states:

“Planning for a proper certification and trademark program is essential to the success of most consortia. The process of creating such a program should begin before the formal launch of the consortium, and a

careful assessment of the costs of such a program should be included in developing the first year's budget.”⁵

The value of any certification program in the market place is predicated on both the markets awareness of the certification itself and the trust in the certification body's ability to deliver on the certification promise. If the end-users of certified products are unaware that the certification program exists then they will not value certified products from their suppliers and the suppliers will see no benefit going through an expensive certification process. For example, both the Modbus and Foundation Fieldbus organizations offer conformance certification to their respective industrial communications standards. However the Modbus certification is almost unknown in industry and as of September 2006 only 37 products have ever been certified for compliance, as compared to 341 for Foundation Fieldbus. This is despite the fact that Modbus is more widely used in industry and its certification is a far less expensive process compared to Foundation Fieldbus certification.

The second critical component in certification brand development is to create and maintain trust in the assurance process throughout the market. The Certification Authority should be a known and trusted organization within the industry and must be open for external audit and validation. It also must have its own procedure in place to ensure that the certification processes meets the requirements of a good assurance program.

Finally, protecting the Certification Authority from false claims is critical. As Andrew Updegrove notes:

“As noted earlier, standards need to be credible. Standards are only useful to secure market advantage (e.g., “buy this because it will work with that”) if in fact “this does work with that”. If vendors assert compliance where compliance does not exist, then the standard will lose credibility, and the goals of the consortium and its members will be defeated.

The way in which false claims of compliance are prevented by consortia is through the use of trademarks, rather than by asserting patents. Where a consortium gives a name to a standard and the public knows the standard by that name alone, then the consortium may assert its legal right to prevent a vendor from using the name of the standard in connection with a non-compliant product.”

If both the legal structure and systems are not in place from the start to protect the certification process, then the costs later on can be very high.

In summary, brand management for a certification organization needs to address the following factors:

- **Marketing** – creating demand by the end user community for certified products so that vendors can justify involvement in the program. This includes clearly articulating the brand values (what certification means to the end user), creating a clear process to provide recognition to certified products (certification logos, easily assessable certified products lists, etc.) and development of procurement guidance to end users.
- **Assurance** – maintaining procedures to ensure that all processes meet the requirements of a good certification program.
- **Policing** – creating and enforcing guidance and processes for the fair use of the trademark and actively protecting against misguided or false claims.
- **Delivering on the “Promise”** – ensuring that the certification process is well designed and managed so that it delivers on the organization's undertaking.

We will address the later factor in the next subsection.

2.3 Ensuring Technical Relevance

The importance of the technical relevance of both the certification process and the testing methodologies to the market is fairly obvious to most people. However experience indicates that it can be relatively easy to accidentally end up following minor pathways when developing technical specifications, so it is important to develop a series of “tests” to determine that the development process is on track. These tests for technical relevance should be used as guiding principals for the technical teams and as acceptance criteria for the governing board.

Setting up this list of criteria for technical relevance and a process for adherence to the list needs to be one of the early tasks for the Certification organization. This need not be developed from scratch – there is extensive guidance

in this area. For example, we have provided a slightly tailored version of a typical requirements list based on published work by the Open Group⁶:

Appropriate

1. *Mapped to the lifecycle of a technology – early technology has more risk, so there’s more need for certification. However, too early and there are no standard criteria to use. As a technology becomes more mature, the value of certification becomes somewhat lower.*
2. *Tests should be tailored to the needs of the market for the product, as should the overall certification program.*
3. *Need to know the purpose: need to determine what will be certified and set appropriate certification goals. Testing may be sufficient in some cases.*
4. *A certification program should be optimized for the complexity of the solution – not its parts. A program should avoid spending too much money certifying low-level components where it is very easy to determine whether they work or not. The certification program should be mapped to the appropriate value-add chain.*
5. *A certification program should address synchronization and assessment of the parts.*
6. *A certification program should be inclusive in the sense that it considers the issues and practicalities of small to medium enterprises.*

Cost-Effective

7. *A certification program should be tailored to match the needs to benefits as it evolves throughout a lifecycle of the technologies and products of the solution.*
8. *Over time, the cost and effort of certifying a maturing product or technology should decline.*

Criteria-Based Measures

9. *A certification program should be based upon good measurable standard criteria, or set of standard criteria, that are objective and testable.*
10. *A certification program for a solution should be based upon an aggregation of standards criteria.*

