

**TECHNICAL REPORT
ISA-TR100.15.01-2012**

**Backhaul Architecture Model:
Secured Connectivity over Untrusted
or Trusted Networks**

Approved 29 October 2012

ISA-TR100.15.01-2012

Backhaul Architecture Model: Secured Connectivity over Untrusted or Trusted Networks

ISBN: 978-1-937560-66-9

Copyright © 2012 by ISA. All rights reserved. Not for resale. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic mechanical, photocopying, recording, or otherwise), without the prior written permission of the Publisher.

ISA
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, North Carolina 27709

Preface

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-TR100.15.01-2012.

This document has been prepared as part of the service of ISA towards a goal of uniformity in the field of instrumentation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA; 67 Alexander Drive; P. O. Box 12277; Research Triangle Park, NC 27709; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

The ISA Standards and Practices Department is aware of the growing need for attention to the metric system of units in general, and the International System of Units (SI) in particular, in the preparation of instrumentation standards. The Department is further aware of the benefits to USA users of ISA standards of incorporating suitable references to the SI (and the metric system) in their business and professional dealings with other countries. Toward this end, this Department will endeavor to introduce SI-acceptable metric units in all new and revised standards, recommended practices, and technical reports to the greatest extent possible. Standard for Use of the International System of Units (SI): The Modern Metric System, published by the American Society for Testing & Materials as IEEE/ASTM SI 10-97, and future revisions, will be the reference guide for definitions, symbols, abbreviations, and conversion factors.

It is the policy of ISA to encourage and welcome the participation of all concerned individuals and interests in the development of ISA standards, recommended practices, and technical reports. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA, or of any of the standards, recommended practices, and technical reports that ISA develops.

CAUTION — ISA ADHERES TO THE POLICY OF THE AMERICAN NATIONAL STANDARDS INSTITUTE WITH REGARD TO PATENTS. IF ISA IS INFORMED OF AN EXISTING PATENT THAT IS REQUIRED FOR USE OF THE DOCUMENT, IT WILL REQUIRE THE OWNER OF THE PATENT TO EITHER GRANT A ROYALTY-FREE LICENSE FOR USE OF THE PATENT BY USERS COMPLYING WITH THE DOCUMENT OR A LICENSE ON REASONABLE TERMS AND CONDITIONS THAT ARE FREE FROM UNFAIR DISCRIMINATION.

EVEN IF ISA IS UNAWARE OF ANY PATENT COVERING THIS DOCUMENT, THE USER IS CAUTIONED THAT IMPLEMENTATION OF THE DOCUMENT MAY REQUIRE USE OF TECHNIQUES, PROCESSES, OR MATERIALS COVERED BY PATENT RIGHTS. ISA TAKES NO POSITION ON THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS THAT MAY BE INVOLVED IN IMPLEMENTING THE DOCUMENT. ISA IS NOT RESPONSIBLE FOR IDENTIFYING ALL PATENTS THAT MAY REQUIRE A LICENSE BEFORE IMPLEMENTATION OF THE DOCUMENT OR FOR INVESTIGATING THE VALIDITY OR SCOPE OF ANY PATENTS BROUGHT TO ITS ATTENTION. THE USER SHOULD CAREFULLY INVESTIGATE RELEVANT PATENTS BEFORE USING THE DOCUMENT FOR THE USER'S INTENDED APPLICATION.

HOWEVER, ISA ASKS THAT ANYONE REVIEWING THIS DOCUMENT WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE DOCUMENT NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER.

ADDITIONALLY, THE USE OF THIS DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS DOCUMENT MUST EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER MUST ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND

ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS DOCUMENT.

THE USER OF THIS DOCUMENT SHOULD BE AWARE THAT THIS DOCUMENT MAY BE IMPACTED BY ELECTRONIC SECURITY ISSUES. THE COMMITTEE HAS NOT YET ADDRESSED THE POTENTIAL ISSUES IN THIS VERSION.

