ISA100.15 Backhaul/Backbone Networks RFI
Request for Information

Date: October 1, 2009
Version: Final v1.0

ISA100.15 RFI 1
Request for Information 1
1 Purpose 2
2 ISA100.15 Working Group 2
3 Reference 2
4 Acronyms 2
5 Definitions 3
6 Wireless Backhaul/backbone 4
7 Example ISA100.15 Topology 5
8 Information Requested 6
8.1 General Information 6
8.2 Application 7
8.3 Wireless Network Management 7
8.4 Security Management 8
8.5 Application Prioritization / Quality of Service (PQS) 9
8.6 Backhaul/Backbone Maintenance 9
9 Schedule 10
10 Presentation Requirements 10
10.1 Presentation 10
10.2 Format 10
11 Intellectual Property 11
12 Appendix 12
12.1 Wireless Backhaul/backbone interfaces 12
IF1 Specifics 12
IF2 Specifics 12
IF3 Specifics 13
IF4 Specifics 13
IF5 Specifics 13

1 Purpose

The ISA100.15 Working Group is seeking technical presentations that will form the basis for its work on recommended best practices and standards considerations on interoperability of wireless backhaul/backbone networks and wireless sensor networks and wireless devices usable by the process automation industry.

This document describes the process to participate to this Request For Information (RFI),

2 ISA100.15 Working Group

The International Society of Automation (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 technical problems, while enhancing their leadership and personal career capabilities.

The ISA100 committee is part of ISA standards and practices organization. ISA100 was formed in 2005 to establish standards and recommended practices for implementing wireless systems in the automation and control environment.

The ISA100.15 Working Group, composed of process automation users, vendors and service providers, is charted to define recommended practices to enable interoperability between backhaul/backbone wireless networks and field wireless networks and devices.

The backhaul/backbone wireless networks will interface with field wireless networks and devices for example ISA100, *Wirelessl*HART™, IEEE 802.11a/b/g/n, ZigBee, RFID and other wireless technologies. It also interfaces with the process control network and control applications. It needs to provide support for variety of process control protocols which includes but is not limited to Fieldbus Foundation High Speed Ethernet (HSE) and ISA100.11a protocols. In a unified wireless network it also expected that other traffic such as voice, video, etc. would share the same backhaul/backbone wireless medium in a segregated manner.

3 Reference

1. ISA Home Page http://www.isa.org/
2. ISA Standards and Procedures
http://www.isa.org/filestore/standards/2008_ISA_Standards_Procedures.doc

4 Acronyms

AAA	Authentication, Authorization and Auditing
CCCP	Commodity Commercial Communications Provider
CCCP-IF	Commodity Commercial Communications Provider Interface
CCD	Characterized Control Domain
CS	Control System
IF	Interface
NMS	Network Management System
UOC	User-Owned Communications
SM	Security Manager
Dynamic QoS	Dynamic Quality of Service
IDS	Intrusion Detection Service
IPS	Intrusion Prevention Service
QoS	Quality of Service
WAD	Wireless Access Domain

