Security Guide

Honeywell

Touchpoint Pro

Revision History

Revision	Comment	Date
Issue 01	A04815	Nov 2016

LEGAL NOTICES

Disclaimer

In no event shall Honeywell be liable for any damages or injury of any nature or kind, no matter how caused, that arise from the use of the equipment referred to in this manual.

Strict compliance with the safety procedures set out and referred to in this manual, and extreme care in the use of the equipment, are essential to avoid or minimise the chance of personal injury or damage to the equipment.

The information, figures, illustrations, tables, specifications, and schematics contained in this manual are believed to be correct and accurate as at the date of publication or revision. However, no representation or warranty with respect to such correctness or accuracy is given or implied and Honeywell will not, under any circumstances, be liable to any person or corporation for any loss or damages incurred in connection with the use of this manual.

The information, figures, illustrations, tables, specifications, and schematics contained in this manual are subject to change without notice.

Unauthorised modifications to the gas detection system or its installation are not permitted, as these may give rise to unacceptable health and safety hazards.

Any software forming part of this equipment should be used only for the purposes for which Honeywell supplied it. The user shall undertake no changes, modifications, conversions, translations into another computer language, or copies (except for a necessary backup copy).

In no event shall Honeywell be liable for any equipment malfunction or damages whatsoever, including (without limitation) incidental, direct, indirect, special, and consequential damages, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss, resulting from any violation of the above prohibitions.

Warranty

Honeywell Analytics warrants the Touchpoint Pro system against defective parts and workmanship, and will repair or (at its discretion) replace any components that are or may become defective under proper usage within 12 months from the date of commissioning by a Honeywell Analytics approved representative* or 18 months from shipment from Honeywell Analytics, whichever is sooner.

This warranty does not cover consumables, batteries, fuses, normal wear and tear, or damage caused by accident, abuse, improper installation, unauthorized use, modification or repair, ambient environment, poisons, contaminants or abnormal operating conditions.

This warranty does not apply to sensors or components that are covered under separate warranties, or to any 3rd-party cables and components.

Any claim under the Honeywell Analytics Product Warranty must be made within the warranty period and as soon as reasonably practicable after a defect is discovered. Please contact your local Honeywell Analytics Service representative to register your claim.

This is a summary. For full warranty terms please refer to the Honeywell Analytics' General Statement of Limited Product Warranty, which is available on request.

* A Honeywell Analytics approved representative is a qualified person trained or employed by Honeywell Analytics, or a qualified person trained in accordance with this manual.

Copyright Notice

CONTENTS

1 Contents

INTRODUCTION

2 Introduction

This guide has been designed for use by operators and Information Technology (IT) personnel of customers who have a Honeywell Touchpoint Pro (TPPR) system.

It is intended for use when planning the configuration and maintenance of the network infrastructure in which the TPPR system exists.

It provides information supporting identification and mitigation of security risks associated with the day to day use of the system in connected IT infrastructures

2.1 Scope

This document applies to Touchpoint Pro systems in a networked environment, associated computers, and data storage media.

2.2 Assumptions and pre-requisites

This guide assumes a high degree of technical knowledge and familiarity with:

- PC administration and operating systems
- Networking systems and concepts
- Security issues and concepts

2.3 Related documents

This guide should be read in conjunction with the following documents:

Document	Part Number
Touchpoint Pro Technical Handbook	2400M2501
Webserver User Guide	2400M2563
PC Configuration Software Operating Manual	2400M2564

Table 1. Related Documents

2.4 Security Controls

The Touchpoint Pro system has a number of built in security controls. These include:

- Limitation of access to designated users
- Password protection of user accounts
- Secure (https) web server connection
- Web server device certificate
- Reduction of confidential data

2.4.1 Additional User Controls

This guide focuses on additional security controls that should be implemented by users.

2.4.2 Further Information

Contact your Honeywell representative if you need more information on securing your TPPR system.

IT ARCHITECTURE

3 IT System Architecture

Touchpoint Pro may be configured in a variety of network topologies, from simple peer to peer or isolated LAN to a corporate network with internet access.

This guide is primarily concerned with systems connected to a WAN or corporate network with possible Internet access.