This ISA Technical Report was prepared on behalf of the ISA100 standards committee by ISA100 Working Group 15, Backhaul:

ISA100 Co-Chair: *Herman Storey*, Herman Storey Consulting
ISA100 Co-Chair: *Wayne Manges*, US Dept. of Energy, Oak Ridge National Laboratory
ISA100 Working Group 15 Co-Chair: *Penny Chen*, Yokogawa Corp of America
ISA100 Working Group 15 Co-Chair: *David Glanzer*, Fieldbus Foundation
ISA100 Working Group 15 Editor: *Steven Venema*, Boeing

Contents

1	Scope	7
1.1	General.....	7
1.2	Wireless vs. wired backhaul networks	7
1.3	Specific goals	8
2	Normative references	8
3	Terms, definitions and abbreviations	9
3.1	Terms and definitions.....	9
3.2	Abbreviations	17
4	Backhaul architecture.....	19
4.1	General.....	19
4.2	Backhaul model	19
4.3	Architecture elements	20
4.4	Interface model	21
4.5	Interface definitions	21
5	Security model	22
5.1	Overlay of IEC 62443 on this architectural model	22
5.2	Per-interface security description	24
5.3	System policies.....	26
5.4	Identity and authentication	26
5.5	Status and event logging.....	27
6	Distributed management model	27
6.1	General.....	27
6.2	Functions of the “configuration, security and management domain (CSMD)”	27
6.3	Management communication channels	27
6.4	Distributed management security	28
6.5	Event logging	29
6.6	Common configuration sets	29
6.7	Management protocols	29
6.8	Bootstrapping challenges	29
7	Fault tolerance model.....	29
7.1	General.....	29
7.2	Redundant backhaul networks	29
7.3	Redundant backhaul interfaces	30
7.4	Redundant links	31
7.5	Fault detection, notification and handling actions (auto/manual).....	31
7.6	Online maintenance and upgrades	31
8	Mobility model (for example, mobile workers)	32
8.1	General.....	32
8.2	Mobile workers in different zones	32
8.3	Multi-access-point mobility for a given user	33
9	Flow control model.....	34

Copyright International Society of Automation
Provided by IHS under license with ISA
No reproduction or networking permitted without license from IHS
Full document details: ISA TR100.15.01 2012

9.1	Overview.....	34
9.2	Functions of flow control	35
9.3	Per-interface flow control functions	39
9.4	Flow control policies	40
9.5	Flow control model for mobility.....	41
9.6	Flow control model for security.....	41
Annex A (informative) – Example implementation using the Purdue reference model		43
BIBLIOGRAPHY		44

Figure 1 — Example applications using a shared backhaul network.....	7
Figure 2 — Example industrial control system using backhaul connectivity	19
Figure 3 — Generalized backhaul interface model	20
Figure 4 — Example showing mapping of backhaul interfaces to IEC 62443 security model	23
Figure 5 — Example of remote management capability.....	28
Figure 6 — Redundant BSPs and multi-homed BHIs.....	30
Figure 7 — Redundant BHIs and redundant links.....	31
Figure 8 — Example of mobile workers in different zones	32
Figure 9 — Example of a single mobile worker migrating between access points in a given zone	33
Figure 10 — Flow control example for backhaul.....	34
Figure 11 — Example of flow control with third-party BSP	36
Figure 12 — Examples of edge router locations	38
Figure 13 — Example using backhaul architecture model and extended Purdue reference model	43

1 Scope

1.1 General

This document presents an architecture model for interconnecting automation system elements over untrusted backhaul networks. The focus is on wireless physical layer but is not limited to wireless.

