



ISA Security Compliance Institute

Call for Input for

Requirements and Test Specifications Embedded Controller Security Assurance

CFI ID-TCPIPSA-01
25 July 2008

Contact: Andre Ristaino
ASCI
67 Alexander Drive
RTP, NC 27709

Phone 919-990-9222
Fax 919-549-8288
aristaino@isa.org

ISA Security Compliance Institute Technical Steering Committee

I. SUMMARY

The ISA Security Compliance Institute is releasing this Call for Input to encourage a variety of experts to collaboratively create an Embedded Controller Security Assurance (ECSA) conformance specification that assures secure network communication for network connected devices. It will apply to all classes of embedded controllers with a focus on TCP/IP based controllers.

Devices may be used in such applications as automatic, direct control of primary actuators for process loops in plant controlling flow, temperature, pressure, etc. using wired communication within the loop, cascaded loops controlling a process variable (such as low frequency temperature loops), coordinated interlocks between automation cells, closed loop speed controls for rotating equipment.

Abbreviations used in this document:

1. ISA Security Compliance Institute Conformance Specification – *ISASecure*
2. Industrial Automation Control Systems - IACS
3. Call for Input – CFI
4. ISA Security Compliance Institute – Institute
5. ISA Security Compliance Institute Technical Steering Committee – TSC
6. Security Assurance – SA
7. Security Assurance Specification Working Group – WG
8. Automation Standards Compliance Institute – ASCI
9. Intellectual Property – IP
10. Standards Development Organization – SDO

The Institute’s CFI process is included in Section VII of this document and major steps with deadlines are listed in Annex B.

The Input is to be organized in a form that aligns with the ISA 99 Standard Foundational Requirements as defined in Part 1 of the ISA99 Standard. Foundational requirements are:

- FR 1 - Control access to selected devices, information or both to protect against unauthorized interrogation of the device or information.
- FR 2 - Ensure the integrity of data on selected communication channels to protect against unauthorized operation of the device or use of information.
- FR 3 - Ensure the integrity of data on selected communication channels to protect against unauthorized changes.
- FR 4 - Ensure the confidentiality of data on selected communication channels to protect against eavesdropping.
- FR 5 - Restrict the flow of data on communication channels to prevent the publication of information to unauthorized sources.
- FR 6 - Respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and automatically taking timely corrective action in mission critical and safety critical situations.

- FR 7 - Ensure the availability of all network resources to protect against denial-of-service attacks.

In the event that your Input addresses a subset of the seven foundational requirements, clearly identify which foundational requirements are being met by the Input.

While not yet defined in the ISA99 Standard, the Standard is expected to address security levels and map directly to security levels defined in the NIST 800-53 documentation. As such, we are seeking to map your Input to NIST 800-53 security levels and request that your Input include definitions of security levels for certified embedded devices.

II. ISA Security Compliance Institute Background and Purpose

Founded in 2007 as an Interest Area in the Automation Standards Compliance Institute, an ISA-owned not for profit entity, The ISA Security Compliance Institute's focus is to improve the security, confidence, integrity, and availability of components or systems used for manufacturing or control, and to provide criteria for procuring and implementing secure technology in the control system environment. Compliance with the Institute's *ISASecure* conformance specification will improve secure manufacturing and control system deployment, and will help identify security vulnerabilities and address them, thereby reducing the risk of compromising or causing manufacturing control systems degradation or failure.

The Institute's TSC was created by the Governing Board in June 2008 with the mission of managing the *ISASecure* specification development process. The output of the TSC is a recommended IACS security conformance specification. Example IACS applications within the scope of the Institute include automatic, direct control of primary actuators for process loops in plant controlling flow, temperature, pressure, etc. using wired communication within the loop, cascaded loops controlling a process variable (such as low frequency temperature loops), coordinated interlocks between automation cells, closed loop speed controls for rotating equipment.