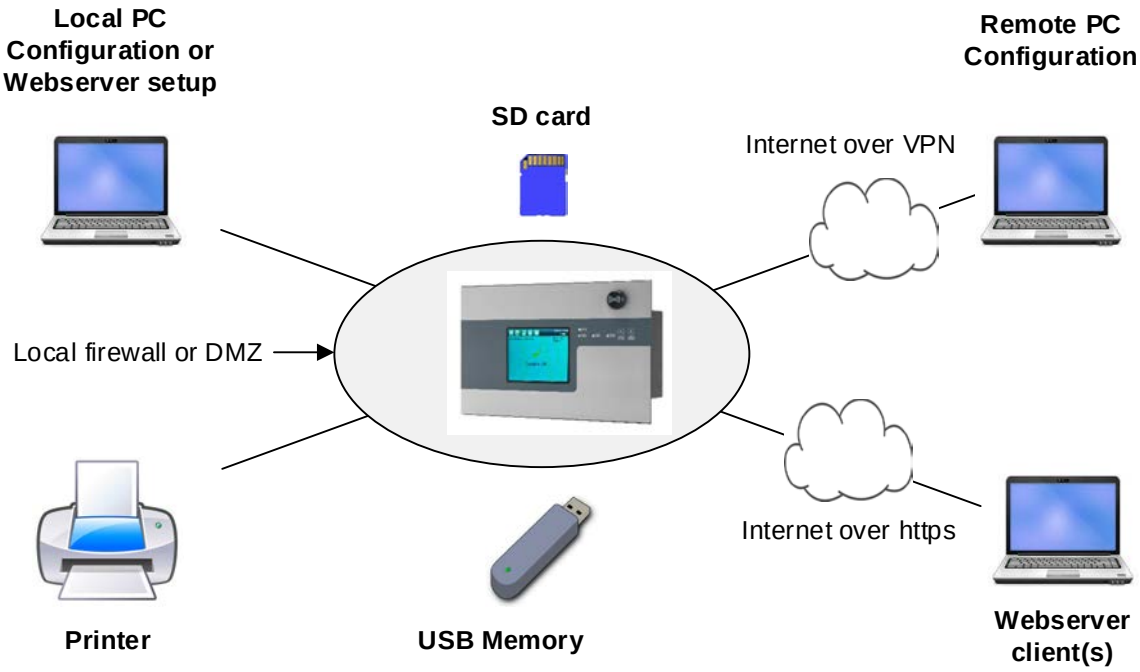

Figure 1. System Architecture Options

3.1 Ethernet Remote Connections

Possible Ethernet connections include:

Connection	Scope	Remark
PC Configuration Tool	Intranet or internet	Single user permitted
Webserver clients	Intranet or internet	Multiple clients
Ethernet printer	Intranet or internet. Typically intranet.	Single printer supported
Webserver Setup	Intranet or internet. Typically intranet.	Short term single user access

Table 2. Connections via Ethernet

3.2 Physical and Local connections

Physical connections are:

- Touch screen/front panel
- USB memory device
- SD memory device

4 Threats

Security threats applicable to networked systems include:

- Unauthorised Access
- Communications Snooping
- Viruses and other malicious software agents

4.1 Unauthorised access

This threat includes physical access to the controller and intrusion into the network to which TPPR system is connected, from the business network / intranet or the Internet.

Unauthorized external access can result in:

- Loss of system availability
- Incorrect execution of controls causing damage to the building, incorrect operation, or spurious alarms
- Theft or damage of its contents
- The capture, modification, or deletion of data
- Loss of reputation if the external access becomes public knowledge

Unauthorised access to the system can result from:

- Lack of security of user name and password credentials
- Uncontrolled access to the controller
- Uncontrolled access to the network and network traffic

4.2 Communications snooping

This threat includes snooping on or tampering with the Ethernet communication link on port 4000 (remote configuration port) while the port is enabled, by means of man-in-the-middle, packet replay or similar methods.

Tampering with the communication link can result in:

- Loss of system availability
- Incorrect configuration and so incorrect execution of TPPR safety function
- The capture, modification, or deletion of data

The configuration port is open when the PC Configuration tool is in use, and for initial setup and maintenance of the Webserver utility.

The configuration port can only be opened by users having physical access to the controller and suitable login credentials. The configuration port is time limited and cannot be left open when not in use.

4.3 Viruses and other malicious software agents

This threat encompasses malicious software agents such as viruses, spyware (trojans), and worms. These may be present:

- On a PC which is used for PC Configuration Software
- On PCs from which TPPR web interface is accessed using web clients
- On any other nodes of the network to which TPPR system is connected

The intrusion of malicious software agents can result in:

- Performance degradation
- Loss of system availability
- The capture, modification, or deletion of data, including configuration data and device logs

Viruses can be transmitted by media such as USB memory devices and SD cards, from other infected systems on the network, and from infected or malicious Internet sites.

MITIGATION STRATEGIES

5 Mitigation Strategies

The following mitigation strategies should be followed

5.1 Touchpoint Pro System

5.1.1 Monitor System Access

In addition to the security controls listed in paragraph 3.4, the TPPR has the following facilities which can be used to identify unexpected configuration changes:

1. On Screen Warning

   The TPPR system displays an on-screen warning when the configuration has been changed since the last backup. The warning can only be cleared by a sufficiently authorised user backing up the system, or restoring a previous backup. These operations can only be carried out locally at the TPPR controller.

2. Configuration Counter

   TPPR maintains a configuration counter which is incremented when any configuration change is made. The increment is variable. Any change indicates a configuration change.

   The configuration counter is accessible from **Tool box, Help**

3. Last Login

   The login name of the last logged in user may be viewed and checked if changes have been carried out.

   The last login username is accessible from **Tool box, Help**

4. Event History and Log

   All user logins and system operations are recorded in the event log and may be viewed on the event history screen or by generating an event report.

The above should be routinely monitored and verified as part of system maintenance.

