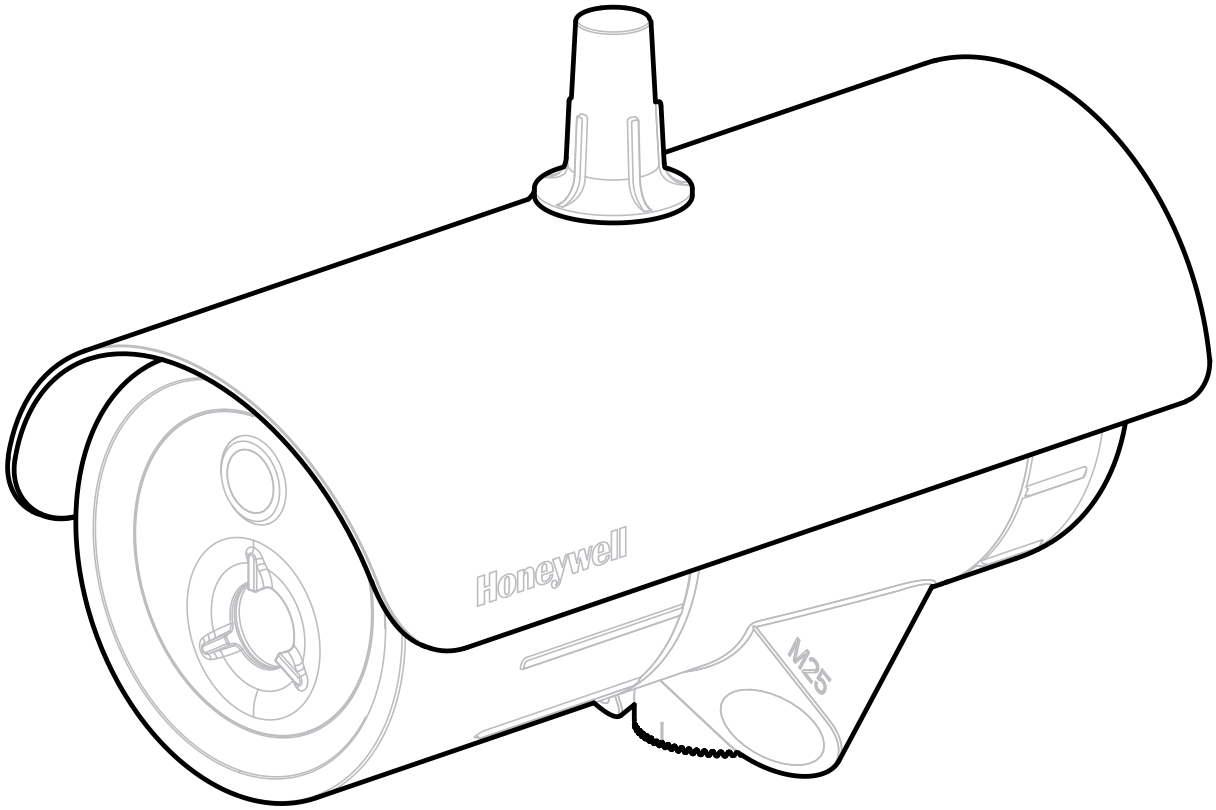
SECURITY GUIDE

SEARCHZONE SONIK™

Acoustic Gas Leak Detector



Honeywell

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 Searchzone Sonik™ Ultrasonic Gas Leak Detector against defective parts and workmanship and will repair or (at its option) replace any instruments which are or may become defective under proper use within 36 months from date of shipment from Honeywell Analytics. This warranty does not cover consumable items, normal wear and tear or damage caused by accident, abuse, improper installation, poisons, contaminants or abnormal operating conditions. Under no circumstances shall Honeywell Analytics liability exceed the original purchase price paid by the buyer for the product. Any claim under the Honeywell Analytics Product Warranty must be made within the warranty period and as soon as reasonably possible after a defect is discovered. In the event of a warranty claim please contact your local Honeywell Analytics Service representative.

This is a summary, for full warranty terms please refer to the Honeywell “General Statement of Limited Product Warranty” available upon request.

Copyright Notice

Find out more at www.sps.honeywell.com

1 Introduction

This guide has been designed for use by operators and engineering personnel of customers who utilize Searchzone Sonik system. It is intended for use when planning the configuration and maintenance of the network infrastructure in which the Searchzone Sonik 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.

1.1 Scope

This document applies to Searchzone Sonik system, to associated mobile application and device, and to wireless data transfer.

1.2 Revision history

Revision	Comment	Date
Issue 1	ECO A05126	July 2018
Issue 2	ECO A05425	February 2021

1.3 Assumptions and pre-requisites

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

- Management through mobile application
- Networking systems and concepts
- Security issues and concepts

1.4 Related documents

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

Document	Part Number
Searchzone Sonik Technical Manual	2331M1220

1.5 Security controls

Searchzone Sonik system has a number of built in security controls. These include:

- Limitation of access to designated users
- Password protection of user accounts
- Device certificate
- User certificate