5 Definitions

Term	Definition
Authentication	Mechanism used to verify the identity of a device connecting into a network.
Authorization	After initial authentication, authorization looks at what that authenticated device/user has access to.
Auditing	Systematic process of objectively obtaining and evaluating evidence regarding assertions about security and performance to ascertain the degree of correspondence between those assertions and established criteria and communicating the results to interested users."
Commodity Commercial Communications Provider	Providers offering backhaul/backbone that will be used to bring information (sensor data, process data, video, voice, location) back to a control domain via either a long or short distance wireless communications mechanism.
Commodity Commercial Communications Provider Interface	Interface between control network and backhaul/backbone
Characterized Control Domain	A set of interconnected control equipment functioning to monitor and control a defined set of process equipment.
Control System	A system used to automatically control a process such as product manufacturing, chemical, oil refineries, and paper and pulp factories.
Dynamic QoS	The ability of the user to dynamically request a change in the QoS (ref QoS below) provided by the communications provider.
IF1	Interface specific to the requirements of a particular CCCP/UOC.
IF2	Interface handling CCCP-IF interoperability and coordination
IF3	Multiple ISO/OSI Layer 2 (e.g., 802.3) interfaces with management protocols on top. IF3 profiles expected to be based on layer2 standards. This is operational data flows, not CCCP-IF configuration management.
IF4	Interface providing transparent connectivity between CCDs; no interpretation of application protocols (out of scope of .15)
IF5	Interface specific to configuration, security and operation management.
Network Management System	A combination of hardware and software used to monitor and administer a network.
User Owned Communications	Communication equipment owned and managed by the end user.
Security Manager	Function that allows the end user to monitor and control the security aspects of the communication system.
Intrusion Detection Service	Intrusion detection service is a type of service or security management system that gathers and analyzes information from various areas within a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). Intrusion detection functions typically include: Monitoring and analyzing both user and system activities, analyzing system configurations and vulnerabilities, assessing system and file integrity, ability to recognize patterns typical of attacks, analysis of abnormal activity patterns, and tracking user policy violations
Intrusion Prevention Service	Intrusion prevention service is a type of service or security management system that monitors network and/or system activities for

	malicious for unwanted behaviour and can react, in real-time, to block or prevent those activities.
Quality of Service	QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies including Frame Relay, ATM, Ethernet and 802.1 networks, SONET, and IP-routed networks. In particular, QoS features provide improved and more predictable network service by providing the following services: • Supporting dedicated bandwidth • Improving loss characteristics • Avoiding and managing network congestion • Shaping network traffic • Setting traffic priorities across the network
Wireless Access Domain	Secure location for network and security management.
Wireless Backbone	Wireless network bringing information back to a control domain via a short distance wireless communications mechanism. Communications capabilities are often purchased from wireless equipment suppliers.
Wireless Backhaul	Wireless network bringing information back to a control domain via a long distance wireless communications mechanism. Throughput is often significantly less than found on the high-speeds communications networks that they interconnect. Commercial telecommunications providers may be involved.

Please read the Appendix to better understand backhaul/backbone integration interfaces IF1, IF2, IF3, IF4 and IF5.

6 Wireless Backhaul/backbone

The wireless backhaul/backbone networks will be used to fulfill four different use case categories:

A. Process control center to distant control/monitoring site using wireless
B. Process control center to distant control center using wireless
C. Process control center to in-plant control center using wireless
D. In-plant blanket of wireless coverage

Use case categories A & B are sometimes referred to as “backhaul” because they bring information back to a control domain via a long distance wireless communications mechanism. Throughput is often significantly less than found on the high-speed communications networks that they interconnect. Commercial communications providers are often involved.

Use case categories C & D are sometimes referred to as “backbone” because they bring information back to a control domain via a short distance wireless communications mechanism. Communications capabilities are often purchased from communication equipment suppliers and thereafter are often owned and operated by the “user”.

Responders should provide a table summarizing the capabilities of their network. The table below is an example of how the network characteristics can be summarized.

Characteristics	Backbone	Backhaul
Bandwidth		
Latency		
Jitter		
Loss		

7 Example ISA100.15 Topology

The following topology is an example of how the backbone/backhaul is intended to be used by the process automation users.