CFI Goals and Objectives

The Institute's goal for this CFI is to define security requirements and a measurable conformance specification for SA of embedded controllers and their network communication. The intent is that this specification will ensure robust security and availability characteristics in devices and systems using the TCP/IP communication protocol in industrial automation control networks.

The specification must address the security needs in the industrial environment of wired sensors, actuators and other automation devices, as well as that of wired workers and first responders. Those needs include coexistence, robustness to interference, capability to maintain control during network attacks and interoperability with other wired plant infrastructure networks.

CFI Scope

This scope of the CFI for this project includes the SA specifications, security specifications, and management (including network and device configuration) specifications for wired embedded controllers in industrial device applications.

It is the intent of this project to address appropriate levels of coexistence with other wired devices anticipated in the industrial automation work space.

It is also the intent of this project to address appropriate levels of secure interoperability or inter-working with other technologies and protocols in the industrial automation work space.

All network connected devices utilize a command protocol for communicating with the device. In many cases this command protocol is a well known protocol such as MODBUS that is used by multiple controllers. The advanced *ISASecure* certification tests for conformance to the protocol's published security requirements where they exist, plus the ISA99 security requirements. The scope of the CFI includes test requirements for the most common industry standard communication protocols (such as IP, TCP, UDP, HTTP, etc), command protocols (such as MODBUS and PROFIBUS) and vendor specific proprietary protocols.

Institute TSC Role

The TSC's role is to manage and contribute to the development of the Institute's IP and technical work products, and for this CFI, complete a draft *ISASecure* specification. The ultimate decision of whether or not to adopt and promote the draft specification will be made via a majority vote of Institute's voting Technical Members with ratification by the Institute's Governing Board.

Upon ratification of the SA specification, the Institute may offer the specification to the ISA99 Standards Committee as a contribution to the collective input for the Committee's standards initiatives.

The approach used by the TSC will be open and collaborative among the members of the Institute, with the goal of achieving consensus when possible. Each participating company whose membership level carries voting rights is entitled to a single vote. The voting process on technical issues is determined by the ISA Security Compliance Institute's Bylaws and the Governing Board.

The TSC is empowered to solicit input from industry organizations who are non-members. However, donor organizations who are not Institute members will not have voting rights in the specification development and ratification process.

III. SA Specification in Relation to the *ISASecure* Roadmap

The SA specification will be delivered as the first release of the *ISASecure* conformance specification. The *ISASecure* conformance specification is designed to address security throughout the entire systems lifecycle beginning with supplier device development practices, off-the-shelf device/system security characteristics and, operator deployment, maintenance, and end of life security management practices. As such, the SA specification represents a minor portion of the entire *ISASecure* conformance specification articulated in the Roadmap.

IV. Relationship of the ISA99 Standard to the *ISASecure* Designation

The ISA99 Standards Committee is a globally recognized ANSI-accredited standards development activity sponsored by ISA and staffed by volunteer committee members. ISA is a Standards Development Organization (SDO) that does NOT engage in standards compliance

programs. ISA is comprised of members who are individuals sponsored by their respective organizations and employers.

The ISA Security Compliance Institute is an industry consortium comprised of companies, not individuals, who pay annual membership dues. It is NOT an ANSI-accredited standards development organization. The Institute's mission is to develop a set of Security conformance test specifications derived from industry standards such as ISA99, IEC Standards, and government regulations and to manage conformance programs and associated supporting activities.

The Institute was founded by thought leaders from major IACS suppliers and asset owner/operators. A number of these organizations also sponsor volunteers on the ISA99 Standards Committee. As such, a commitment exists to include the ISA99 Security Standards in the *ISASecure* conformance requirements as they become available. In the absence of ANSI accredited security standards, the Institute will base *ISASecure* specifications on draft work products from SDOs and input from members who represent a fair cross section of asset owners/operators, suppliers, and other interests. The Institute expects to donate key work products to the ISA99 Standards Committee who will properly vet the IP for inclusion in the ISA99 Standard. Further, the Institute will promote the output of the ISA99 Standards Committee.