1.5.1 Additional user control

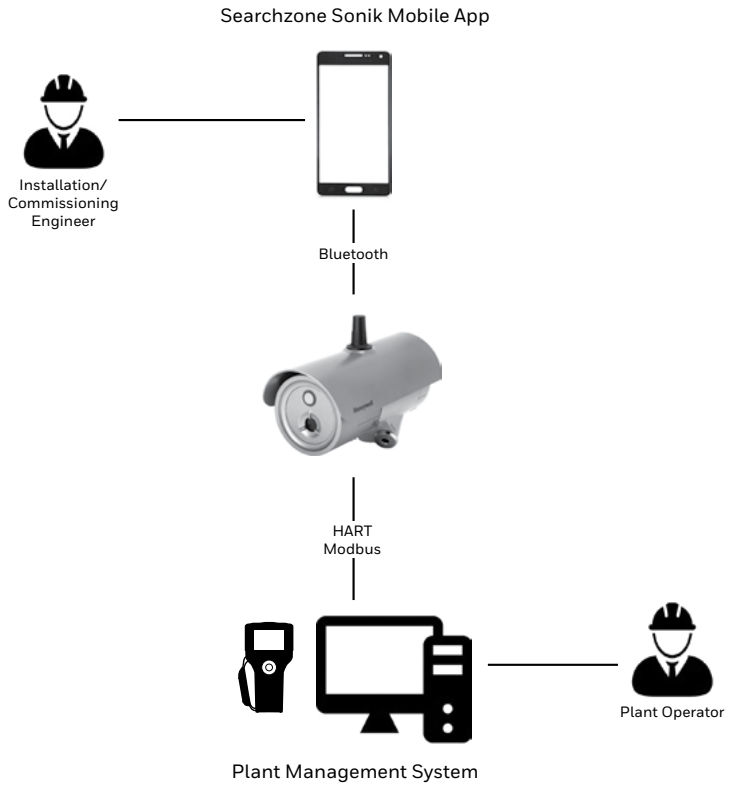
This guide focuses on additional security controls that should be implemented by users.

1.5.2 Further information

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

2 IT System architecture

Searchzone Sonik can be configured using Bluetooth connection, HART or MODBUS communications.
See the communications diagram below.



2.1 Wireless connections

Searchzone Sonik utilizes Bluetooth wireless connection, single user permitted.

2.2 Physical and local connections

Searchzone Sonik utilizes HART and MODBUS communications.

3 Threats

Security threats applicable to networked systems include:

- Unauthorised access
- Communications snooping
- Viruses and other malicious software agents

3.1 Unauthorized access

This threat includes physical access to Searchzone Sonik and intrusion into the network to which Searchzone Sonik system is connected, from the business network.

Unauthorized external access can result in:

- Loss of system availability
- Incorrect execution of controls causing damage to the facility, 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 detector
- Uncontrolled access to the network and network traffic

3.2 Communications snooping

This threat includes snooping on or tampering with Bluetooth 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 the Searchzone Sonik safety function
- The capture, modification, or deletion of data

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

3.3 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 mobile device which is used for setup and configuration
- If the connected mobile device's software has been changed to enable capabilities that might not otherwise be present (rooted).

The intrusion of malicious software agents can result in:

- Performance degradation
- Loss of system availability
- 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.

4 Mitigation strategies

The following mitigation strategies should be followed.

4.1 Searchzone Sonik system

4.1.1 Monitor system access

In addition to the security controls, Searchzone Sonik has the following facility which can be used to identify unexpected configuration changes:

- 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. Use Searchzone Sonik Mobile App to access Event History and Log.

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

4.1.2 User access and passwords

Searchzone Sonik recognizes only one level of users. Users have unique usernames and passwords.
Each device is PIN protected. Observe the following good practice:

- Ensure physical security of passwords. Avoid writing user names and passwords where they can be seen by unauthorised personnel.
- Create a separate user name and password for each user. Avoid sharing of user names and passwords among multiple users.
- Ensure that users only log in using their own credentials.
- Periodically audit user accounts and remove any that are no longer required.
- Ensure that passwords and user credentials are regularly changed.
- Administer user name and password through Searchzone Sonik Mobile App.

4.1.3 Software and unusual operation

If Searchzone Sonik Mobile App becomes unresponsive, shut it down and relaunch.

4.1.4 Memory media

Observe the following good practice when using mobile device equipped with removable SD card:

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

4.2 Access

Good security practices should be observed on devices to which Searchzone Sonik may be connected. See below.

4.2.1 Operating Software

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

4.2.2 User Access and Passwords

Good password security practices should be followed.

- Require the use of strong passwords and user account controls.
- Ensure physical security of passwords. Avoid writing user names and passwords where they can be seen by unauthorised personnel. Searchzone Sonik Mobile Application should not be left unattended when a configuration session is open. Access should be restricted to authorised users.

4.2.3 Synch with server

Searchzone Sonik Mobile Application shall be connected to server at least once a year to refresh the detector certificate registration.

4.2.4 Access PIN, Activation Key

Prior to using Searchzone Sonik Mobile App you will receive Access PIN and Activation Key. Basic security measures should be taken.

- Do not share Access PIN or Activation Key with unauthorized personnel.
- Do not write down or record Access PIN or Activation Key.

Find out more
www.sps.honeywell.com

Contact Honeywell:

Europe, Middle East, Africa, India
Life Safety Distribution GmbH
Javastrasse 2
8604 Hegnau
Switzerland
Tel: +41 (0)44 943 4300
Fax: +41 (0)44 943 4398
India Tel: +91 124 4752700
gasdetection@honeywell.com

Americas
Honeywell Analytics Inc.
405 Barclay Blvd.
Lincolnshire, IL 60069
USA
Tel: +1 847 955 8200
Toll free: +1 800 538 0363
Fax: +1 847 955 8210
detectgas@honeywell.com

Asia Pacific
Honeywell Analytics Asia Pacific
7F SangAm IT Tower, 434 Worldcup Buk-ro,
Mapo-gu, Seoul 03922
Korea
Tel: +82-2-69090300
Fax: +82-2-69090328
analytics.ap@honeywell.com

Technical Services
EMEA: HAexpert@honeywell.com
US: HA.us.service@honeywell.com

Honeywell

02/2021
2331M1230 Issue 2