Timely

11. *A certification process should be sensitive to the lifecycle changes of technology and should take (much) less time to certify than the lifecycle of a product.*

Holistic

12. *A certification program should have a publicly named certification authority.*
13. *A certification program should have a public policy statement of liability, warranty, and guarantee.*
14. *A certification program should include certification policy development, certification program development, certification testing, certification operations, certification problem resolution, and recourse procedures.*
15. *A certification program should include automation wherever possible to control costs and scale*
16. *A program should provide a level of certification appropriate to the need for the program since one size does not fit all cases. For example, different levels could be test, letter of conformance, certificate, etc. using different techniques such as plugfests, bake-offs, certification test audits, etc.*
17. *A certification program should have a stated position on testing, should have a means to do testing, and needs to be driven by objective tests.*
18. *A certification program should focus on standards that are testable.*

Other excellent sources for guidance on this topic can be found in the ISO Committee on Conformity Assessment (CASCO) reference library⁷ and the American National Standards Institute (ANSI) “Manual of Operations for Accreditation of Certification Programs (ANSI-ACP-CA-002)”⁸

2.4 “Do Not Reinvent the Wheel”

Finally it is important to recognize that creating an organization like the CSSCO is not a unique undertaking. Even though this might be the only group dealing with the issues of industrial security certification, setting up similar certification authorities has been done thousands (if not hundred of thousands) of times before. For example, the American National Standards Institute’s NSSN site⁹ currently tracks the status of some 270,000 current standards worldwide, most of which have some sort of certification authority associated to them.

There are numerous not-for-profit support organizations, for profit consultancies and government agencies willing to provide process and policy templates, sample legal documents and specific advice. It is critical that the CSSCO take advantage of these resources so it can focus its valuable resources on the technical tasks and not on administrative and legal details.

3 Membership, Governance, and Voting Models

3.1 Membership

Surveys of similar industrial organizations with certification authority (such as the Fieldbus Foundation, the 61508 Association and the Profibus Trade Organization) indicate that the bulk of the core membership comes from the vendor community, followed by the consulting community. Typically end-users are involved in a relatively minor way through structures such as end-user councils. However, if the interest and support shown in the initial CSSCO study is any indication, then the bulk membership may come from major end- users, followed by equipment vendors. Consultants, testing houses and academics are not currently active in the CSSCO but will likely want to be involved as it evolves. This would be desirable since they can offer considerable technical expertise. Finally, due to the importance placed on this topic by the US and European governments, we may also see considerable governmental interest. Thus we see five types of members:

- Control equipment end users
- Security and control equipment vendors
- Consultants and testing houses
- Government Agencies
- Associate Members

This wide variation in member types is good for the CSSCO for a number of reasons. First it will help prevent the CSSCO being diverted to meet the needs of special interests, rather than the industry as a whole. Second it reduces potential anti-trust concerns, although these can also be dealt with in other ways (see Whitepaper #3 for a detailed discussion of anti-trust issues). Finally, this wide variation is more likely to provide the wide range of expertise needed to successfully create the technical solutions needed by the CSSCO. Thus membership fee structures and policies should be designed to encourage this diversity, a topic we will address in more detail in Whitepaper #3.

One issue that needs special study is the question of restrictions on memberships for security reasons. While most certification organizations are open to a person or entity willing to pay the membership fees, the CSSCO will be dealing with security issues that can be sensitive to both corporate and national wellbeing. Thus some mechanism to prevent undesirable organizations or individuals from joining is desirable.

This need for control of membership needs to be balanced against possible anti-trust issues. There are several well reported legal cases where a consortium’s members have been convicted under US anti-trust legislation for deliberately restricting membership to limit competition. To avoid this possibility, we propose an open and transparent process where all new membership applications are voted on by the board of directors. As well, board members from the same membership type as the applicant should abstain from voting. In other words, if a new vendor applies to be a member of the CSSCO, then all board members that belong to equipment vendors shall abstain. In this way, charges of restrictive and anti-competitive activities can likely be avoided, although an expert on legal advice on this topic should be obtained before this process is finalized.