V. Structure of *ISASecure* Specification and Development Sequence

The Institute's Roadmap for the *ISASecure* Specification groups device/system certifications (characteristics) separately from organizational certifications (practices). Device certifications will be pursued by the Institute in the near term and other dimensions of the *ISASecure* certification are being addressed as a separate effort in a lag phased schedule. **This CFI is specific to devices/systems only** and addresses the Embedded Controller SA segment of the *ISASecure* specification. Remaining segments of the *ISASecure* specification will be defined in future releases of the *ISASecure* specification.

Proposed *ISASecure* Certification Levels

Where appropriate, the Institute has established multiple certification levels for the *ISASecure* conformance specification for devices, grouped by device/system class. Separately, *ISASecure* designations are awarded for supplier practices and asset owner/operator practices. The certifications addressed by this CFI include devices only:

- Embedded Controllers – Level 1 Certification
- Embedded Controllers – Protocol Certification.

Embedded Controllers – Level 1 Certification

Embedded Controllers are those devices that are interconnected to the IACS using commercial networking technology such as Ethernet and IP protocols. Embedded Controllers are a class of devices that run an embedded operating system and code. The types of embedded devices to be considered for this class of certification are devices such as network connected Programmable Logic Controllers (PLCs), Safety Controllers, Process Controllers, Batch Controllers and, Remote Terminal Units.

The level 1 certification is a basic level of certification to assure that the network connected device is immune to issues related to basic IP and TCP/UDP network attacks and denial of service. The purpose of the level 1 certification is to assure that devices are not affected by excessive or malicious network traffic in a way that causes the devices to fail to perform their primary function of controlling the process.

Embedded Controllers – Protocol Certification

All Embedded Controller devices as described above utilize a command protocol for communicating with the device. In many cases this command protocol is a well known protocol such as MODBUS that is used by multiple controllers. The Protocol Certification tests for conformance to the protocol's published security requirements where they exist, plus the ISA99 security requirements.

Respondents should list this as an additional certification level if your specification includes requirements that are appropriate for this topic area.

VI. Intellectual Property

Institute specifications and conformance to *ISASecure* are affected by patents and copyrights and the associated intellectual property rights of the holders who contribute them to the *ISASecure* Specification.

To ensure usefulness to the Institute, all written or electronic contributions in response to this CFI automatically imply that the submitting participant agrees that:

1. The WG may publicly disclose the contribution, and reference the name(s) of the participant(s) for the purpose of acknowledging and publishing the contribution.
2. The participant identifies any holders of copyright interests in the contribution, and affirms that the copyright holder grants to ASCI a perpetual, irrevocable, non-exclusive, royalty-free, worldwide license to include the contribution and derivative works within any document arising from the work of the Institute.
3. If the resulting candidate specification(s) may require the use of a patented invention, the participant identifies any holders of patent(s) or patent interests in the contribution, and affirms that the patent holder agrees to comply with policies contained in the ASCI Patent Policy. The participant or patent holder must provide ASCI with either: a general disclaimer to the effect that such party does not hold and does not presently anticipate holding any invention the use of which would be required for compliance with the proposed specification or a written assurance that either: (a) a license will be made available without compensation to applicants desiring to utilize the license for the purpose of implementing the specification, or (b) a license will be made available to applicants royalty free, that are demonstrably free of any unfair discrimination.

NOTE: The form for the ASCI Patent Policy and Letter of Assurance is in Annex A

Unless there is no alternative, patented or proprietary technology should not be included in *ISASecure*. Patents may be included in *ISASecure* only if the patent holder agrees to permit universal, royalty-free use of the patent for purposes of meeting *ISASecure* or agrees to license

the patent on uniform, royalty-free basis, non-discriminatory, and reasonable terms. If anyone believes that a patent may cover a part of *ISASecure*, it should be brought to the attention of the Institute's Governing Board and the Institute's Executive Director.

ISASecure is copyrighted and trademarked by the Institute. Institute specifications should not include any materials not specifically prepared by donor company participants for inclusion in *ISASecure* without permission from the copyright holder, royalty-free, in a form satisfactory for broad publication and distribution of the specification with that material. Donors should notify the TSC chair and Institute's Executive Director of any excerpted text or artwork that may require a copyright release from another organization before the material is submitted to the TSC for consideration.

VII. Technology Selection Process and Schedule

The selection and evaluation process steps are listed in Annex B showing key dates and responsibilities. The Embedded Controller SA is a subset of topic areas that are identified in the *ISASecure* Roadmap. As such, the Institute expects to harmonize donated IP and develop *ISASecure* test specifications for this limited scope by the end of 2008. Key deadlines listed in Annex B include:

Date	<i>ISASecure</i> Responsibility	Proposer Responsibility
01 August 2008	Issue Call for Input	Review CFI
01 August 2008-15 August 2008	Add names to tcpipqos@isa-online.org and to 'Intent to Propose' list.	Deadline: Notify aristaino@isa.org by email of intent to propose and request to be added to email reflector.
15 August 2008	Host the Input Teleconference Explain process, content, format, IP issues, confidentiality, and antitrust. Deadline for Notice of Intent.	Mandatory participation in Input teleconference. Signed NDA required to participate for ISCI non-members
31 August 2008	Input due to Institute; content and format specified to proposers.	Deadline: Email electronic format Input to aristaino@isa.org

RELEASE DATE: 01 August 2008 CFI is published on ISA99 reflector, press release, and mailer to ISA database.

NOTICE OF INTENT: Due 15 August 2008 (11 PM Eastern Daylight saving time)

The Notice of Intent is a process step in which all interested parties are asked to identify their intention to submit Input. **YOU MUST DECLARE YOUR INTENT.** You may decide later, if necessary, to retract your intent, but it must be declared. Send your notification of intent to aristaino@isa.org. If your response is not acknowledged within two business days please resend. All proposers are required to join the ISA listserv for the SA work group tcpipqos@isa-online.org. Please submit your request to join the tcpipqos@isa-online.org listserv to aristaino@isa.org.

INPUT TELECONFERENCE: 15 August 2008 (Eastern Daylight Time)

Proposers are required, to provide and present a summary version of their Input to the Institute in electronic format for review in advance. It also allows the TSC to review the requirements and selection criteria documents for correctness.

The teleconference agenda will include:

- Presentation by the Institute of available Use Case information, and discussion.
- Walk-through of the Institute's Input and evaluation process. At this meeting any revisions to the project plan for the development of *ISASecure* SA specifications will be discussed.
- PowerPoint or similar presentations (i.e. public disclosure) by proposing companies and individuals addressing the Institute's CFI
- A panel discussion will be held at the conclusion of the presentations where proposers will address questions and concerns from all attendees including fellow panelists.

INPUT DUE: 31 August 2008 (due 11 PM Eastern Standard Time)

All proposers are required to provide and present a final version of their Input to the TSC in electronic format by email to tcpipqos@isa.org.

PROCESS:

All submissions to the CFI shall be formatted as per the TSC format with a cover page. The cover page releases the submission for internal use by the Institute. Rules for Institute submissions and formats for Microsoft Word and Power Point documents will be distributed via the tcpipqos@isa-online.org listserv.

All requests for procedural help, submissions, and questions should be submitted to aristaino@isa.org.

Once the Input process has completed, the TSC will vote to determine if the proposed contributions should be included in the baseline for the draft *ISASecure* SA specification using a simple majority and subsequently ratified by the Institute's Governing Board.

The ISA Security Compliance Institute through this CFI is making a public solicitation to vendors who currently test network stacks in an industrial setting (including but not limited to Mu Security, Codenomicon, and Wurldtech) to determine their interest in donating compliance requirements and test specifications that comprise their respective test suites. The goal is to have the testing vendors donate their test requirements to the ISA Security Compliance Institute for inclusion as the *ISASecure* Embedded Controllers Level 1 Certification test requirements.