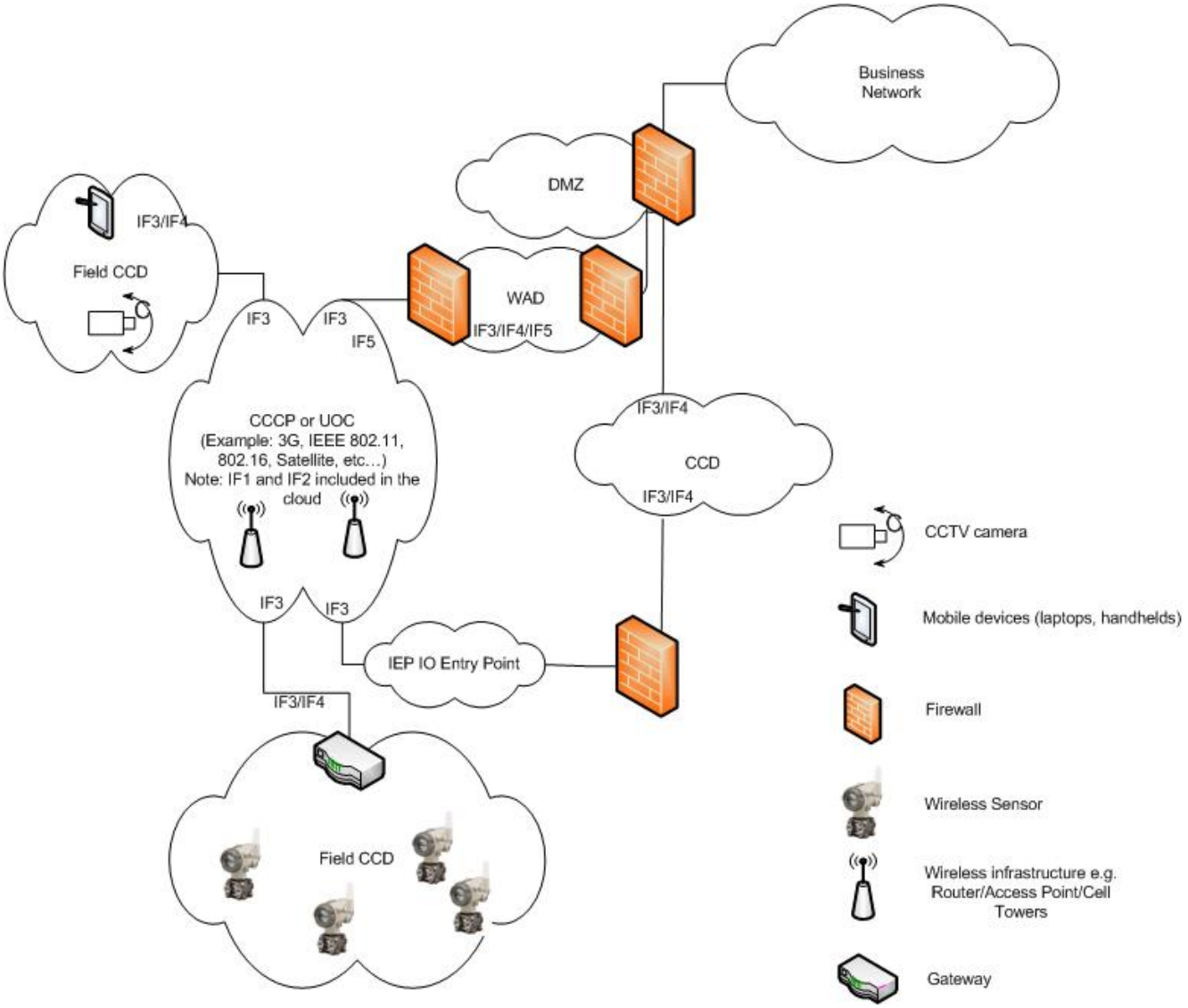

Figure 1: Example of ISA100.15 Topology

8 Information Requested

8.1 General Information

Requirement ID	Description	Use Case Categories
BSR1 Segregated or Integrated Wireless	Describe how your solution allows the segregation of various application data streams. This segregation could be logical, physical, or mixed.	All
BSR4 Time Sync	Describe how your solution supports time synchronization. What is provided guaranteed resolution and accuracy?	All
	How can end-users determine the latency of the backhaul? What is the typical latency observed on the backhaul? What is the typical variation in the latency (i.e. jitter, standard deviation) observed on the backhaul?	All
BSR5/BSR10 Scalability	How does your solution allow users to scale up? User wants to increase the covered area User wants to have more data capacity (e.g., 250 Kbps to “x” Gbps) Ingress/egress point count, user counts, etc.	All
	Please specify the type of topology supported (example: linear, star, star-mesh, mesh, etc…)	C, D
BSR7/ APP1 Future-Proof	What future technology improvements to you anticipate and when? What are the implications to today’s investment?	All
BSR11a Availability (Diversity, Redundancy)	Please describe how your solution ensures that there is no single point of failure.	All
BSR11b	Specify worst, typical and best case automatic failover recovery time.	All

BSR15 Ownership Types	Please define which backhaul category or categories your solution belongs to: (1) user-owned and operated backhaul (e.g. IEEE 802.11); (2) backhaul provider-owned and operated (e.g., cellular, satellite); (3) combinations of above.	All

8.2 Application

APP2 Future Applications	Describe how your backhaul supports IP-based (e.g.IPv4 and/or IPv6) or non-IP-based (e.g. IEEE 802.1AS, Qat, Qau) packet based applications such as real-time video streaming and mobile workers.	All
APP4 Communications Paradigms	What type of communication paradigms do you support? (Client-Server, Multi-cast, publication, rstp, etc.)	All

8.3 Wireless Network Management

WNM1 Availability; No Single Point of Failure	How does your solution handle and report failover when: there are multiple interfaces to a single CCCP ; individual interfaces to multiple CCCPs; multiple interfaces to multiple CCCPs?	All
WNM3 Common Network Manager	What communication interfaces are provided at the CCCP interface to manage the backhaul system? What tools/user interfaces are provided to management the backhaul system (QoS, Freq, data transmission, etc…)?	All
BSR16/PQS2/ **WTR3** Physical Link Conditions, Stress, Predictable	Do you provide a means for the user to determine the current traffic level? Do you provide a means for the user to request a change to the QoS?	All
PQS3/WNM2 Overload; Graceful Degradation	Describe the interface your solution provides to indicate real-time link quality.	All

8.4 Security Management

SMR1a Data Security	In your solution, how are confidentiality, integrity, and authenticity of data stream across the various interfaces assured?	All
SMR1b/BSR2/BSR3 AAA Services	If applicable, how is AAA for IF1, IF2, and/or IF3 provided?	All
SMR2a/ SMR2b	Does your CCCP-IF support IP address and IP address-family translation? If so, how?	All
SMR3 Zone Isolation	Describe how your solution supports segregation of multiple ISA99 security zones of controls data utilizing the same CCCP-IF as an ingress/egress conduit. (e.g., by frequency, by VLAN tag, by channel, MTLS label, etc.)	All
SMR4a QoS	If applicable, describe how your solution provides AAA for configuring QoS (Quality-of-Service)?	All
SMR4b QoS	If applicable, describe how your solution prevents QoS mechanism tampering. Example: user connects to the network using laptop, modify their QoS quality and view a movie on YouTube.	All
SMR5 Network Management	How do you provide AAA for remote network management and monitoring of CCCP-IF?	All
SMR6 Network IDS	Does your solution support Network IPS and/or IDS? If so, describe this feature?	All

8.5 Application Prioritization / Quality of Service (PQS)

PQS1/APP3 Coordinated Access for Multiple Applications	What type of QoS do you provide at IF1 (connection-based, packet-based, absolute, etc…)? How many priority levels do you support? What type of QoS do you provide at IF3? (connection-based, packet-based, absolute, etc…) And how many priority levels do you support? How do you map between the two QoS (IF1 and IF3) if there is no one-to-one mapping of levels and functions?	All
PQS2 Physical Link Conditions	Do you provide a means for the user to determine the current traffic level? Do you provide a means for the user to request a change to the QoS?	All
PQS3/WNM2 Overload; Graceful Degradation	Describe the interface your solution provides to indicate real-time link quality.	All
	Describe how prioritized traffic is handled when the network is congested. Example: data re-allocation.	All
	Describe how users will upgrade network.	All

8.6 Backhaul/Backbone Maintenance

BSR11	Describe how the network is updated. Is a network outage required to upgrade the network?	All

9 Schedule

RELEASE DATE: Oct 1, 2009 (11 PM EST)
ISA100.15 releases RFI and contacts wireless network vendors and communications providers. ISA100.15 anticipates several wireless network vendors and communication providers to express their intent to participate to this RFI.

CALL FOR INTENT TO PARTICIPATE: Response due Oct 16, 2009 (11 PM EST)
The call for Intent to Participate is a process in which all interested parties are asked to identify their intention to participate to this Request for Information. You must declare your intent. You may decide later, if necessary, to retract your intent, but it must be declared.
The purpose of this step is to schedule a webinar to ensure responders understand the requirements. Send your notification of intent to lwolffe@ISA.org If your response is not acknowledged within two business days please resend.

PRELIMINARY PRESENTATIONS: Due Nov 13, 2009 (11 PM EST)
Responders are required to provide a preliminary version of their presentation to the ISA100.11 Working Group. This allows the ISA100.15 Working Group to review the proposals and provide feedback.

Webinars/teleconferences may be scheduled as needed to clarify questions regarding the preliminary presentations.

PRESENTATIONS: Due December 4, 2009 (11 PM EST)
Respondents are required to provide and present a final version of their presentation to the ISA100.15 Working Group to share the breadth and advantages of their solutions.
Schedule for the presentations will be provided as soon as possible (preferably in December).

BEST PRACTICES
After evaluating these presentations, the ISA100.15 Working Group will create the Best Practices for industrial wireless backhaul/backbone. The ISA100.15 Working Group expects technical participation from selected technology providers to this activity.

10 Presentation Requirements

10.1 Presentation

ISA100.15 Working Group expects technical presentations answering the requirements identified in section 8. It is expected that the presenters will be technical experts (example: system architects or consultants).

It is expected that each presentation will be two (2) hours in length including time for questions.

The submission may contain supporting documentation to provide more details than the presentation.

ISA100.15 Working Group, attending and evaluating the presentations, is composed of technical experts from backhaul/backbone end-users (example: Boeing, BP, Chevron, ExxonMobil, Shell), process automation vendors (example: Emerson, GE, Honeywell, Yokogawa) and industry consultants.

10.2 Format

Presentations are expected to be in Microsoft's PowerPoint or Adobe Acrobat.

11 Intellectual Property

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

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

1. The ISA100 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 ISA100 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 ISA patent policy (see Annex D of http://www.isa.org/filestore/standards/2008_ISA_Standards_Procedures.doc).

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. 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.

12 Appendix

12.1 Wireless Backhaul/backbone interfaces

The following diagram illustrates functions required to securely and easily connect wireless field devices to the process control system via a wireless backhaul/backbone.

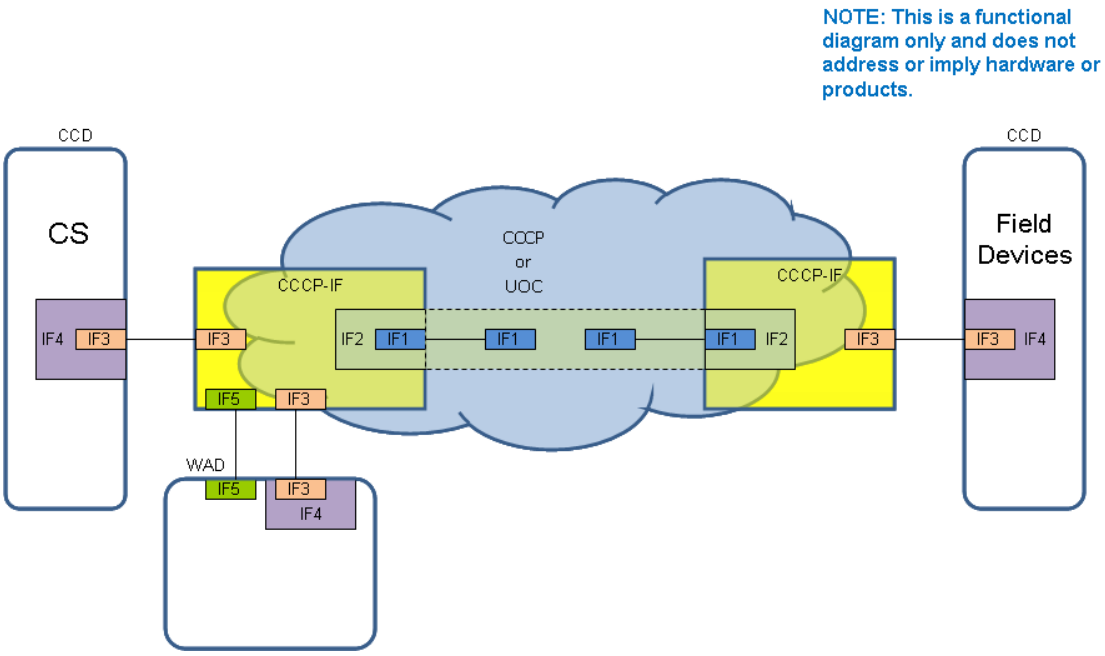

Figure 2: Interfaces diagram

The ISA100.15 members envision a set of interfaces (ref diagram above) that will allow communication between control domains (CCD) using various backhaul/backbone networks and pre-defined interfaces.

The following sections define the characteristics of each of these interfaces.

IF1 Specifics

Interface 1 (IF1) handles QoS and security within CCCP or UOC.
IF1 must support at least one of CCCP technologies such as cellular, 802.16, 802.11, and 802.3.

The interface must support sufficient functionality of a given CCCP technology (as standardized) in order to:
Satisfy any CCCP providers requirement (e.g., authentication)
Support .15 functional requirements (e.g., QoS, etc.) – listed in the requirements matrix

The interface may provide CCCP link management/status/diagnostics and statistics information to the CCCP-IF (e.g. AAA, *need more detail on management function)

IF2 Specifics

Interface 2 (IF2) is required only if the CCCP provider does not provide the CCCP-IF. This interface handles QoS and security between CCCP and CCD.

IF2, between the two CCCP-IFs, shall authenticate each other. CCCP-IF shall provide IF2 encryption/decryption and data integrity protection capabilities. The data encryption shall be enabled by default. However users may be able to disable the data encryption. Users may want to disable encryption for debugging & diagnostics purposes.

CCCP's IF5 shall provide configurable access control (authorization) for specifying which peer CCCP-IFs may communicate using IF2.

IF2 audit functionality shall support:
Peer authentication success and failures
Access control denials (peer identity, IP, failed access count, timestamp, …)
Failed message integrity checks (could be link errors, could be replay/injection attacks)

IF2 shall also provide collection of performance statistics of IF2 data flow(s)

Finally, IF2 shall support IPv4 and/or IPv6 for layer 3 data transport. If necessary, future work could specify non-IP network environments

NOTE: There may be additional communications for managing specific layer 2 functionality (e.g., radio management) that is specific to the CCCP technology.

IF3 Specifics

Interface 3 (IF3) requires multiple channels with different QoS and security.
AAA is required even if IF3 is a trusted, physically secure interface.
Data packets within data flows may include QoS priority indication.
Example application data flows:
Process control data
Historical data
Configuration data
Video monitoring,
Alarms, alerts, downloads,
Voice over IP…

For the first phase of work, we expect that IF3 to support IP. If necessary, future work could specify non-IP network environments.

If CCCP-IF is a stand-alone device then the CCCP-IF must support "well-behaved" connectivity to CCD.

IF4 Specifics

Interface 4 guarantees transparency of the traffic between CCDs, i.e. no interpretation of application protocols (out of scope of .15)
IF4 shall support multiple application data flows.
IF4 supporting control applications shall support data segregation or merge.
IF4 may support multicasting.
IF4 shall support security from the CCD to the CCD.
This interface is not supported by the CCCP.

IF5 Specifics

Interface 5 handles the management function of the network.