3.2 Governance Structure and Voting Models

The governance structure of most certification organizations follows a fairly standard model consisting of an Executive Board and a Technical Steering Committee. In the words of Andrew Updegrave:

*“While there are many variations, a consortium is most typically managed by a Board of Directors and has a Technical Committee, which in turn has various work groups, subcommittees and special interest groups (SIGS). Many consortia also have business and/or marketing committees. In most cases, member rights extend principally to technical adoption and promotion, while the Board has authority over strategic direction and overall management.”*¹⁰

We see little reason for the CSSCO to deviate from this proven model.

3.2.1 *Size and Composition of the Executive Board*

The function of the executive board is to set the overall strategic direction of the CSSCO. It is critical for the CSSCO and all its stakeholders that this board performs its functions appropriately and that there is a clear division of responsibilities between the Executive Board, the Technical Steering Committee and the operational and support staff. In particular, it is important that the board not become preoccupied with technical issues and rather leave that to the Technical Steering Committee and its various sub-groups.

A board that is balanced in terms of both industry sector and member type is essential for maintaining both member-neutrality and industry relevance. Obviously a board that is completely dominated by vendor interests could be an issue, but even sector domination can cause difficulties. For example, consider the implications of a board that contained two individuals from the power utilities, two vendors that only supplied the power sector and two consultants that only serviced the power industry. This would tend to push the organization towards satisfying the needs of the power sector, and may neglect the needs of the other sectors. In the end the organization would lose credibility, which would cause members of the other sectors to seek fulfillment of their needs elsewhere.

At the same time, a balance must be found between representation and workability. The board must be large enough to provide adequate representation, but it cannot be so large that it becomes a barrier to its own progress. As pointed out in numerous interviews, as board size increases, it becomes harder to schedule and conduct board meetings. Since most organizations interviewed felt a board having between 8 to 12 members was ideal, a possible distribution of ten board seats could be:

- Control equipment end users – 4 Board Seats
- Security and control equipment vendors – 4 Board Seats
- Consultants and testing houses – 1 Board Seat
- Government Agencies (Rotated between countries) – 1 Board Seat

In addition, every effort should be made to ensure that at least one board member is selected to represent each of the key industrial sectors of Power, Oil and Gas, Water/Waste Water and Chemicalsⁱⁱ. Examples of this type of Board structure can be seen in many organizations, one example of which is the Eclipse Foundation.¹¹

To facilitate decision making, the Executive Director of the CSSCO should have a vote for tie-breaking purposes, except for matters dealing with his or her performance.

Since the Executive Board should focus on strategic direction and not on technical issues, we recommend that the Board members should be senior management in their respective organizations and not be technically oriented individuals. For example, the Fieldbus Foundation's board includes people such as John Berra (CEO of Emerson Process Solutions), John Eva, (Vice President and General Manager of Invensys Process Systems) and David Eisner, (Vice President of Engineering of Honeywell). Members at this management level have the authority to take action on matters resolved during board meetings and do not have to refer back to their companies for all decisions, ensuring that the CSSCO resolutions will not be hampered by management in other organizations, and facilitating prompt action on resolutions.

During our interviews with executive management in similar industrial certification organizations, the importance of this high level management support in their organizations was repeatedly stressed. Over the years it has been occasionally necessary for both an organization and the industry it supports to take action as a group. If the board members do not have the necessary authority to affect change in their native organizations, they can only commit to being the "champion for change" rather than committing to actually making the change happen.

3.2.2 *Technical Steering Committee*

While the Executive Board sets the general direction of the organization, the Technical Steering Committee regulates the technical programs and reviews and, when appropriate, the technical activities of the organization. It oversees the establishment of standards and specifications, and typically proposes specific projects, reviews projects

ⁱⁱ As other sectors such as food and beverage or automotive increase their interest in industrial cyber security, they may also need to have representation, possibly requiring the size of the board to be increased.

proposed by others, and makes recommendations to the Board of Directors. The Technical Steering Committee also monitors pending projects to facilitate their successful completion.

Like the Board, a Technical Steering Committee consisting of between 8 and 12 members was often reported as ideal by most organizations. These seats may or may not need to be distributed across member types like the Executive Board is.

3.2.3 Voting

Typically voting is based on a one vote model for full members and no voting rights for associate members. Founding members may get special voting privileges but this varies. As well, as we noted above, often organizations control the number of seats for each type of member, such as allowing four vendor member seats and four end-user member seats.

Based on these starting points, organizations use one of two voting models for selecting the Executive Board and Technical Steering Committee members. The first is for each member to be able to vote to for all seats, regardless of their member type. The second is for each type of member to vote only for the seat reserved for the member of the same type. We were unable to determine which one was a better model.

3.2.4 Staffing

Based on the interviews held with successful certification organizations, we strongly recommend that the Executive Director be a professional position. As well, the day-to-day operations should be either contracted out to a supporting organization or managed by professional staff. Expecting the CSSCO to be largely volunteer-driven is unrealistic. For example, Andrew Updegrave offers the following advice to companies trying to decide whether or not to join an established certification organization:

“While there are examples of all-volunteer consortia that have been quite successful, this type of organization requires greater commitment by both member companies as well as their representatives. If a consortium which lacks paid staff also lacks a culture of strong committee chairs, timely process and continuity of membership, its efforts are vulnerable to failure.”¹²

In addition the CSSCO will likely need to engage the services of one of more technical subject matter experts (SME) in the area of security testing. While some of this expertise will come from volunteers, we expect that a considerable amount of it will need to be paid for, either through having a professional on staff or through contracts to experts.

4 Processes for Creating Product Certifications

4.1 Conformity Assessment and Certification Processes

The ISO/IEC has formally defined three types of conformity assessment processes¹³. These are:

- **First-party Assessment:** the assessment of conformity to a standard, specification or regulation is carried out by the supplier organization itself. In other words, it is a self-assessment. This is also known as a supplier's declaration of conformity.
- **Second-party Assessment:** assessment of conformity is carried out by a customer of the supplier organization.
- **Third-party Assessment:** the assessment of conformity is performed by a body that is independent of both supplier and customer organizations.

While testing, inspection and examination can be first, second or third party, certification is, by the ISO/IEC definition, a third party activity. Provided that the 3rd party is a trusted entity, this offers the highest level of confidence and is the ultimate goal for the CSSCO. However it is also the most expensive path, and due to financial challenges, certification programs have evolved which fall across a range of increasing cost and credibility. Andrew Updegrave describes a number of different so-called "certification" processes that are common in the information technology world:

1. Self-Assertion without a Test Suite. At the most modest end of the scale is self-assertion, which is not a certification process at all, in any true sense of the word. In this model, the vendor simply asserts that its product conforms to a given standard, and there is no third party verification of either the result, or the means by which the vendor reaches its conclusion. Where this is the best that can be done, it is important for a consortium to make it clear that only limited credibility should be given to such assertions, and that the marketplace understands that no formal certification process is in place.

As a result, the term "certification" should not be used in connection with a self-assertion program. Rather, the implementers of standards in this setting should only be permitted to assert compliance with, or conformance to, a standard or specification. Self-assertion programs are quite common, notwithstanding the limited level of credibility which they offer. One reason is that, unlike safety features, interoperability failures do not lead to dire non-financial consequences, and the government therefore has not to date sought to impose regulations in this area. Hence, the incentive for a high level of certainty is sometimes comparatively low.

Second, a wide range of factors may preclude the ability of a consortium to create a test suite and/or engage a third party testing service. For example, the commercial value of compliance may not be high enough, or the standard itself may not be robust enough to achieve a conclusive result, and therefore compliance with the standard alone would not imply a result that has significant public commercial value. Most frequently, a self-assertion program is simply the result of the fact that the budget of the organization will not support the creation and employment of a test suite. Whatever the reason may be that leads a given consortium to forego development of a test suite, the achievements of that organization are apt to be more modest than those of another group which supports a full certification program.

2. Self-Asserted Compliance (or Self-Certification): In this model, some type of test suite exists, but the vendor performs the test itself. In some cases, there may be little effort to publicize the fact that a product meets the test, because the test suite has been created primarily as a tool for vendors to use in order to achieve interoperability or another goal at a lower cost. In other cases, credibility is an important goal, but the consortium has not been motivated, or able, to arrange for verification. As a result, only a very modest increase in credibility is gained over self-assertion of compliance.

3. Self-Certification with Verification: If a higher degree of credibility for the certification program is deemed to be desirable, the vendor is required to return some type of evidence of satisfactory test completion to the consortium (or a third party) for verification. The deliverable typically will be a paper or electronic record of the test results. Again, depending on the consortium's resources and the degree to which vendors are willing to pay certification fees, the report may either simply be filed away, or may be

examined for completeness and consistency, but not directly confirmed by an independent test of the product. Hence, an element of trust is still involved, and the credibility of the certification is still qualified.

4. Third Party Testing: *This is the highest standard of testing, since the vendor must submit its product to a third party for testing. However, the efficacy of testing may vary widely, being limited in part by the sophistication of the standard to which the test applies. Some standards and specifications are very detailed and comprehensive, while others are less so. Hence, a product built to one standard which successfully passes certification testing may indeed "plug and play" with another compliant product, while a product built to another, less comprehensive standard may require further refinements in order to reliably interoperate. The degree to which a standard is capable of meeting the highest standard is also affected by factors other than technical challenges, including political compromises among members who are, after all, usually competitors.*

With third party testing, the final results are often submitted to the consortium or standards development organization, which will then issue the actual certification, along with a license to use its trademarks in connection with assertions of satisfactorily passing a certification test.

Obviously the first alternative (Self-Assertion without a Test Suite) is unlikely to be acceptable to industry since, security is considered by many to be a safety related issue. The second alternative (Self-Asserted Compliance) is also likely to fall short of industry expectations. This leaves either Self-Certification with Verification or Third Party Testing as possible alternatives and while the latter is clearly the preferred route, it is also the most expensive to set up, administer and to conduct over the long term. Thus the CSSCO will need to determine the level of resources it is likely to have at its disposal and the level of expense that the industry is willing to bear for testing over the long run. It may be necessary to start with the less desirable 3rd model and then evolve to the full Third Party Testing over a period of a few years. The financial strength of the CSSCO in the first few months of its existence will indicate which path we need to follow.

4.2 A Possible Path to Create Third Party Certification

There are a number of possible processes to get to a place where the CSSCO is able to offer Third Party Certification of the security of industrial control products. We have outlined one possible path below based on the strategy and goals defined in Whitepaper #1, which are:

- 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.

As we noted in Whitepaper #1, the second of these goals is the primary objective for the CSSCO, so we focus on how to achieve this in the short term, but also to address the others goals as well. There are seven core steps which we will describe in more detail below.

The first step is the *Initial Setup of the CSSCO* and is the most critical in the entire process. The remaining steps proceed out of the first one and will need to be redefined as the first is completed. Each step will involve considerable interaction with other industry players such as the relevant standards bodies, industry participants and certification entity specialists and support organizations. Figure 1 shows these relationships and the key information flows between them.