5.1.2 User Access and Passwords

Touchpoint Pro has three levels of user. Users at each level have unique usernames and passwords. Observe the following good practice:

1. Ensure physical security of passwords. Avoid writing user names and passwords where they can be seen by unauthorised personnel.
2. Set the minimum level of access for each user. Do not provide users with privileges they do not need.
3. Create a separate user name and password for each user. Avoid sharing of user names and passwords among multiple users.
4. Ensure that users only log in using their own credentials.
5. Periodically audit user accounts and remove any that are no longer required.
6. Ensure that passwords and user credentials are regularly changed.
7. Create a new Administrator account with new credentials and delete the default Administrator user.
8. Minimise the number of Administrator level users. The recommended number is two.

MITIGATION STRATEGIES

5.1.3 Software and Unusual Operation

Touchpoint Pro isolates the gas detection system from the user interface. If unusual operation is observed on the user interface, the following measures may be taken:

1. Restart the user interface to reload the software. This will not interrupt operation of the gas detection system, although reporting to the touchscreen will be interrupted for a short time:

   Press and hold the Accept and Reset buttons on the front panel for approximately ten seconds, until the user interface software is observed to restart. This operation can only be carried out at the controller. The system will indicate a fault for several seconds. It may be necessary to isolate interfaces to higher level equipment.

2. Power cycle the controller. The gas detection and user interface software will be reloaded. The gas detection system will be unavailable for several minutes, and outputs will be generated. It may be necessary to isolate interfaces to higher level equipment. It is not necessary to remove power to modules if separately powered.

Unusual operation of a TPPR controller should be reported to your service representative.

5.1.4 Memory Media

Touchpoint Pro uses SD Card and USB memory media:

1. Use only authorized removable media that has been scanned and checked for viruses and malware using up to date anti-virus software.
2. Ensure that memory media used for Touchpoint Pro is not used for other purposes, to avoid risk of infection.
3. Control access to media containing backups, to avoid risk of tampering.

5.1.5 Configuration Port

The Configuration Port allows access for the PC Configuration Software tool and for setting up and licensing the Webserver. The port may only be opened by a sufficiently authorised user at the controller, and closes automatically after a fixed period, or when an inactivity timeout occurs.

1. The configuration port should only be used in a trusted safe environment on a secure network.
2. The port should be closed manually from the controller IP Configuration screen when access is no longer required.

5.1.6 Software and Firmware Updates

System software and firmware updates and upgrades may be offered from time to time, which may include additional or updated security features. To remain informed of updates:

1. Ensure that your local representative has up to date contact details.
2. Periodically visit the Touchpoint Pro web site. _____

5.2 Computers and Access

Good security practices should be observed on computers and networks to which TPPR systems may be connected, including peer to peer and LAN connections.

5.2.1 Operating Software

Operating systems and browsers should be kept up to date by installing the manufacturer's updates.

5.2.2 Virus Protection

Maintain up to date anti-virus software on all computers which may be connected, either directly or via a network, to TPPR systems. Ensure that computers are regularly scanned.

5.2.3 Files and Media

Allow only files and software from trusted sources to be installed and used on associated computers.

Use only authorized removable media, e.g. CD/DVD, external hard drives, USB memory sticks that have been scanned using up to date anti-virus software.

MITIGATION STRATEGIES

5.2.4 User Access and Passwords

Good password security practices should be followed.

1. Require the use of strong passwords and user account controls.
2. Ensure physical security of passwords. Avoid writing user names and passwords where they can be seen by unauthorised personnel.

Computers connected to TPPR systems should not be left unattended when a configuration session is open. Access should be restricted to authorised users.

5.2.4.1 TPPR Passwords

TPPR passwords are not held or stored on computers running PC Configuration Software or Webserver clients. Remote users are required to log in after connection. Physical security of TPPR passwords should be maintained at computers used for remote connection.

5.3 Networks, Firewalls & VPN connections

5.3.1 Physical Access

Physical access to network nodes and infrastructure should be limited to authorised personnel to prevent tampering.

5.3.2 Firewall and DMZ

The network design should limit the access to the TPPR system from the wider network, for instance by use of local firewalls or DMZ area. The number of components in the same area as the TPPR should be kept to the minimum, especially when the configuration port may be in use.

5.3.3 Internet and VPN

Where access from untrusted networks is required, such as internet access, a VPN must be used to ensure the security of the connection.

GLOSSARY

6 Glossary

6.1 Abbreviations

The following abbreviations are used:

Abbreviation	Meaning
DMZ	De-Militarized Zone, used to restrict access from parts of a network
https	Hypertext Transfer Protocol secure version
LAN	Local Area Network
PC	Personal Computer
SD	Secure Digital memory card
TPPR	Touchpoint Pro gas detection system
USB	Universal Serial Bus memory devices
VPN	Virtual Private Network

Find out more at

www.norrscope.com

www.norrscope.com

.

Please Note:

While every effort has been made to ensure accuracy in this publication, no responsibility can be accepted for errors or omissions. Data may change as well as legislation and you are strongly advised to obtain copies of the most recently issued regulations, standards and guidelines. This publication is not intended to form the basis of a contract.

Honeywell

Part Number 2400M2567

Issue 1

AP: