

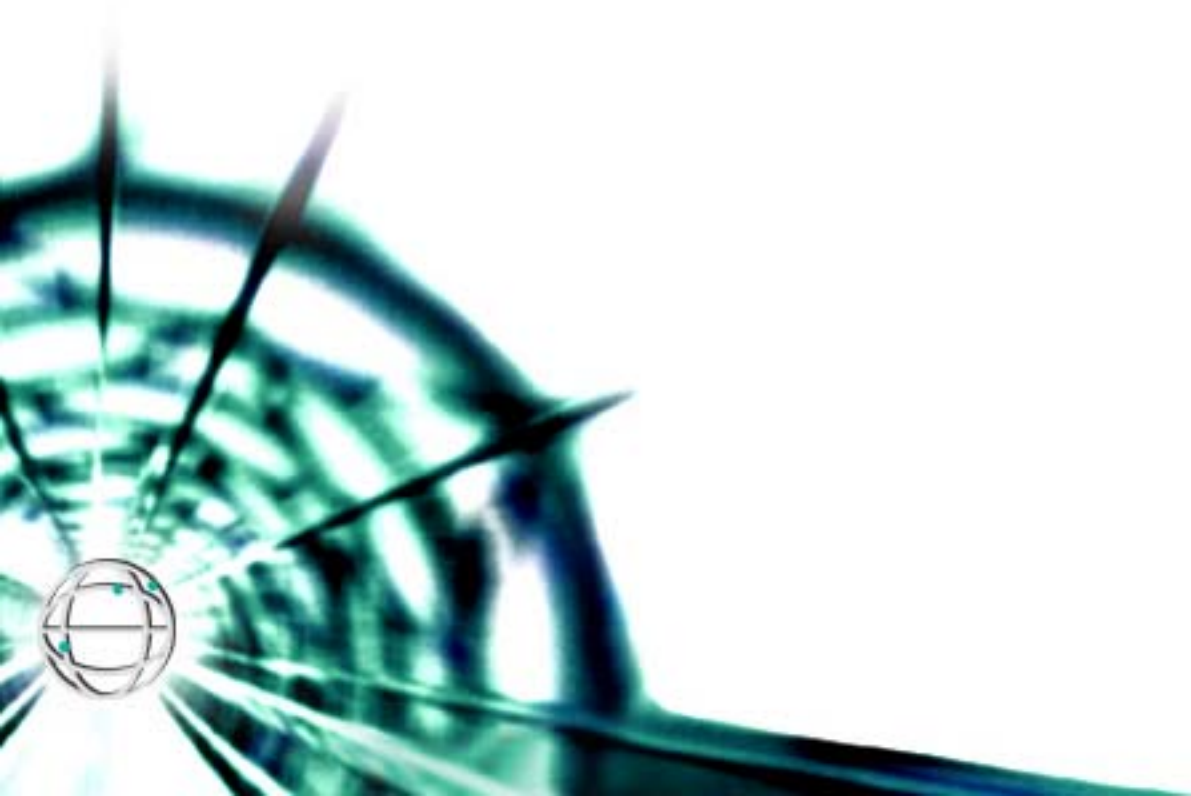
iaona



IAONA Handbook

Network Security

Version 1.3



The IAONA Handbook for Network Security

Version 1.3

Published by IAONA e.V.

Based on the work of IAONAs Joint Technical Working Group (JTWG) Network Security.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

The following parties have contributed to this document:

DEHOF computertechnik	Matthias Dehof (Chairman JTWG Network Security)
ABB	Martin Naedele, Dacfeý Dzung
Data Systems	Detlef Kilian
Innominate AG	Steffen Bruß, Frank Merkel
iniNet GmbH / VPI	Peter Brügger
Hirschmann AC GmbH	Klaus Reister, Ralf Kaptur
TRUMPF Laser GmbH + Co. KG	Rainer Thieringer
University Magdeburg	Marcus Tangermann
WAGO Kontakttechnik	Christoph Möller

All illustrations, charts and layout examples shown in this document are intended solely for purposes of example. IAONA assumes no responsibility or liability (including intellectual property liability) for actual use based upon examples given in this publication.

Reproduction of the contents of this copyrighted publication, in whole or in part, without written permission of IAONA is prohibited.

© IAONA, 2005
IAONA e.V.
Universitätsplatz 2
39106 Magdeburg
Germany
info@iaona.org
<http://www.iaona.org>

Contents

- 1 Introduction..... 5**

- 2 Basics for Industrial Ethernet Security 7**
 - 2.1 What is Security? 7
 - 2.2 Security Classification 9
 - 2.2.1 Security Classification Example - Light Bulb Factory 10
 - 2.2.2 Security Classification Example - *Automotive parts* 10
 - 2.2.3 Security Classification Example – *Pharmaceutical process* 11
 - 2.3 The IP protocol family 11
 - 2.3.1 Design of the IP family 12
 - 2.3.2 Security Problems of IP 13
 - 2.4 Communication relations in an enterprise network 14
 - 2.5 Network architecture for Industrial Ethernet 16
 - 2.6 Defense strategy 18
 - 2.6.1 Hard-perimeter 18
 - 2.6.2 Defense-in-depth 19
 - 2.7 Security Components 20
 - 2.7.1 Packet Filter 20
 - 2.7.2 Application Gateway 22
 - 2.7.3 Demilitarized Zone (DMZ) 23
 - 2.7.4 Switches 23
 - 2.7.5 Router 23
 - 2.8 Differences between Office and Automation Networks 24

- 3 IAONA Security Methodology..... 27**
 - 3.1 Security demand classification 28
 - 3.2 Communication relations 29
 - 3.3 Defense Strategy 31
 - 3.4 Defense Structures 31
 - 3.5 Devices / Protocols 33
 - 3.6 Defense measures 34

- 4 The Security Cookbook..... 37**
 - 4.1 Remote Access 37
 - 4.1.1 Terminal Server 37
 - 4.1.2 Network Manager 38

- 5 IAONA Security Data Sheet 40**
 - 5.1 How to fill out the SDS 40
 - 5.1.1 General 40
 - 5.1.2 Page 1 - General 41
 - 5.1.3 Page 2 - Network Ports and Services 41
 - 5.1.4 Naming Conventions 42
 - 5.2 Security Data Sheet Creator (SDS-C) 42

- 6 Annex: Communication Relations Table Template 43**

- 7 Annex: Security Data Sheet Template 44**

- 8 Annex: Security Data Sheet XML Schema 47**

9 Annex: Network Services.....	49
9.1 ICMP	51
9.2 ARP	52
9.3 DHCP	52
9.4 DNS.....	53
9.5 FTP	53
9.6 TFTP	54
9.7 Telnet	54
9.8 SMTP	55
9.9 SSH.....	56
9.10 SNMP	56
9.11 HTTP	57
9.12 DynDNS	58
9.13 Modbus-TCP	59
9.14 EtherNet/IP.....	59
9.15 ETHERNET Powerlink	60
9.16 RPC / DCOM.....	60
9.17 LDAP	61
9.18 Kerberos.....	61
9.19 IPSEC	62
9.20 PPTP	63
9.21 L2TP / IPsec.....	63
9.22 SOAP	64
9.23 Remote control software	65
9.24 NDDS	65
9.25 MAP/MMS	66
9.26 RADIUS.....	66
10 Annex: IAONA SDS Logo.....	68
11 References	69

1 Introduction

Ethernet based communication systems have entered the factory floor. During the last 5 years different fields of application using different Ethernet based communication protocols and technologies have been established ranging from web based management of devices to motion control applications.

This increasing use of Ethernet based services and devices came for many companies through the backdoor: first a simple FTP session for firmware uploads and a telnet session for changing settings, then a web server for advanced and comfortable configuration and diagnostics, and finally the use of real-time Ethernet communication protocols for device communication within control applications. It was a small step from using these devices point-to-point connected to a serviceman's laptop to connecting the devices to a company network. With the broad use of PC based devices, it was possible to connect anything and for quite a time, finally, the network was just what it was made for.

But with the increasing use of Ethernet based communication technologies also the problems of this technology have entered the factory network. The possible data exchange using eMails or direct device access will enable an undue influence on the devices by hackers, with-collar criminals, or even unilluminated employees.

When more people were accessing the network - and an increasing number of non-technicians and non-employees were among them - the network was opened to the Internet and was used for web-access and eMail services. Thereby, viruses and worms coming with laptops and eMails, some of them do no harm but others may cause the loss of a complete production line. Even when these viruses have no direct effect on devices, overloaded network traffic is even worse than a single deleted hard disk.

The direct access to control devices using HTTP or SNMP based device management systems will, in principle, enable unauthorized people to acquire control system and production system sensitive data and to change sensitive system settings causing economic disadvantages.

As a matter of fact, the IT departments are confronted with a complete new line of problems. Any intrusion, by accident or intention has a bigger effect than in the office world.

An automation network needs to be fail-safe. Data within an automation system need to be protected from unauthorized access. The unauthorized change of control relevant data or even the circumvention of a data exchange may result in a production system break down. A down time of a production line of a few minutes can cost some thousands of Euros because it may take some hours to restart the complete line. In contrast to this a short breakdown in the office environment is equally disturbing, but the consequences are different.

To cope with the mentioned problems and to ensure the security of industrial communication systems special technologies and strategies have been developed or even from the office world adapted to the factory floor. One important role within this process has been played by the IAONA Joint Technical Working Group (JTWG) "Network Security". Within this JTWG the state of the art of network security technologies for industrial application have been collected and aggregated to an advice for best practice.

Based on the results of the IAONA JTWG "Network Security" the Handbook - Network Security has been created. It will be maintained by the members of the JTWG and reflects the current status of technology. The Handbook is not a static book, but subject to change to keep up with threats and developments.

The Handbook was designed to

- establish "know-how" for network security in industrial applications and make this accessible for to users

- give recommendations on how to plan secure networks
- provide tools for network analysis and escalation schemes
- create guideline for network security to be provided to IT and factory floor personnel
- give input to normative committees, such as IEC

The user's benefits are

- support for security risk analysis,
- support in the selection of appropriate security measures and
- most important - the avoidance of production down time caused by security leaks.

All-in-all, the IAONA Handbook - Network Security will provide interested people with the necessary knowledge about existing security problems, useable security architectures, and all necessary activities to establish these architectures.

To follow this aims the handbook is organized as follows.

Within the following (the second) chapter necessary basics about network security will be described. This includes a definition of the term "Security", the term of IAONA Security Classes, the description of basic protocols, structures, and architectures and its security problems, defense strategies, and security components with its security relevant behavior.

The third chapter will describe in detail the security methodology developed by IAONA JTWG "Network Security" with strategies, structures, devices, protocols, and defense measures.

Chapter four can be seen as a cookbook for network security providing best practice scenarios for special application cases.

Chapter five introduces the IAONA Security Data Sheet, a mean for collection and distribution of security relevant information of devices, systems, and networks based on the IAONA Security Methodology. Within this chapter the IAONA Security Data Sheet will be described in detail and its application and benefits in practice will be considered.

The handbook will conclude with three annexes. The first annex will provide a template of the IAONA Security Data Sheet and the second one will give the XML schema used for the computer based processing of the IAONA Security Data Sheet. The third annex will provide a detailed listing and description of 28 Ethernet based communication protocols used within factory communication systems including a security relevant survey of each protocol.

The full version of this IAONA Handbook is currently only available for
IAONA's members!

Please contact IAONA's office for more information!