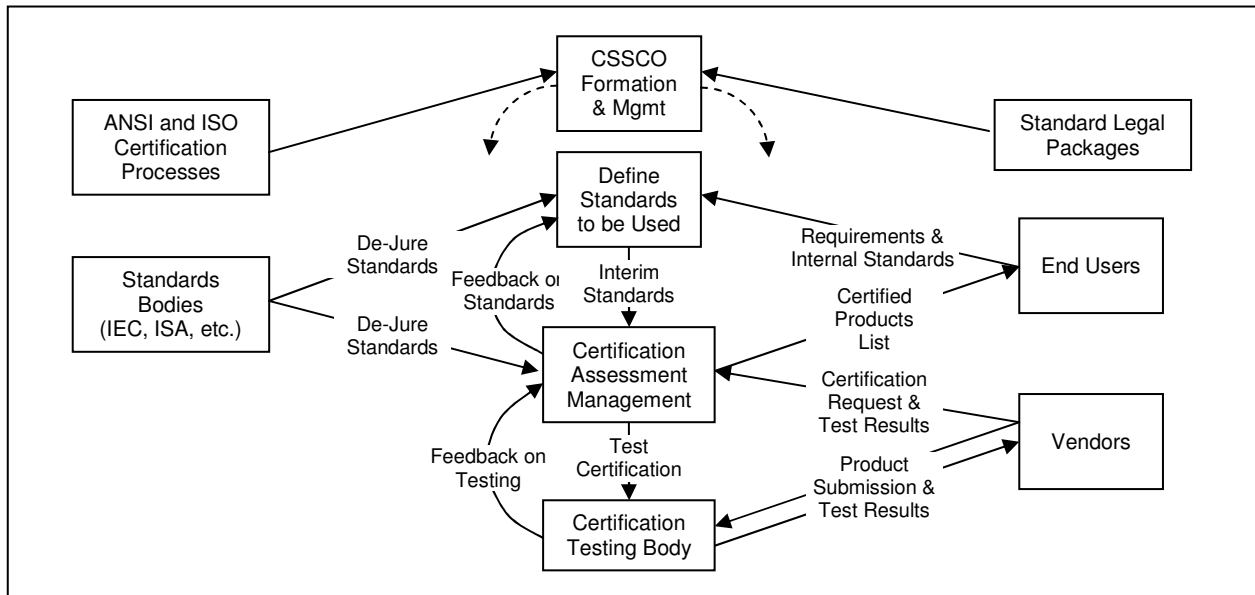


Figure 1: Information Flows in the Certification Process

1. Initial Setup of CSSCO

- a. Determine Intent and Commitment of Founding Members – Convene a formational meeting for interested founding members to state their goals for the CSSCO and their commitment in terms of time and resources
- b. Form Interim Board - Create a working board of interested founders to operate until elections are held.
- c. Determine Formal Goals and Objectives – Based on Step 1(a) the Interim board states the mission of this organization, the priority targets and what is beyond the scope for the group (both short term and long term).
- d. Select Support Organization – Choose an appropriate organization (such as ISA or Open Group) to supply logistic support.
- e. Obtain Appropriate Legal Document Package – Purchase or contract for development legal package including bylaws, incorporation and basic operational policies
- f. Incorporate CSSCO
- g. Collect Membership Dues - Dues from founding members to be payable on date of incorporation
- h. Elect Executive Board and Technical Steering Committee - From the list of paid-up members elect executive.
- i. Select/Hire Executive Director: Selection of a professional to represent and lead the organization on a day-to-day basis. This person must have the drive to execute resolutions and be trusted to do so in a member-neutral fashion.
- j. Create Road Map for Organizational Objectives - The Executive Director, Executive Board and Support Organization shall work together to create a roadmap to achieving the Formal Goals and Objectives determining in Step 1 (c) above.

2. Define and Setup Overall Certification Process

- a. Define Proposed Certification Process – Select or create 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. This should be based on standard ISO and ANSI Guidelines.

- b. Define Trademark Licensing Management – Select or create the processes and agreements for vendors to use the “certification test” trademarks and enforcement of the trademark against false claims. This should be based on standard proven packages available from consultants or supporting organizations.
- c. Define Basic Conformance Requirements – Define in general terms what a conforming product must do to be certified. This should be based on standard ISO and ANSI Guidelines.
- d. Define Operational Guidelines – Creating or obtaining processes and manuals for quality control and audit procedures. This should be based on standard proven packages available from consultants or supporting organizations.

3. Set Technical Direction

- a. Establish Security Requirements - Conduct an industry needs analysis to determine the security requirements for control systems products and identify priority control system components that require security certification (the latter may significantly influence possible technical objectives).
- b. Determine Reasonable Technical Objectives for Certification – Some desirable security requirements may not be economically or technically testable. In this sub-stage the committee will decide what security requirements are possible to test and give the CSSCO and industry resources. This work will require a mix of security testing SMEs and members of the vendor/end-user communities.
- c. Identify Technical Resource Requirements (and Budget)
- d. Locate Appropriate Technical Resources – At this stage it is critical to enlist the appropriate experts in security testing standards and methodologies. Many may be outside the industrial controls world.

4. Create Interim Standards as Certification Targets

- a. Research Existing Security Standards for Appropriate Requirements – This includes control system based documents such as PCSRF’s “System Protection Profile for Industrial Control Systems” (SPP-ICS)” and IT focused standards like ISO/IEC 15408 (Common Criteria).
- b. Research Corporate In-house Standards and Procedures for Appropriate Requirements
- c. Compile a Current “Body of Knowledge” on Existing Control System Security Products Requirements
- d. Conduct Gap Analysis – Compare the Current “Body of Knowledge” with earlier industry needs analysis of security requirements for control systems products.
- e. Define Measurable Product Security Requirements - Create a set of measurable product security requirements, based on existing documents where possible and new specifications as required.
- f. Offer Security Requirements for Member or Public Comment
- g. Converted to Standards-like Language – These will be used as the target for the subsequent development of a process for conformity assessment.

5. Create Specific Assurance Requirements and Test Methodologies

- a. Define Compliance Requirements – Define the method with which compliance to Interim Standards will be measured (in other words, if testing, what sort of tests?).
- b. Create Draft Testing Methodologies and Specifications – This may be contracted out or done internally.
- c. Conduct Trials of Testing Methodologies – The proposed tests should be checked for feasibility (can they be done in an efficient manner?), repeatability (do they consistently give

the same results?), effectiveness (do they detect what they should?) and completeness (do they miss anything?).

- d. Revise Testing Methodologies – Based on the previous step, the testing methodologies should be revised and retested until acceptable.
- e. Release Preliminary Testing Methodologies – The methodologies should either be distributed for comment and trials by the industry and academic communities or public trials of the testing methodologies should be conducted.
- f. Finalize Testing Methodologies and Processes

6. Provision of Services to Conduct Certification Testing

The actual certification testing could be conducted by the CSSCO, but considering the high capital costs and manpower requirements for most testing services, it is probably better for the CSSCO to certify independent testing organizations like TUV or UL to provide this service. At the same time, 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.

A less desirable, but also less expensive route is *Self-Certification with Verification* as noted in Section 4.1. This will require the contracting with a commercial entity to provide the appropriate test suites (software or hardware) to the vendors and then setting up a results validation process as part of Step 7.

7. Setup Certification Process and Enforcement

Based on the work of Step 1 (d) above, a process should be put in place that ensures impartiality, confidentiality, and predictability at all times. It will do this by being the Certification Authority for the program. This 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.

Clearly this path to a fully functional certification process is neither simple nor quick. As we will discuss in Whitepaper #3, the CSSCO will require a minimum of one year, to become fully operational and it could take considerably longer. Nor is this path the only possible way to achieve the CSSCO goals and we expect the later steps to change significantly as the CSSCO is created and begins to operate. However what is certain is that there are considerable expertise and resources available in the market to assist the CSSCO in achieving its objectives in the most efficient manner possible.

5 Conclusions

Creating a functional organization for compliance assurance and certification for the security of control system products is definitely an achievable goal. Hundreds of thousands of similar organizations have been created over the past twenty five years, so the path forward has been well tread by others before us. Both the certification processes and the formation of conformity assurance bodies are a well understood problem by experts in the field and can be based on proven methods and practices. We have laid out one possible path for the goals of the CSSCO to be achieved, but there are many others. What is important is that the CSSCO take advantage of the past experiences of other organizations, the experts in the field and the proven strategies so as to be as efficient as possible. It is also equally important that the CSSCO clearly define and articulate its goals and objectives early on in its formation.

In addition, the steps toward a successful CSSCO will require considerable resources. While financial support is one obvious aspect, technical support will be equally important. Member organizations must be willing to provide access to their own experts in order to facilitate the efficient flow of information for the purpose of satisfying the CSSCO objectives. The CSSCO will be attempting to tackle a number of difficult technical problems that will require synergy among its members. It will be critical to involve the best technical personnel available, so that the technical issues can be resolved correctly, efficiently and with the confidence of the entire industry.

References

-
- ¹ Allen Brown; "Best Practices in Compliance and Certification", Seminar on Best Practices in Standards Setting, Kavi Corporation, March 3, 2004, http://seminar.kavi.com/bios/3_3_materials/best_practices_brown.ppt , Page 10
 - ² Andrew Updegrove, "Forming, Funding, and Operating Standard-Setting Consortia," IEEE Micro, vol. 13, no. 6, pp. 52-61, Nov/Dec, 1993
 - ³ <http://www.consortiuminfo.org/laws/>
 - ⁴ Allen Brown, Page 9
 - ⁵ <http://www.consortiuminfo.org/forming/#cb>
 - ⁶ "Business Scenario: Certification" The Open Group, Revision 1.0 January 23, 2004, Pages 11 -13
 - ⁷ <http://www.iso.org/iso/en/comms-markets/conformity/iso+conformity-06.html>
 - ⁸ <http://publicaa.ansi.org/sites/apdl/Documents/Conformity%20Assessment/Product%20Certification%20Accreditation/Vintara%20Document%20Management%20Platform/TO%20VIEW%20ANY%20OF%20THE%20DOCUMENTS%20LISTED.htm>
 - ⁹ <http://www.nssn.org>
 - ¹⁰ <http://www.consortiuminfo.org/forming/#structure>
 - ¹¹ <http://www.eclipse.org/>
 - ¹² <http://www.consortiuminfo.org/evaluating/#eval>
 - ¹³ ISO/IEC 17000:2004, Conformity assessment -- Vocabulary and general principles