Setting the Standard for Automation™

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

ISA-SP100.14
Call for Proposal

Wireless Network Optimized for Industrial Monitoring

14 July 2006

ISA
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709
PHONE (919) 549-8411
FAX (919) 549-8288
E-MAIL info@isa.org
www.isa.org

Call for Proposals (CFP)
SP100.14 – Wireless Network Optimized for Industrial Monitoring

Revision History

Revision	**Version**	**Date**	**Description**
0	R6	14-July-06	First release of CFP

I – Summary

CFP RELEASE DATE: 14 July 2006

Candidate technical proposals are requested by the ISA SP100.14 work group (WG) to form the baseline for its draft standard that will address wireless networking for Industrial Monitoring. This document describes the process and requirements for responding to this call for proposals.

The SP100.14 Work Group is chartered to develop an ISA SP100 Standard that will define the OSI layer specifications (e.g. PHY, DLL, etc), security specifications, and management (including network and device configuration) specifications for wireless devices, optimized for classes 4 through 5 industrial device applications and with consideration for class 0-3 applications.

This CFP solicits proposals and data that will form the baseline of a draft standard that will fulfill the scope and purpose of SP100.14. Additionally, there are three (3) other documents that the proposer is advised to read: the Use Case Summaries, the Technical Requirements Document (TRD), and the Evaluation Criteria. All of these documents will be accessible on the SP100 committee web site subsequent to the release of this CFP. Please note that the target set of use cases has only been partially documented and therefore the technical requirements are subject to change.

CALL FOR INTENT: Due 1 August 2006

The Call for Intent is a process in which all interested parties are asked to identify their intention to submit proposals, with an abstract. The abstract should include a high level description of the scope of the proposal as well as the overall approach. YOU MUST DECLARE YOUR INTENT. You may decide later, if necessary, to retract your intent, but it must be declared. The purpose of this call is to enable scheduling for the optional preliminary Proposer Conference in September as well as assignment of document numbers.

The Intent to Propose is due on 1 August 2006. Send your notification of intent to ISASP10014CFP@isa.org. If your response is not acknowledged within two (2) business days please resend.

All submissions to the CFP shall be formatted as per the ISA format with a cover page. The cover page releases the submission for public use by the ISA. Rules for ISA submissions and formats for Microsoft Word and PowerPoint documents may be found on the SP100 web site.

The CFP process is described in more detail in the sections IX and X.

II – ISA-SP100.14 Call for Proposal Scope

ISA-SP100.14 is publishing this Call for Proposal in order to encourage a variety of experts to collaboratively create a networking standard for low-cost wireless industrial monitoring devices. During the evaluation process, preference will be given to proposals where sufficient data is readily available to assess the validity of claims. The ISA-SP100.14 Working Group requests proposals that are targeted at ISA-SP100 Classes 4-5, including such applications as process monitoring, equipment monitoring, environmental monitoring, inventory monitoring, asset management, and validation. These applications may include tasks that are classified as non-critical control.

III – ISA-SP100.14 Background and Purpose

Founded in 1945, ISA is a leading, global, nonprofit organization that is setting the standard for automation by helping over 30,000 worldwide members and other professionals solve difficult problems. Based in Research Triangle Park, North Carolina, ISA develops standards; certifies industry professionals; provides education and training; publishes books and technical articles; and hosts the largest conference and exhibition for automation professionals in the Western Hemisphere.

The ISA-SP100 Committee will establish standards, recommended practices, technical reports, and related information that will define procedures for implementing wireless systems in the automation and control environment with a focus on the field level. Guidance is directed towards those responsible for the complete life cycle including the designing, implementing, on-going maintenance, scalability or managing manufacturing and control systems, and shall apply to users, system integrators, practitioners, and control systems manufacturers and vendors.

The Committee's focus is to improve the confidence, integrity, and availability of components or systems used for manufacturing or control, and provide criteria for procuring and implementing wireless technology in the control system environment. Compliance with the Committee's guidance will improve manufacturing and control system deployment, and will help identify vulnerabilities and address them, thereby reducing the risk of compromising or causing manufacturing control systems degradation or failure.

The overall CFP process as defined by the ISA SP100 Committee is included in this document as Annex C. The major steps in the CFP process are listed in Annex D.

The ISA-SP100.14 Working Group was created by ISA-SP100 in April 2006, with the mission of recommending a wireless communication standard for industrial monitoring. Example applications include process monitoring, equipment monitoring, environmental monitoring, inventory monitoring, asset management, validation, and potentially slow non-critical control.

ISA-SP100.14 Purpose

To provide a wireless connectivity standard for class 4 (alerting) and class 5 (logging and downloading/uploading) applications (see Table 1 – Usage classes). The intent is that this standard will allow compliant devices that are relatively low complexity, reasonable cost, and low power consumption to allow long battery life where needed. The communication data rate must be sufficient to satisfy a set of generic needs such as alerting, logging, and downloading/uploading. The standard must also address the specific needs of sensors and automation in the industrial environment such as coexistence, robustness to interference, interoperability with plant infrastructure networks, etc.

ISA-SP100.14 Working Group Scope

This project will define the required and optional OSI layer specifications (e.g. PHY, DLL, etc), security specifications, and management (including network and device configuration) specifications for wireless devices serving the Class 4 and Class 5 industrial applications operating within a facility. Fixed or moving devices will operate with very limited power consumption. Handheld HMI devices will operate with variable latency and throughput requirements. Since this industrial environment could include high power interference sources the standard will also address the network's robustness. It is the intent of this project to address appropriate levels of coexistence with other wireless devices anticipated in the industrial work space, such as 802.11x, 802.16x, cell phones, et al. It is also the intent of this project to address appropriate levels of interoperability with communication networks and field busses anticipated in the industrial work space, such as 802.3, 802.11x, 802.16x, HART, et al.

ISA-SP100.14 Working Group Role

The ISA-SP100.14 committee's role is to develop a draft standard. The ultimate decision of whether or not to adopt and promote the standard will be made by ISA-SP100's parent organization, ISA. The working group may be disbanded or restarted at the discretion of ISA without prior notice.

On completion of the SP100.14 standard, it will be made available to other standards organizations such as IEC as a baseline for other standards initiatives.

The approach used by the ISA-SP100.14 group will be open and collaborative, with the goal of achieving consensus when possible. Each participating company will get a single vote, with voting rights based on participation. The ISA-SP100 voting membership is by election and the rules are set by the ISA parent organization.

IV – ISA-SP100 Usage Classes

Analysis of the applications of inter-device industrial wireless communications resulted in a partitioning of those communications into six classes. These classes were introduced in ISA-SP100 and are summarized in tabular form in Table 1.

Table 1 – Usage classes

Category	Class	Application	Description	
Safety	0	Emergency action	*(always critical)*	↑ Importance of message timeliness increases
Control	1	Closed loop regulatory control	*(often critical)*	
	2	Closed loop supervisory control	*(usually non-critical)*	
	3	Open loop control	*(human in the loop)*	
Monitoring	4	Alerting	*Short-term operational consequence (e.g., event-based maintenance)*	
	5	Logging and downloading/uploading	*No immediate operational consequence (e.g., history collection, sequence-of-events, preventive maintenance)*	

Alarms and communications with wireless workers are within the scope of SP100.14. Alarms can be of any class; they may require either human or an automated response. The communications of wireless workers fall into classes 3 - 5.

Batch levels 3 and 4 (as defined by ISA S88, where L3 = "unit" and L4 = "process cell") can be of Class 2, Class 1, or even Class 0, depending on their function.

ISA-SP100.14 focuses on Class 4 and 5 applications. The last digit of "ISA-SP100.14" is intended to indicate classes 4 and 5 inclusively.

ISA-SP100 has identified examples of the wireless automation classes in Table 1:

Class 5: Monitoring without immediate operational consequences
This class includes items without strong timeliness requirements. Some, like sequence-of-events logs, require high reliability; others, like reports of slowly-changing information of low economic value, need not be so reliable since loss of a few consecutive samples may be unimportant.

Class 4: Monitoring with short-term operational consequences
This class includes high-limit and low-limit alarms and other information that might instigate further checking or dispatch of a maintenance technician. Timeliness for this class of information is typically low (slow), measured in minutes or even hours.

Class 3: Open loop control
This class includes actions where an operator, rather than a machine, "closes the loop" between input and output. Such actions could include taking a unit offline when conditions so indicate. Timeliness for this class of action is human scale, measured in seconds to minutes.

Class 2: Closed loop supervisory control
This class of closed-loop control usually has long time constants, with timeliness of communications measured in seconds to minutes. Examples are batch unit and equipment selection.

Class 1: Closed loop regulatory control
This class includes motor and axis control as well as primary flow and pressure control.

Class 0: Emergency action
This class includes safety-related actions that are critical to both personnel and plant. Most safety functions are, and will be, performed through dedicated wired networks to limit both failure modes and susceptibility to external events or attack. Examples are safety interlock, emergency shutdown, and fire control.

V – Relationship of ISA-SP100.14 to ISA-SP100.11

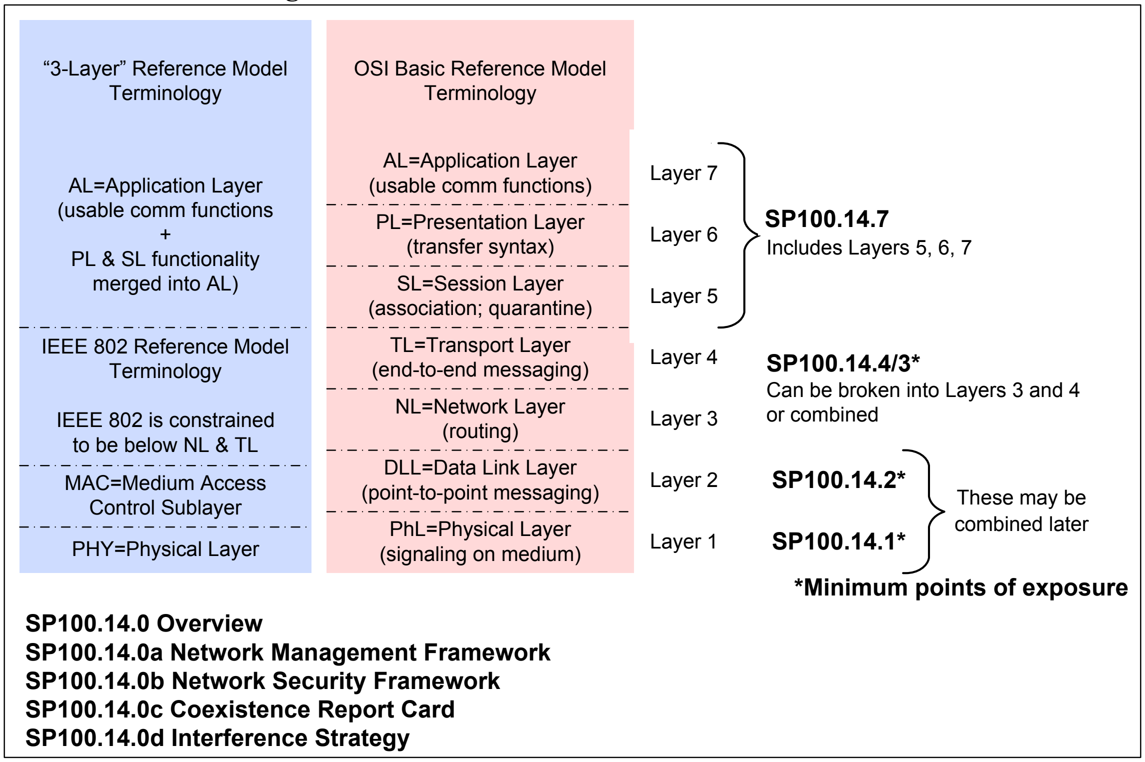
The ISA-SP100.11 Working Group was formed at the same time as ISA-SP100.14. The two efforts are intended to be complementary.

ISA-SP100.14 is optimized for Classes 4-5, and may meet some of the performance objectives of Classes 0-3. ISA-SP100.11 and ISA-SP100.14 have substantially overlapping members, and those individuals will identify common ground and assure integration of the two efforts.

VI – Structure of ISA-SP100.14 Standard

The overall structure envisioned for the ISA-SP100.14 standard is shown in Figure 1. It is expected that all sections shown, except for ISA-SP100.14.7 (application layer), will be covered in the first version of the standard.