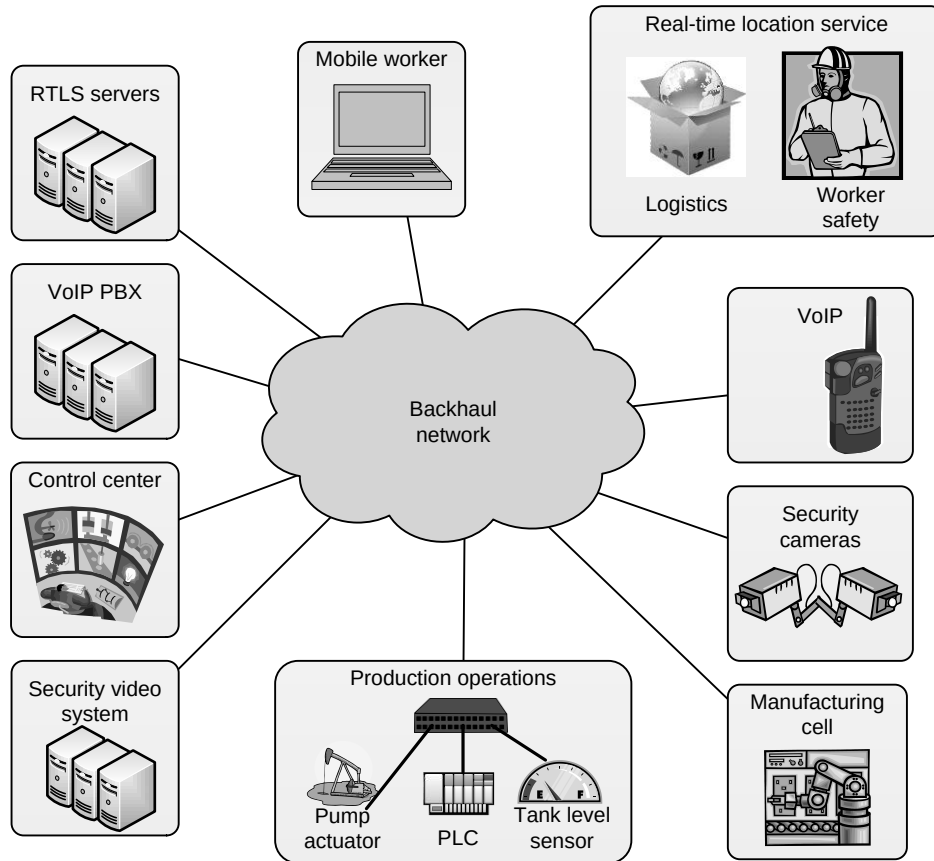


Figure 1 — Example applications using a shared backhaul network

Figure 1 provides an example of the variety of (potentially simultaneous) uses for backhaul networks. In this example, the “Backhaul Network” cloud could represent a short-distance network such as the user-owned network within a building or site, or it could represent a potentially heterogeneous long-distance network (for example, satellite or cellular communication networks) that are provided as a service effectively by multiple third parties. These backhaul links may be provided by one or more commercial providers such as satellite communications providers, cellular, LTE (see Clause 3), WiMax data services, etc. Alternatively, the backhaul may also be provided by the user—for example, Wi-Fi services, point-to-point microwave links, etc.

1.2 Wireless vs. wired backhaul networks

There is nothing in this architecture that precludes the use of wired network technologies (for example, Ethernet) for backhaul networks.

1.3 Specific goals

1.3.1 Provide an architecture model

One of the primary goals of this document is to create an architecture model that insulates the industrial control system elements from the variety of protocols and interfaces associated with various backhaul technologies and providers. Conversely, this architecture model is also intended to insulate the backhaul providers from many of the technical issues associated with specific industrial control systems vendors, protocols, and interfaces.

1.3.2 Define a common vocabulary

This generalized architecture model describes elements and interfaces associated with using backhaul services; the resulting model and vocabulary provide a common framework by which industrial control system vendor, user, and backhaul provider communities can better communicate and collaborate in this rapidly evolving space.

1.3.3 Anticipate backhaul technology evolution

Backhaul network technologies continue to evolve rapidly. For example, new protocols and capabilities for cellular data backhails continue to emerge—as evidenced by the recent introduction of WiMax and LTE service offerings. Similarly for Wi-Fi, a succession of technologies and standards has emerged over time (for example, IEEE 802.11b, 802.11g, 802.11a, 802.11n, etc.).

1.3.4 Allow for mixed use of a shared backhaul

In collecting backhaul network use cases, the authors documented a strong demand from the automation user community for general-purpose backhaul utilization beyond that of just transporting industrial control system data. Specifically, as illustrated in Figure 1, many of the use cases drive the need to use the backhaul to support general data services such as security cameras, voice over internet protocol (VoIP) telephony, emergency first responders, and real-time location services. These use cases also drive the need to support industrial application data service models such as client/server, event multicast, and publish/subscribe. This mixed use of the backhaul network means this model also needs to address automation needs regarding backhaul security, backhaul management, backhaul flow control, backhaul user mobility, etc.

1.3.5 Provide a framework for future profile specifications

As a non-normative document, this architecture has insufficient authoritative detail to enable separate implementers to create products that interoperate.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7498-1, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

ISO/IEC 62443-1-1, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

IETF RFC 2205, *Resource reservation protocol (RSVP) – Version 1 functional specification*

IETF RFC 2474, *Definition of the differentiated services field*

IETF RFC 2475, *An architecture for differentiated services*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

3.1.1

access point

device that allows wireless devices to connect to a wired network

3.1.2

accounting

tracking of network resource consumption by users for the purpose of capacity and trend analysis, and cost allocation

3.1.3

availability

assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them

3.1.4

authentication

process where an entity's identity is authenticated, typically by providing evidence that it holds a specific digital identity such as an identifier and the corresponding credentials

3.1.5

authorization

process of determining whether a particular entity is authorized to perform a given activity, typically inherited from authentication when logging on to an application or service

3.1.6

application

specific implementation or instantiation of this architecture that is designed to address the specific needs of a given installation

3.1.7

backhaul network

communication link between industrial control system elements as well as local and remote field networks

Note 1 to entry: The backhaul may be provided by one or more commercial providers such as satellite communications data services, cellular data services, WiMax data services, etc. Alternatively, the backhaul may also be provided by the user itself—for example, Wi-Fi™ services, point-to-point microwave links, etc.

3.1.8

backhaul interface

interface between a Characterized Control Domain and a Backhaul Service Provider

Note 1 to entry: In the nomenclature of IEC 62443, this is a type of edge device.

3.1.9

backhaul service provider

communications infrastructure that provides connectivity between Characterized Control Domains

3.1.10

characterized control domain

designated set of control equipment

**3.1.11
channel**

logical or physical point-to-point or point-to-multipoint data flow between components in one zone to one or more components in another zone

SOURCE: IEC 62443-1-1

**3.1.12
conduit**

logical grouping of channels, connecting two or more zones that share common security requirements

Note 1 to entry: A conduit is allowed to traverse a zone as long as the security of the channels contained within the conduit is not impacted by the zone.

SOURCE: IEC 62443-1-1

**3.1.13
confidentiality**

assurance that information is shared only among authorized persons or organizations

**3.1.14
connection**

association established between two or more end points which support the establishment of a session

SOURCE: IEC 62443-1-1

**3.1.15
configuration, security and management domain**

logical entity that contains the network and security management functions

**3.1.16
demilitarized zone**

common, limited network joining two or more zones for the purpose of controlling data flow between zones

Note 1 to entry: Demilitarized zones are typically used to avoid direct connections between different zones.

SOURCE: ISO/IEC 62443-3-3

**3.1.17
differentiated services**

specification for a simple, scalable and coarse-grained mechanism for classifying and managing network traffic and providing Quality of Service (QoS) on modern IP networks

SOURCE: Wikipedia

**3.1.18
differentiated services code point**

six-bit field in the IP header for packet used classification purposes in Differentiated Services

Note 1 to entry: This field is part of the Type of Service octet in the case of IPv4, and the Traffic Class octet in the case of IPv6.

SOURCE: IETF RFC 2474

**3.1.19
dynamic host configuration protocol**

protocol used on IPv4 networks that allows the IPv4 address for a device to be assigned automatically

Note 1 to entry: The protocol *may be used to support a central database which keeps track of devices that have been connected to the network and prevents two devices from accidentally being configured with the same address.*

3.1.20

edge device

communication security asset, within a zone or conduit, that provides an interface between a zone and a conduit

SOURCE: IEC 62443-1-1

3.1.21

edge router

router existing at the edge of a Flow Control Domain

3.1.22

extended service set identifier

name that identifies a particular 802.11 wireless LAN

SOURCE: IEEE 802.11

3.1.23

extensible access control markup language

declarative access control policy language and a processing model, describing how to interpret authorization policies

SOURCE: OASIS Extensible Access Control Markup Language, v2.0 (<http://www.oasis-open.org/committees/xacml/>)

3.1.24

extensible authentication protocol

authentication framework providing for the transport and usage of keying material and parameters generated by Extensible Authentication Protocol methods

3.1.25

flow control domain

administrative domain for configuring and managing flow control parameters

3.1.26

Fieldbus Foundation/ISA cooperation

cooperative project between the Fieldbus Foundation and ISA to develop a wireless backhaul architecture model

3.1.27

field network

local area networks that consist of sensors, valves, mobile workers, etc.

3.1.28

integrity

assurance that the information is authentic and complete. Ensuring that information can be relied upon to be sufficiently accurate for its purpose

3.1.29

interface for metadata access points

client/server protocol specification published by the Trusted Computing Group as one of the core protocols of the Trusted Network Connect open architecture

Note 1 to entry: Interface for Metadata Access Points provides a common interface between a database server acting as a clearinghouse for information about security events and objects, and other elements of the Trusted Network Connect architecture. See http://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_specification

3.1.30

interface

conceptual point of interaction between architectural components that allows components to function independently

3.1.31**Internet protocol**

primary protocol in the network layer of the most common Internet protocol suite, which has the task of delivering datagrams (also known as packets or connectionless messages) from the source host to the destination host, based solely on their addresses

Note 1 to entry: For this purpose, each specific version of the Internet protocol defines corresponding addressing methods and structures for datagram encapsulation.

3.1.32**Internet protocol version 4**

1981 version of the Internet network protocol

3.1.33**internet protocol version 6**

1998 version of the Internet network protocol

3.1.34**jitter**

variation of latency from message to message

3.1.35**human-machine interface**

interface by which human users interact with a computerized system

3.1.36**Kerberos**

computer network authentication protocol that uses "tickets" to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner

Note 1 to entry: Kerberos uses symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography by utilizing asymmetric key cryptography during certain phases of authentication.

3.1.37**local area network**

communication network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building or automation facility

3.1.38**latency**

delay between transmission and reception of a message

3.1.39**loss**

message non-receipt or corruption

3.1.40**long term evolution**

standard in the mobile phone network technology tree that is a project of the 3rd Generation Partnership Project

Note 1 to entry: The 3rd Generation Partnership Project is managed by the ITU Radiocommunication Sector.

3.1.41**media access control**

sub-layer of the Data Link Layer that provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multi-point network

3.1.42

mapping function

function that converts flow control attributes between different technologies or flow control policies

3.1.43

marking function

function that marks flow control attributes on packets

3.1.44

netconf

network management protocol to install, manipulate, and delete the configuration of network devices

3.1.45

open systems interconnection model

model from ISO standard 7498 that subdivides a communication system into smaller parts called layers

Note 1 to entry: Similar communication functions are grouped into logical layers. A layer provides services to its upper layer while receiving services from the layer below.

3.1.46

policy

constraints on functions and information flow between functions

Note 1 to entry: Policy is typically described as principles or rules to guide decisions and achieve rational outcomes.

3.1.47

policy decision point

logical entity that makes admission control and policy decisions in response to a request from a user wanting to access a protected resource

3.1.48

policy enforcement point

logical entity that intercepts a user's access request to a resource and enforces the policy-decision-point entity's decision

3.1.49

policy information point

logical entity that can provide external information to a policy-decision-point entity

3.1.50

Physical layer

communication protocol layer that defines electrical and physical specifications for connecting a device and a transmission medium

3.1.51

programmable logic controller

programmable microprocessor-based device that is used in discrete manufacturing to control assembly lines and machinery on the shop floor as well as many other types of mechanical, electrical and electronic equipment in a plant

3.1.52

profile

definition of functionality that provides sufficient information to guide implementers and support the creation of conformance tests that validate conformant operation

3.1.53**Purdue reference model**

architectural model for implementation of Computer Integrated Manufacturing, commonly used for plant information and control.

SOURCE: <http://www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.html>

3.1.54**quality of service (QoS)**

flow control method to measure and manage network bandwidth in an appropriate manner, per user expectations or goals

3.1.55**remote authentication dial-in user service**

networking protocol that provides centralized Authentication, Authorization, and Accounting management for computers to connect and use a network service

Note 1 to entry: See IETF RFC 2865 for more information.

3.1.56**request for comments (RFC)**

memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems

3.1.57**resource-reservation protocol**

network-control protocol that enables Internet applications to obtain special qualities of service for their data flows

Note 1 to entry: Resource-Reservation Protocol is not a routing protocol; instead, it works in conjunction with routing protocols and installs the equivalent of dynamic access lists along the routes that routing protocols calculate. See IETF RFC 2205 for more information.

3.1.58**satellite link**

communication path between a communication satellite and an earth-based communication station

3.1.59**security assurance level**

measure of confidence that computer systems and data are free from vulnerabilities, either intentionally designed into computer components or accidentally inserted at any time during its lifecycle, and that the computer systems function in the intended manner.

3.1.60**security content automation protocol**

protocol that combines a number of open standards used to enumerate software flaws and configuration issues related to security

Note 1 to entry: The constituent protocols measure systems to find vulnerabilities and offer methods to score those findings in order to evaluate the possible impact. It is a method for using those open standards for automated vulnerability management, measurement, and policy compliance evaluation. See NIST SP800-126 Rev. 2 for more information.

3.1.61**session**

semi-permanent, stateful, interactive information interchange between two or more communicating devices

SOURCE: IEC 62443-1-1