The donated specifications would be evaluated, rationalized, reformatted into the *ISASecure* style. Contributing vendors will participate in the Institute's TSC working group to complete the *ISASecure* draft specification and the test requirements will be voted on for approval by the ISA Security Compliance Institute Membership.

The TSC will schedule a weekly conference call for this CFI and may call additional meetings as needed.

Working sessions may also be scheduled from time to time to create, review, and finalize *ISASecure* work products. These working sessions will be open to any representatives of donors, but are primarily intended for donor representatives who are deeply involved in the process.

Where appropriate, the Institute plans to contribute *ISASecure* work products to the ISA SP99 Part 4 working group for consideration as part of the ISA99 Part 4 Standard.

VIII. *ISASecure* Proposer Conference and Mailing List

As stated above, an Input teleconference will be held during the week of 15 August 2008. In the open and collaborative spirit of the TSC, this conference is intended to help participants improve their Input and identify potential collaborators.

The agenda will include:

- Presentation by *ISASecure* of available information, and discussion.
- Walk-through of the *ISASecure* Input and evaluation process. At this meeting a project plan for the development of *ISASecure* will be discussed and will include a down-selection process so as to encourage collaboration particularly if there are a significant number of Input.
- PowerPoint or similar presentations (i.e. public disclosure) by proposing companies and individuals addressing the *ISASecure* technical CFI.
- Panel discussion at the conclusion of the presentations where a panel (consisting of the proposers) will address questions and concerns from all attendees (including fellow panelists).

Participants in the conferences are expected to cover their own travel expenses. There may be modest fees to cover the cost of holding the events.

The *ISASecure* Working Group will accept written questions and distribute responses through the email reflector at tcpipqos@isa-online.org. Questions should be directed to the email reflector. Requests to be included on the reflector mailing list (with primary and secondary email contact) should be sent to aristaino@isa.org.

Thank you in advance for your constructive participation in *ISASecure*.

Annex A

Recognizing the relevance of patented technology and copyrighted material to the development and use of Conformance Specifications and Test Kits (hereinafter called **specifications**) for ASCI Interest Areas (hereinafter called **Institutes**), the following rules with respect to disclosure, enforcement, and licensing of patents and or copyrights have been adopted. These rules are intended to supplement the Automation Standards Compliance Institute Intellectual Property Rights (IPR) Policy published in the ASCI Membership Agreement. Any person or entity involved in the conformance specification development process (hereinafter called **process**) as a member, participant, or contributor, voting or non-voting, of an Institute, Institute Working Group, Institute Task Group, Institute Study Group, or any other sub-group formed within an ASCI Institute, is bound by these rules and is deemed to have agreed and acquiesced to these rules by virtue of such participation.

1. Disclosure by individual participants. Each individual participating in the process shall disclose to the Institute any patents or published applications held by the individual or any firm the participant represents, of which the participant is aware and which, to the best of the participant's knowledge, has a likelihood of being infringed by compliance with an Institute's specification.
2. Disclosure by participating firms. Companies, organizations, agencies, and other firms participating in the process through their representatives shall disclose to the Institute any patents or published applications held by them and which they know or have reason to believe has a likelihood of being infringed by compliance with an Institute's specification.
3. Timing of disclosure. Disclosure shall be made promptly upon the individual or firm becoming aware of a patent or published patent application required to be disclosed as provided above.
4. Letter of assurance. For any patent or patent application disclosed, ASCI shall request a Letter of Assurance in which the holder agrees either: (a) not to enforce its patent with respect to compliance with the specification, or (b) to grant a license to an unrestricted number of applicants on a worldwide, non-discriminatory basis, with NO royalties and fair and reasonable terms and conditions.
5. Default provision. With respect to any patent or patent application owned or controlled by a individual participant or firm that may be infringed by compliance with a specification that is not disclosed, such person or participant shall either (a) not enforce its patent with respect to compliance with an Institute's specification, or (b) grant a license to an unrestricted number of applicants on a worldwide, non-discriminatory basis, with NO royalties and fair and reasonable terms and conditions.

With respect to any copyrighted material owned or controlled by an individual participant or firm, any and all copyrighted material contributed by that individual participant or firm during the specification development process, shall become the property of the Institute.

6. Good faith. Every participant in the conformance specification process, individuals and firms, shall at all times act in good faith and in an open and honest manner.

Please mail or FAX to: Andre Ristaino, ASCI c/o ISA, 67 Alexander Drive, Research Triangle Park, NC 27709 USA
FAX: 919-549-8288

A. PATENT HOLDER/ORGANIZATION:

Legal Name of Person or Entity (the "Patent Holder"):

B. PATENT HOLDER'S CONTACT FOR PATENT LICENSING:

Name & Department: _____

Address: _____

Telephone: _____ Fax: _____ E-mail: _____

C. PROPOSED INSTITUTE SPECIFICATION:

Number: _____

Title: _____

D. PATENT HOLDER'S POSITION ON ENFORCEMENT OR LICENSING PATENT RIGHTS:

Those patent(s) and/or pending applications owned or controlled by the Patent Holder that would be, or that Patent Holder believes may be, infringed by compliance with the proposed Institute's Conformance Specifications, are as follows:

Patent Number(s): _____

Title(s): _____

The Patent Holder states that its position with respect to enforcement or licensing such patent(s) is as follows (*check one box only*):

- 1. The Patent Holder will not enforce its patent so as not to impede compliance with the proposed ASCI Institute Conformance Specification.
- 2. The Patent Holder will grant a license to an unrestricted number of applicants on a worldwide, non-discriminatory basis and on fair and reasonable terms and conditions, with NO royalties, to allow compliance with the proposed ASCI Institute Conformance Specification.
- 3. The Patent Holder is currently undecided whether it will adopt position 1 or 2, above, but will declare its position to ASCI by no later than the date of issuance of the first ballot on the proposed ASCI Institute's Conformance Specification.

E. SIGNATURE:

The person signing below certifies that he/she is duly authorized to execute this Letter of Assurance on behalf of the Patent Holder:

Print name of authorized person: _____

Title of authorized person: _____

Signature of authorized person: _____

Date: _____

Note: This assurance applies from the date of the Institute's Specification approval to the date of the Institute's Specification withdrawal and is irrevocable during that period.

Annex B

Major Steps in *ISASecure* Call for Input Process

Date	TSC Responsibility	Proposer Responsibility
01 August 2008	Issue Call for Input	Review CFI
01 August 2008 15 August 2008	Add names to tcpipqos@isa-online.org and to 'Intent to Propose' list.	Deadline: Notify aristaino@isa.org by email of intent to propose and request to be added to email reflector.
15 August 2008	Host the Input Teleconference Explain process, content, format, IP issues, confidentiality, antitrust	Mandatory participation in Input teleconference. Signed NDA required to participate for ISCI non-members
31 August 2008	Input due to Institute; content and format specified to proposers.	Deadline: Email electronic format Input to aristaino@isa.org
15 September 2008	Notify proposers of ISCI intent to include / forgo donated IP described by Input.	Maintain confidentiality.
30 September 2008	1st draft Embedded Controller SA conformance specification submitted for review by TSC	Accepted proposers only. Participate collaboratively with ISCI to develop Embedded Controller SA conformance specification.
14-16 October 2008	ISCI announces Embedded Controller SA <i>ISASecure</i> specification at ISA Expo 2008	Joint ISCI press releases pre-approved for Expo 2008.
14 November 2008	Final <i>ISASecure</i> Embedded Controller SA conformance specification submitted to ISCI Governing Board for ratification.	Accepted proposers only. Participate collaboratively with ISCI to develop Embedded Controller SA conformance specification