Figure 1 – Overview of ISA-SP100.14 Standard



Proposals may focus on certain aspects of the total solution, such as physical layer, networking, or security. Proposals that only address certain aspects or layers must be structured such that they can be used as building blocks in a total solution; these will be considered for the appropriate aspects of the overall standard. Complete proposals should address all of the requirements and use cases, and it is recommended that complete proposals be structured so that portions can be used in combination with other proposals.

VII – Scope of ISA-SP100.14

Overview

The immediate goal of ISA-SP100.14 is to enable vendors to build compatible network devices, shown as Field, Routing, Handheld, and Gateway devices in Figure 2. Areas of initial focus are indicated by red ovals.

Figure 2 – Minimum scope of ISA-SP100.14 Standard

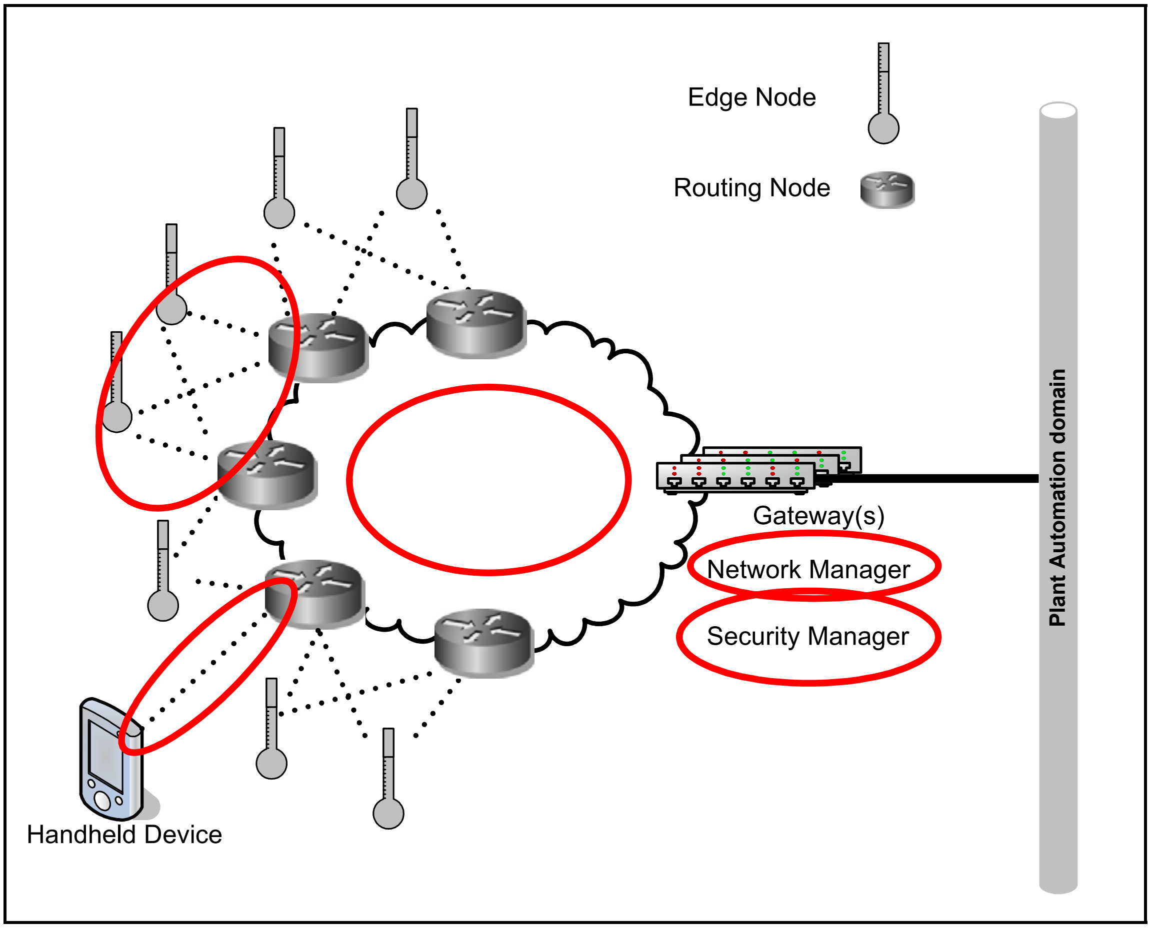


Figure 2 is intended to emphasize the key goal of a standardized link to Field Devices and Handheld Devices, with integrated Network Management and Security. This graphic is not intended to be precise or to constrain the creativity of proposals. For example:

- Field Devices may connect directly to Gateways even if this isn't explicitly shown in the graphic.
- The network cloud in Figure 2 is drawn so as to not limit proposals to specific network architectures. The red oval drawn inside the cloud indicates that the network is within the scope of SP100.14.
- The link drawn to handheld devices is not intended to prescribe a particular type of connection.

Field Devices may be sensors, actuators or I/O interfaces. They may also include "intelligent" field devices that already exist in a plant, but which lack connectivity to the Plant Network. These Field Edge nodes will connect to nearby Routing nodes, which will in turn provide connectivity to a Gateway. In this context, the current members of ISA-SP100.14 agreed on a minimum scope for the first standard, shown as red ovals in Figure 2. More detail will be provided in the Technical Requirements Document.

It is generally expected that Routing nodes will be stationary, while limited mobility should be supported for Edge nodes. For example, Field Devices may be used for sensors on an overhead crane. Performance tradeoffs related to mobility should be discussed in proposals. Some Field Devices are required to run for years on battery power.

Device localization is not formally within the scope of SP100.14, but if a proposal has location capabilities this would be of interest. As a simple example, the protocol might enable a Field Device to transmit frequent beacons on command, enabling a Handheld user to find the device by signal strength methods.

While Edge nodes and Routing nodes are drawn separately, it is expected that (for at least some proposals) Field Devices might also be Routing nodes in a number of configurations and vice versa. Mechanisms used to form a network must be specified so that network devices are interoperable.

Proposals may support various architectures, adaptable based on application requirements. For example:

- Routing nodes may form a multihop network that directs data to and from a Gateway.
- Routing nodes may be zero or more hops away from a wired or wireless backbone, which may be used to tunnel messages to a Gateway.
- Devices may be installed in a cluster that is located remotely from a Gateway. In this case, the devices may be directly or indirectly connected to a wireless bridge that tunnels messages to and from the Gateway.
- Routing may support peer-to-peer communication.

