

TECHNICAL REPORT
ANSI/ISA-TR100.15.01-2012
A Technical Report prepared by ISA and registered with ANSI

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

Approved 29 October 2012
ANSI registration effective 22 March 2015

ANSI/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 ANSI/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.

The following participated in the development of this ISA Technical Report:

Penny Chen, *ISA100 WG15 Co-Chair*
David Glanzer, *ISA100 WG15 Co-Chair*
Steven Venema, *ISA100 WG15 Editor*
Soloman Almadi
Soliman Al-Walaie
Soroush Amidi
Patricia Brett
Eric Byres
Kouji Demachi
Sicco Dwars
Marcelo Barros de Almeida
Andy de Clerck
Marcello Luis Dultra
Denis Foo Kune
Peter Fuhr
Brian Green
Ted Hansen
Toshi Hasegawa
Jean-Pierre Hauet
Hisanori Hayashi
William Hodson
Ji Huang
James Jamison
Gareth Johnston
Patrick Kinney
David Lafferty
Greg LaFramboise

Wayne Manges, *ISA100 Co-Chair*
William J. Miller
Hiroshi Miyata
Geoff Mulligan
Mark J. Nixon
Johan Nye
Kenji Ooishi
Tom Phinney
Jeff Potter
Gary Reeves
Flavien Richard
Shoichi Sakane
Onkar Sangha
Patrick Schweitzer
Paul Sereiko
Daniel Sexton
Justin Smith
Warren Smith
Rene Struik
Herman Storey, *ISA100 Co-Chair*
Tatsuaki Takebe
Sergio Tateishi
Steve Toteda
Kevin Towers
Nigel Townsend
Quan Wang
David Womack

Contents

Foreword	7
1 Scope	9
1.1 General.....	9
1.2 Wireless vs. wired backhaul networks	9
1.3 Specific goals	10
2 Normative references	10
3 Terms, definitions and abbreviations	11
3.1 Terms and definitions.....	11
3.2 Abbreviations	19
4 Backhaul architecture.....	21
4.1 General.....	21
4.2 Backhaul model	21
4.3 Architecture elements	22
4.4 Interface model.....	23
4.5 Interface definitions	23
5 Security model	24
5.1 Overlay of IEC 62443 on this architectural model	24
5.2 Per-interface security description	26
5.3 System policies.....	28
5.4 Identity and authentication	28
5.5 Status and event logging.....	29
6 Distributed management model	29
6.1 General.....	29
6.2 Functions of the “configuration, security and management domain (CSMD)”	29
6.3 Management communication channels	29
6.4 Distributed management security	30
6.5 Event logging	31
6.6 Common configuration sets.....	31
6.7 Management protocols.....	31
6.8 Bootstrapping challenges	31
7 Fault tolerance model.....	31
7.1 General.....	31
7.2 Redundant backhaul networks	31
7.3 Redundant backhaul interfaces	32
7.4 Redundant links	33
7.5 Fault detection, notification and handling actions (auto/manual).....	33
7.6 Online maintenance and upgrades	33
8 Mobility model (for example, mobile workers)	34
8.1 General.....	34
8.2 Mobile workers in different zones	34
8.3 Multi-access-point mobility for a given user.....	35
9 Flow control model.....	36

9.1	Overview.....	36
9.2	Functions of flow control	37
9.3	Per-interface flow control functions	41
9.4	Flow control policies	42
9.5	Flow control model for mobility.....	43
9.6	Flow control model for security.....	43
Annex A (informative) Example implementation using the Purdue reference model.....		45
BIBLIOGRAPHY		46
Figure 1	— Example applications using a shared backhaul network.....	9
Figure 2	— Example industrial control system using backhaul connectivity	21
Figure 3	— Generalized backhaul interface model	22
Figure 4	— Example showing mapping of backhaul interfaces to IEC 62443 security model	25
Figure 5	— Example of remote management capability.....	30
Figure 6	— Redundant BSPs and multi-homed BHIs.....	32
Figure 7	— Redundant BHIs and redundant links.....	33
Figure 8	— Example of mobile workers in different zones	34
Figure 9	— Example of a single mobile worker migrating between access points in a given zone	35
Figure 10	— Flow control example for backhaul.....	36
Figure 11	— Example of flow control with third-party BSP	38
Figure 12	— Examples of edge router locations	40
Figure 13	— Example using backhaul architecture model and extended Purdue reference model	45

Foreword

Publication of this Technical Report that has been registered with ANSI has been approved by ISA, 67 Alexander Drive, Research Triangle Park, NC 27709. This document is registered as a Technical Report according to the Procedures for the Registration of Technical Reports with ANSI. This document is not an American National Standard and the material contained herein is not normative in nature. Comments on the content of this document should be sent to the Secretary, Standards and Practices Board; ISA; 67 Alexander Drive; P. O. Box 12277; Research Triangle Park, NC 27709.

This technical report is of wide applicability because it provides a common framework enabling multiple industrial communication protocols to run over a shared wireless backhaul network in process automation systems.

This page intentionally left blank.

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.

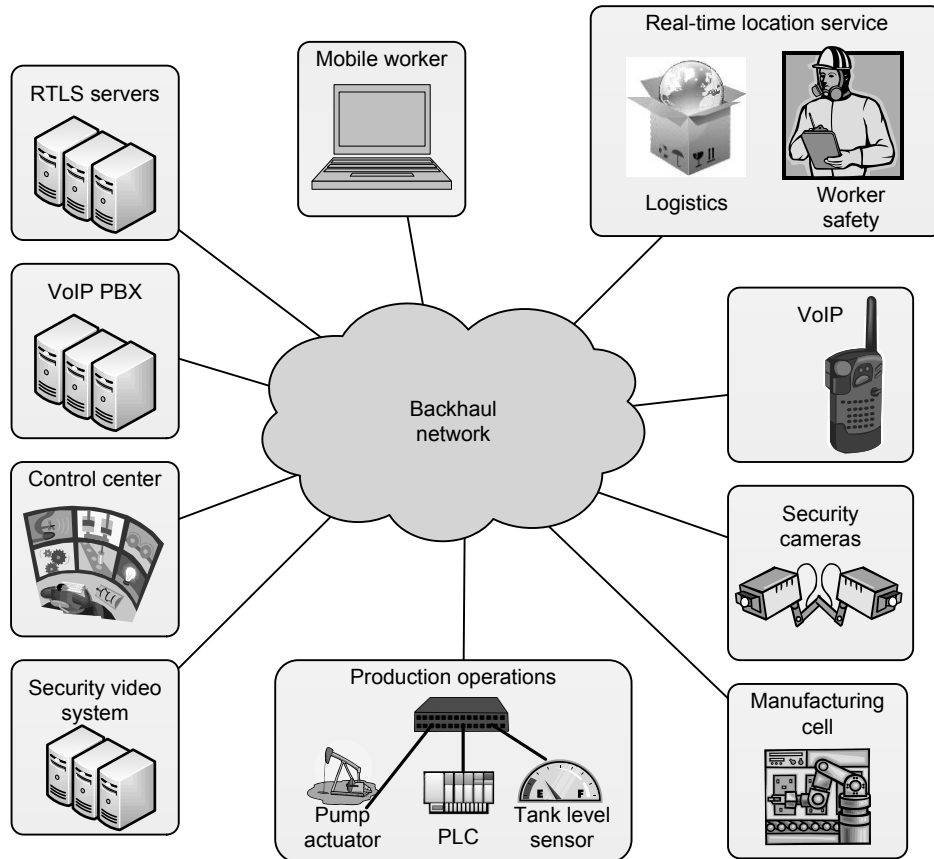


Figure 1 — Example applications using a shared backhaul network

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.