These illustrative examples are not intended to be a complete set of use cases, or to constrain proposals. Use cases will provide a reference point for evaluation, but not a complete set of application scenarios.

Successful proposals will be scalable from tens to thousands of Field Devices, and from small clusters to a large outdoor plant. Initial installations may be limited in scope, potentially with a limited number of devices sparsely distributed through a facility. With expansion over time, there are realistic commercial scenarios for clusters of 10,000 devices actively participating in a network and reporting data periodically.

The network should be able to accommodate a heterogeneous mixture of devices utilizing a variety of power sources, ranging from primary cell batteries to line power. It is anticipated that some if not most proposals will support multihop routing. Such proposals should include plausible options for both line power and battery power for the Routing nodes. Battery-powered Routing nodes may have increased latency and reduced routing capacity. The option for a Routing node to be battery-powered should not be at the expense of router capacity and performance when power is freely available.

A handheld device is shown in Figure 2. It is intended primarily for configuring and monitoring the Field Devices either directly or through the infrastructure, with latencies that a human operator would find reasonable. Figure 2 shows a connection to a Routing node, which is not intended to preclude proposals capable of connecting directly with Edge nodes.

Security is a pervasive requirement for the ISA-SP100.14 standard. This is shown as a "Security Manager" in Figure 2, which is intended to be the trust center for the network.

The backend of the Gateway and the front end of the Field Device is excluded from the Minimum Scope in Figure 2. This reflects the absence of an application layer (ISA-SP100.14.7) in the first version of ISA-SP100.14; and indicates that (for now) the standard will not define a connection between sensor/actuator and gateway at an application level. ISA-SP100 may adopt one or several standard application layers in the future, such as ZigBee®, IEEE 1451.5, or HART®. A single ISA-SP100.14 network infrastructure should be able to seamlessly and simultaneously handle traffic from multiple application layers. ISA-SP100.14 encourages proposals that focus on an open interface with existing and emerging application layer standards.

Scheduled and Event-driven Messages from Class 4 and 5 Devices

As indicated in Figure 2, ISA-SP100.14 is focused on the network connection between Field Devices and Gateways.

Class 4 and 5 are defined as "Monitoring" applications. Typical examples include temperature, pressure, vibration, switches, signal level, flow, fluid levels, volts, amps and phase.

Monitoring typically involves a periodic report of a limited amount of data, such as temperature, pressure, or signal level. For many applications, reports can occur on a schedule every one or several minutes. However, some applications require an update every few seconds. The criticality of high update rates will be further defined in the Technical Requirements Document and the Evaluation Criteria. Monitoring applications can also require a variable update rate – so called "bandwidth on demand" – where the update rate needs are determined by the state of the process. For example, an application may need to send periodic measurements of a parameter under normal conditions and then to stream waveform data when more accurate condition assessment is required.

Monitoring messages may be periodic and/or event-driven. For example, temperature may be reported every 5 minutes on a regular schedule, but also reported immediately when a temperature threshold is exceeded.

Latency of the report may be important, depending on the application. Controlled and predictable latency is generally more relevant for event-driven reporting.

Class 4 and 5 devices may periodically need to report blocks of data comprising multiple packets. For example, a vibration sensor may capture a 25 KB waveform daily, and transmit this information to a gateway for processing. As another example, an application layer (such as HART or IEEE 1451) may exchange relatively lengthy blocks of data with a Gateway or Handheld for device configuration.

There may be significant latency between transmission of a signal from a Field Device and its reception at a Gateway. Nonetheless, it may be necessary to precisely timestamp data reports. For example, event-driven data reports may need an accurate timestamp for SOE (sequence of events) reporting. As another example, waveform capture may need to be triggered simultaneously on multiple nodes, such as to measure vibration simultaneously from multiple nodes and combine the time-correlated waveforms in a host application or in another Field Device.

Field Device Polling and Configuration

Proposals should discuss tradeoffs related to device polling.

For some applications, it may be necessary to query a Field Device and receive a response within a few seconds. These queries may originate from a workstation or from a handheld. Such applications may relate to a data request or device configuration, and as such may involve a single packet of information or multiple packets.

Host-initiated communications may be a challenge for battery-powered devices on a low duty cycle. For example, a Field Device may be configured to report data every two minutes, and be out of communication between reports. A two-minute response time may be unacceptable for some applications; tradeoffs related to reduced latency should be discussed in proposals.

Battery Life and Device Life Cycle Cost

ISA-SP100.14 is targeting small, easily deployed, battery-operated devices that can operate in a wide range of environmental conditions found in industrial settings. As such, plausible estimates of radio module cost and battery life should be provided for several different scenarios and use cases. As part of its Evaluation Criteria, ISA-SP100.14 will identify reference battery specifications and application scenarios to be used for estimates of battery life under a variety of boundary conditions. Final proposals will need to provide energy consumption profiles for each operating state, including peak transmit and receive current consumption as well as sleep current consumption.

Some applications may involve alternative power sources such as solar, vibration harvesting, and thermopiles.

A key component of life cycle cost is the ability to easily setup, monitor, diagnose, and reconfigure the network over a period of years. Proposals will be expected to balance tradeoffs between the cost/complexity of individual devices, versus the cost of ownership for a system that includes such devices.

Security

The ISA-SP100.14 Working Group recommends that all proposals include a pervasive, manageable, and seamless framework for security.

ISA-SP100.14 welcomes proposals that focus on security. Security topics of interest include message privacy, message integrity, and authentication. Details will be provided in the Technical Requirements Document and Evaluation Criteria.

Radio Selection

ISA-SP100.14 intends to leverage the extensive specification and coexistence work of IEEE 802, especially 802.15, 802.11, and 802.19. Preference will be given to physical devices that are within the scope of these IEEE efforts.

ISA-SP100.14 will be structured in a way to smoothly accommodate alternative radios in the future.

Non-ideal radio path loss due to multipath, reflections, diffractions, shadowing, and non-LOS (line of sight) must be assumed.

Proposals should be tolerant of commonly encountered interference in factories, such as from microwave ovens, IEEE 802.11 and other IEEE radios, RFID readers, and proprietary frequency hoppers. Proposals should also minimize interference with other radio systems, especially IEEE 802.11.

Preference will be given to physical layer proposals based on mature, field-proven technologies with transceivers that are inexpensively available from multiple sources.

Physical layer proposals should clearly address international radio regulations, with particular attention to unlicensed operation.

Physical layer proposals should include complete specifications for radio performance including modulation techniques, bandwidths and frequency requirements, output power and unintended radiated energy levels and spectrum, receiver blocking characteristics, sensitivity, noise floor, coding gains, etc. This information is required so that an estimate for range, coexistence and robustness can be assessed. If features such as power control, antenna diversity, directional antennas, are to be included in the evaluation – they must be clearly defined in the proposals.

VIII – Intellectual Property

ISA standards are affected by intellectual property considerations including patents and copyrights.

The submission of any contribution in response to this CFP is affected by intellectual property considerations including patents and copyrights.

All written or electronic contributions in response to this CFP automatically imply that the submitting participant agrees that:

1. The ISA SP100 working group 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 ISA 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 SP100 committee.

3. If the resulting candidate standard(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 ANSI Patent Policy and ISA Patent Policy. The participant or patent holder must provide ISA 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 standard 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 standard, or (b) a license will be made available to applicants under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

NOTE: The ANSI Patent Policy can be found at http://public.ansi.org/ansionline/Documents/News%20and%20Publications/Links%20Within%20Stories/ANSI%20Patent%20Policy.doc"

NOTE: The form for the Patent letter of Assurance can be found in Annex B.

Unless there is no alternative, patented or proprietary technology should not be included in an ISA standard. ISA is a member of ANSI and follows its policy on inclusion of patents in standards. Patents may be included in an ISA standard only if the patent holder agrees to permit universal, royalty-free use of the patent for purposes of meeting the standard or agrees to license the patent on uniform, non-discriminatory, and reasonable terms. If anyone believes that a patent may cover a part of an ISA standard, it should be brought to the attention of the committee chair and ISA staff.

ISA standards are copyrighted by ISA. ISA standards should not include any materials not specifically prepared by committee members for inclusion in the standard without permission from the copyright holder (royalty-free if possible) in a form satisfactory for broad publication and distribution of the standard with that material. Committee members should notify the committee chair and ISA staff of any excerpted text or artwork that may require a copyright release from another organization before the material is submitted to the committee for consideration.

More detail can be found at: www.isa.org/ISAStandardsProcedures

IX – ISA-SP100.14 Working Group Technology Selection Process and Schedule

ISA-SP100.14 is publishing this Call for Proposal in order to encourage a variety of companies and experts to propose a networking standard for low-cost wireless industrial monitoring devices. The process is top-down, starting with presentations and proceeding to final proposals. Each stage will be increasingly selective, and involve a growing level of commitment by proposers and collaboration among proposers.

Three meetings of the full working group are planned for 2006: a Proposer Conference in Durham NC during the week of 4 September, a White Paper review in Houston TX during the week of 16 October (tentative), and a Proposal review in Amsterdam during the week of 11 December (tentative). Exact dates and locations will be announced by 1 August 2006. ISA-SP100.14 may call additional meetings and teleconferences as needed.

Additionally, there may be working sessions from time to time to create and finalize documents. These working sessions will be open, but are primarily intended for volunteers who are deeply involved in the process.

The proposal and evaluation will proceed generally as described below. Note that there are many more milestones than meetings. This process and schedule is subject to change.

14 July 2006: ISA-SP100.14 distributes Preliminary Call for Proposal (CFP). Interested companies and individuals may join an ISA-SP100.14 Proposer Mailing List at this time. Questions submitted in writing to ISA-SP100.14 will be answered in writing through the mailing list.

28 July 2006: ISA-SP100.14 distributes first draft of Use Cases, Technical Requirements, and Evaluation Process & Criteria. This material will be posted on the ISA-SP100.14 web site. At this stage, use cases will be identified with an abstract for each.

1 August 2006: Deadline for Intent to Propose with a short abstract. The abstract should include a high level description of the scope of the proposal as well as the overall approach. All abstracts will be posted on the ISA-SP100.14 web site.

31 August 2006: ISA-SP100.14 distributes an updated CFP, accounting for issues and ambiguities raised through the Mailing List. The Updated CFP will include Use Cases, Technical Requirements, Proposal Check List, and Evaluation Criteria. The Proposal Check List and Evaluation Criteria will provide a consistent basis for comparing proposals.

6-8 September 2006: Proposer Conference, ISA Headquarters, Durham NC. PowerPoint overviews of all proposals will be presented and discussed in an open forum. In the open and collaborative spirit of ISA-SP100.14, this conference is intended to help proposers to gather feedback from the SP100 committee and facilitate the identification of potential collaborators. Electronic copies of all presentations are due on 5 September so that they may be reviewed in advance. More detail on this Conference can be found at the end of this CFP.

9 October 2006: Due date for White Papers, and preliminary answers to the Evaluation Criteria.

19-20 October 2006 (tentative): ISA-SP100.14 meets in Houston TX, to review and evaluate White Papers. This meeting will be held in conjunction with an ISA-SP100 general meeting.

31 October 2006: Complete review of White Papers by the ISA-SP100.14 Working Group. At this stage, a limited number of participants will be encouraged to provide full proposals. Proposal Checklist and Evaluation Criteria may be updated at this point.

4 December 2006: Final proposals due, including White Paper, Proposal Check List, Evaluation Criteria, and ISA Intellectual Property letters.

12-14 December 2006 (tentative): ISA-SP100.14 meets in Amsterdam to review and evaluate final proposal materials.

31 January 2007: Select final proposal(s).

30 March 2007: Complete ISA-SP100.14.0: Overview

2 April 2007: Begin writing specifications based on ISA-SP100.14.0. The identified documents are:

ISA-SP100.14.0a: Network Management Framework
ISA-SP100.14.0b: Network Security Framework
ISA-SP100.14.0c: Coexistence Report Card
ISA-SP100.14.0d: Interference Strategy
ISA-SP100.14.1: Radio
ISA-SP100.14.2: MAC
ISA-SP100.14.4: Transport and Network

31 August 2007: Complete draft specifications; distribute to ISA-SP100.14 for comments.

October – December 2007: Ballots and comment resolution within ISA-SP100.14.

January – June 2008: Ballots and comment resolution within ISA-SP100.

June 30th 2008: Recommendation to ISA by SP100 to adopt the SP100.14 standard.

X – ISA-SP100.14 Proposer Conference and Mailing List

A Proposer Conference will be held at or near ISA Headquarters in Research Triangle Park, North Carolina on 6-8 September 2006. In the open and collaborative spirit of ISA-SP100.14, this conference is intended to help people improve their proposals and identify potential collaborators.

The agenda will include:

- Presentation by ISA-SP100.14 of available Use Case information, and discussion.
- Walk-though of the ISA-SP100.14 proposal and evaluation process. At this meeting a revised project plan for the development of ISA-SP100.14 will be discussed and will include a down selection process so as to encourage collaboration particularly if there are a significant number of proposals.
- PowerPoint presentations (i.e. public disclosure) by proposing companies and individuals, with opportunity for questions and discussion.

All proposing companies and individuals are requested to:

- Provide an Intent to Propose by 1 August 2006, with an abstract. The abstract should include a high level description of the scope of the proposal as well as the overall approach. This will enable ISA to select an appropriate venue, and schedule presentations. Send your notification of intent to ISASP10014CFP@isa.org. If your response is not acknowledged within two (2) business days please resend.
- Attend the Proposer Conference in September 2006.
- Provide electronic copies of all presentations by 5 September so that they may be distributed and reviewed in advance.
- Present an overview of their proposals at the Proposer's Conference, in an open forum.

Participation in the Proposer Conference is strongly recommended. Non-descriptive abstracts and/or proposals may be excluded from subsequent consideration.

Participants in the conference are expected to cover their own travel expenses. There may be a modest fee to cover the cost of holding the event.

In addition, the ISA-SP100.14 Working Group will accept written questions and distribute responses through an email mailing list. Questions and requests to be included on the mailing list (with primary and secondary email contact) should be sent to ISASP10014CFP@isa.org

Thank you in advance for your constructive participation in ISA-SP100.14.

Annex A
Preliminary Proposal Checklist Revision 1.0

This Annex includes a preliminary draft of the ISA-SP100.14 Proposal Checklist.

This list is not intended to be an outline for the proposal or imply a structure. It should be used as a check list by the CFP responder to measure how complete the proposal is.

Topics to be considered are:

	Check Addressed Topics: Preliminary Proposal	Check Addressed Topics: Final proposal
Robustness of the design		
How does the system deal with:		
1.1. Poor quality RF links due to		
1.1.1. high noise?		
1.1.2. low signal strength caused by long path lengths or obstacles?		
1.1.3. multipath fading?		
1.1.4. Interference?		
1.1.5. Give an example of what end-to-end data delivery reliability is achieved in the presence of noise, unreliable links in a multi-hop network. State the assumptions.		
1.2. Does the system support guaranteed delivery of packets?		
1.2.1. Per link		
1.2.2. End-to-end		
Discuss how the system adapts to		
1.3. Changing RF environments.		
1.4. Loss of key components such as routing nodes, gateways and network managers? What network components can be made redundant?		
2. Coexistence		
2.1. How does the system mitigate its effects on other systems operating in the same band? (see the ISA-SP100 Coexistence Report Card)		
2.2. How will this system coexist with other likely wireless systems within a facility – how will it mitigate the effects of other systems and interference sources?		
3. Security		
Discuss the systems support for:		
3.1. Data privacy (encryption).		
3.1.1. Number of keys		
3.1.1.1. Is there a network key?		
3.1.1.2. Is there a different key between each node pair?		
3.1.1.3. Is there a transport layer key?		
3.1.2. Encryption type		
3.1.3. Encryption key management. Where are they generated and how are they distributed? Can keys be periodically changed in the network?		
3.1.4. Key updates		

3.2. Message integrity		
3.2.1. How is the integrity of the data on the network protected?		
3.2.2. What portions of the packet are protected?		
3.3. Authentication		
3.3.1. How are devices on the network authenticated?		
3.3.2. How is the network authenticated to devices?		
3.4. Freshness: how are replay attacks detected and discarded?		
4. Performance		
4.1. Throughput		
4.1.1. The system operates on one or more channels. How many RF channels are there and what is the available data rate of one of the RF channel? For example the IEEE802.15.4 system in the 2.4 GHz band has 16 separate channels and in each channel the radio has a raw transmission rate of 2 Mcps and an available transmission rate of 250 Kbps after coding.		
4.1.2. What is the available transmission rate per gateway?		
4.1.3. Are multiple gateways supported?		
4.2. Quality of Service		
4.2.1. Latency		
4.2.1.1. Is latency managed in the network? If so how?		
4.2.1.2. Give examples of per link latency and end-to-end latency using an example network.		
4.2.1.3. How does adding other services affect latency of an existing service in the network?		
4.2.2. Bandwidth		
4.2.2.1. Can bandwidth be assigned or reserved for an application?		
4.2.2.2. How quickly can the network adapt to changes in device bandwidth requirements?		
4.2.3. Priority		
4.2.3.1. Does the network support packet priority?		
4.2.3.1.1. What is the algorithm for determining priority?		
4.3. Frame Coding Efficiency		
4.3.1. What is the effective network layer payload throughput of an RF channel when RF, MAC, and network layer overheads are taken into account? The overheads should include such items as guard times and acknowledgement packets that are required.		
4.3.2. Describe the packet structure		
4.3.2.1. What is the maximum and minimum packet size?		
4.3.2.2. Diagram the packet header fields for the RF preamble, MAC and Network layers for each significant packet size. For example if data and control packets follow the same format a common diagram can be given. If Acknowledgement packets are used and they follow a different format then show that.		
4.4. Operational Power		
4.4.1. How does the system manage power of battery operated nodes?		
4.4.2. What is the transmit energy required for a minimum sized packet at a specified transmit power level?		

4.4.3. What is the energy required to receive a minimum sized packet?		
4.4.4. What power is required to listen for a packet?		
4.4.5. What power is required by a node when it is idle?		
4.4.6. Give a battery life calculation example for an application and a specified battery type.		
5. Radio		
5.1. Describe the modulation(s) used to for transmission		
5.1.1. What is the radio's performance in the presence of noise?		
5.1.2. What ranges does the radio have		
5.2. What bandwidth is used per channels and how many channels are required for basic operation?		
5.3. What is the channel spacing and how many channels are available?		
5.4. What RF overheads are required? Preamble and sync symbols.		
5.5. What regulatory issues need to be addressed for by the radio technology?		
5.6. What is the typical transmit power level(s) of the radio?		
5.7. What antenna type is typically used? Are restrictions on the types of antennas required?		
5.8. Show a block level diagram of a typical implementation of the transmitter and receiver portions of the radio from the digital data input/output to the antenna.		
5.9. What coding techniques are used, is the network relying on error correction or coding, what type of BCCs (CRC) are used.		
5.9.1. What is the realized data rate after coding?		
5.10. What is the maximum range of any length and what is the confidence level that this range can be achieved.		
5.11. State any channel assumptions and models that are used.		
5.12. Supply the international certification plan, what countries will have restrictions or how will the product operation be restricted in other countries.		
5.13. State any special antenna system considerations and provide antenna characteristics that were assumed.		
5.14. What are the frequencies of operation?		
6. MAC		
6.1. What topologies are supported? Examples are peer to peer and star.		
6.2. Describe the MAC addressing		
6.2.1. Address size and address structure		
6.2.2. How is address assignment done?		
6.2.3. Is there support for broadcast and multicast messages?		
6.3. Does the MAC support sleeping end nodes? How much buffering is anticipated?		
7. Network		
7.1. What network topologies are supported? Examples are mesh, tree and star.		
7.2. What network services are available like packet resequencing? duplicate packet deletion		
7.3. Describe the network addressing scheme		
7.4. Can an end node also act as a routing node or other infrastructure node?		

7.5. Does the network support mobility? i.e. can a node move throughout the network?		
7.5.1. Does the network require a mobile device to obtain a new address after it moves?		
8. Transport		
8.1. What transport layer services are provided? Principles of operation and performance metrics for each.		
8.1.1. Best effort of service		
8.1.2. Guaranteed service		
8.1.3. Data fragmentation, streaming, and reassembly, to & from gateway		
8.1.4. Firmware code image transmission & reflash		
8.1.5. What flow controls are supported?		
9. Application Layer Interface		
9.1. What services are available to applications? Examples are universal time, priority settings, encryption control.		
9.2. Can a network device support more than one application? If so how are the multiple endpoints distinguished?		
9.3. What are the energy-sparing capabilities of the proposed application layer? What are the constraints caused by this capability?		
10. Scalability		
10.1. How many devices can a network support?		
10.2. What is the maximum cumulative effective throughput of the network, what are the dependencies? How does the number of nodes affect this?		
10.3. How is battery life affected by scalability?		
10.4. How is device bandwidth affected by scalability – can devices still readily obtain extra bandwidth.		
10.5. Please elaborate on any tools or techniques whereby the user will be able to predict the impact of adding additional devices or application traffic to the network.		
10.6. Give an example of a network with a large number of nodes. Describe the performance. How is the performance measured: by calculation, simulation or measurement?		
10.7. Give an example of a network with a large geographic area that spans several maximum RF path lengths. Describe the performance. How is the performance measured: by calculation, simulation or measurement?		
10.8. Can multiple overlapping networks be supported? How?		
10.9. How many hops can the network support?		
11. Network Management		
11.1. How does the network form? How long does this process take and under what conditions?		
11.2. How does a new device join the network? How long does this process take?		
11.3. How does a device respond to the absence of an operating network?		
11.4. Does the network support preprogramming devices?		
11.5. How does the network support heterogeneous devices (from different vendors, with different capabilities)		
11.6. What MIBs are proposed?		

11.7. How can the MIBs be accessed; from within the network, from outside the network?		
11.8. What are the security aspects of network management access?		
11.9. What network management standards are used?		
12. Device		
12.1. Show a block diagram of a typical node device with processor, and memory requirements. What are the typical data storage, and program storage requirements?		
13. General Operation Overview		
13.1. Describe the typical packet transmission process		
13.2. Describe the typical packet reception process		
13.3. Describe the multi-hop downstream transmission process		
13.4. Describe the multi-hop upstream transmission process		
13.5. Describe the effects of loss of power to the system and each node		
13.6. Describe how a system would be configured; including end nodes, router nodes, and other infrastructure nodes		
13.6.1. Is there service discovery?		
13.7. If the system is synchronized, describe how synchronization is maintained.		
13.7.1. If the system provides a universal clock, describe how the clock is propagated. Specify the clock accuracy the system can provide.		
13.7.2. What system overhead is required to maintain synchronization?		
13.7.3. What device clock accuracy is required?		
13.7.4. How is network time maintained across devices, and what is the accuracy?		
13.7.5. Please describe synchronization aspects such as:		
13.7.5.1. scheduling control,		
13.7.5.2. handling missed updates		
13.7.5.3. jitter		

Annex B
ISA PATENT LETTER OF ASSURANCE

[Date]

ISA
67 Alexander Drive
Research Triangle Park, NC 27709
Attention: ___________________

Dear Mr./Ms. ___________________:

This is to confirm that [Company Name] ("the Company"), in consideration of being permitted to participate in the development and/or revision of [Name of Proposed or Current Standard] ("the Standard") through its authorized representatives, agrees to disclose any and all patents owned or controlled by Company that may be relevant to the Standard. Pursuant to this commitment, the Company states that:

- ❑ There are no patents, granted or pending, owned or controlled by the Company that may be relevant to the Standard; or
- ❑ The following patents, granted or pending, may be relevant to the Standard: ____
____
_______________________________.

The Company understands that this disclosure obligation is a continuing one, and therefore should the Company at any time become aware of any patent that may be relevant to the Standard, the Company shall disclose the same on a timely basis.

With respect to any granted or pending patent owned or controlled by the Company, whether or not currently known or disclosed, that may be infringed by compliance with the Standard, the Company agrees that it shall grant a license to an unrestricted number of applicants on a worldwide, non-discriminatory basis, with a fair and reasonable royalty rate and fair and reasonable terms and conditions, in order to allow such applicants to comply with the Standard.

This Letter of Assurance is a binding legal document that is irrevocable unless and until the Standard is withdrawn by ISA, and it incorporates a covenant of good faith and fair dealing. The Company acknowledges that other participants in the development or revision of the Standard are third party beneficiaries of the Letter of Assurance.

[Company Name]

_________________________	_______________________	_________________
Signature of Authorized Representative	Printed Name	Date

Annex C

I. SP100 Mission & Goals

The mission of the CFP process must support the overall SP100 mission, which is: Deploying wireless technology with confidence in industrial automation applications. The trickle down goals for the CFP process would be to support:

a. life-cycle management
b. stake holder needs
c. improved confidence in deployments

II. CFP Mission and Goals

The CFP process is designed to allow the SP100 committee to benefit from the expertise, talent, and efforts of contributors who are not necessarily on the committee. The SP100 committee recognizes that the committee itself can't and shouldn't solve all the problems associated with meeting the mission and goals of SP100. We want to solicit ideas from the technical community as to how to solve the problems identified. The key, then, is to recognize what those issues are, including some the committee may not have thought of, and identify where solutions might be available to solve those problems.

a. What the CFP process is

The process solicits ideas (including issues, alternatives, and criteria for evaluating alternatives) from potential contributors that can be used to construct the work products to be produced by the committee. The process should encourage proposed solutions but only in so far as they can be compared, quantitatively and objectively, against other alternatives proposed. Unsubstantiated opinions, solutions, or designs should be discouraged unless others (other than the contributor) are willing and able to provide the requisite substantiation processes.

b. What the CFP process is NOT

The process is not about "selecting the best of the best" without criteria. It's not a voting process that uses subjective characteristics to create a "popularity contest" to down select from a suite of alternatives. It's quite feasible that no proposals can adequately address all the issues. The key is to allow the stake holders to be fully informed about the risk and subsequent probability of success if a particular option is selected for deployment in a particular application in a particular environment.

c. Expectations

The expectation is that the committee will create the numbered clauses (SP100.11, SP100.14) from the material received in response to the CFP but it is unlikely that large portions of the actual standard will be lifted directly from any particular proposal submitted.

III. Strategy

Accordingly, the strategy of the CFP shall be focused on soliciting input that provides the best <u>approach</u> to solving the critical issues associated with deployment of wireless technology for industrial automation. This implies that the responses should have the following attributes:

1) Modular – allows the committee to pick and choose appropriate sections for inclusion in the final work product and even in other SP100 work products.
2) Specific – allows the committee to cut-and-paste technical sections without heavy editing
3) Consistent – terminology and structure of the responses should ease the editing requirements and not require re-formatting

4) Thorough – responses should be sufficiently detailed to assure the proposal can be adequately evaluated. The responses should include proposed quantitative, objective measures against which committee members can compare options.

IV. CFP Format

All Calls for Proposals from SP100 will follow a logical, consistent format that may be tailored for the specific WG. The committee may decide to update the format and required responses as it determines there are opportunities to improve the process. The current model for a CFP format follows:

a. Introduction – SP100 background, specific clause being addressed (for example SP100.14), and where this particular clause fits into the overall SP100 mission, goals, and strategy.
b. Environments – discussion about the target environments or categories and ranges of environments seen as appropriate for this numbered clause.
c. Application Focus – specific information about the types of applications and/or Use Cases targeted by this particular clause. Reference to more details (perhaps on the SP100 web site) would be appropriate.
d. Constraints – Responses are expected to use terminology consistent with the ISA dictionary and the SP100 glossary. All responses must address proposed solutions in an architecture consistent with the ISO/OSI 7-layer model. All interfaces between/among layers must be specified or declared as internal. Any proprietary segments must be identified with appropriate understanding that, if selected, arrangements can be made for universal access.
e. Schedule – intent, workshops, drafts, responses, best-and-finals, etc.
f. Disclaimer – SP100 can choose to use any part and submitted material becomes property of ISA.
g. Expected Response Format – Details how the proposed solutions address the following:
    1) Introduction – scope of response, general applicability in range of environments, applications, and even some use case examples. How this proposal is seen with respect to overall SP100.
    2) ISO/OSI layers included and interfaces defined with sufficient detail to allow assessment of third-party suppliers of subsequent layers.
    3) Performance Issues Addressed and proposed metrics. This section should provide sufficient detail to allow the committee to ascertain the probability of success of the proposed solution in the proposed application in the proposed suite of environments. These four parameters are, of course, not orthogonal, so responders must provide estimates of each with respect to the other three. For example, expected throughput varies from xxxx KB/s to zzzz KB/s as range varies from 1 to 100 m as security ranges from none to AES as reliability varies from 1 failure to deliver per day to 1 failure in 20 years as expected latency varies from 1 second to 0.010 seconds.
        1. Throughput – valid, relevant data rate
        2. Range – end-to-end of wireless link proposed
        3. Security – authentication, etc.
        4. Reliability – includes probability of failure defined as failure to meet expected performance. Includes mean time between attention – includes battery life expected and MTBA it is computed

    5. Latency – end-to-end – could be quoted as worst case or as some sort of stochastic assessment, if desired. Again, the method used to estimate must be provided.

4) Interoperability – with compatible (eg SP100.14) devices.
5) Coexistence – with expected potential interferers (other wireless communication devices – pagers, walkie-talkies, etc.)
6) EMI – expectations of interference from other industrial processes (ovens, welders, etc.)
7) EMC – expectations that supplied devices will interfere with other devices in the environment (eg old instruments, other networks)
8) Expandability – architecture for growing the network – maximum sizes of each layer, flexibility within layers, hierarchical vs. ad hoc,
9) Environments – ranges of temperature, vibration, humidity, etc over which the performance statistics quoted above, can be expected.

Annex D

Major Steps in ISA-SP100.14 Call for Proposal Process

Date	ISA-SP100.14 Responsibility	Proposer Responsibility
14 Jul 2006	Issue Call for Proposal	
28 July 2006	Distributes first draft of Use Cases, Technical Requirements, and Evaluation Process and Criteria	
1 Aug 2006		Submit brief abstract outlining proposal intent
31 Aug 2006	Issue updated CFP, accounting for issues and ambiguities raised since initial issue and including available Use Cases, Technical Requirements, Proposal Check List, and Evaluation Criteria.	
5 Sep 2006		Submit Overview for Proposer Conference
6-8 Sep 2006	Convene Proposer Conference	Attend Proposer Conference
9 Oct 2006		Submit White Paper and preliminary answers to Evaluation Criteria
19-20 Oct 2006	Tentatively meet to review and evaluate White Papers	
31 Oct 2006	Invite selected Proposer(s) to submit full proposals and issue new Proposal Checklist and Evaluation Criteria as appropriate	
4 Dec 2006		Submit final proposal, including White Paper, Proposal Checklist, Evaluation Criteria, and ISA Intellectual Property letters
12-14 Dec 2006	Tentatively meet to review final proposals	
31 Jan 2007	Select optimal proposal or portions of multiple proposals or no proposal to incorporate in draft standard	