

# **Honeywell**

---

**Honeywell Wireless**

## **Honeywell Wireless Planning Guide**

WN02-100: Draft No. 1

Field Trial

2/07

### **Field Trial Draft**

#### **Honeywell Confidential & Proprietary**

This work contains valuable, confidential and proprietary information. Disclosure, use or reproduction outside of Honeywell Inc. is prohibited except as authorized in writing. This unpublished work is protected by the laws of the United States and other countries.

## Notices and Trademarks

**Copyright 2007 by Honeywell International Inc.  
Release Field Trial February 2007**

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a particular purpose and makes no express warranties except as may be stated in its written agreement with and for its customers.

In no event is Honeywell liable to anyone for any indirect, special or consequential damages. The information and specifications in this document are subject to change without notice.

Honeywell, PlantScape, Experion PKS, and **TotalPlant** are registered trademarks of Honeywell International Inc.

Other brand or product names are trademarks of their respective owners.

Honeywell International  
Process Solutions  
2500 West Union Hills  
Phoenix, AZ 85027  
**1-800 343-0228**

## About This Document

*Describe the purpose of the document. Example:* This document describes how to install and configure the Experion Station-TPS (ES-T) and Experion Server TPS (ESVT) nodes. The nodes become full members in Experion PKS as well as connect directly to the TPN (TotalPlant Network).

### Release Information

Document Name	Document ID	Release Number	Publication Date
Honeywell Wireless Planning Guide - WN02	WN02-100: Draft No. 1	Field Trial	2/07

### References

The following list identifies all documents that may be sources of reference for material discussed in this publication.

---

#### Document Title

---

### Contacts

#### World Wide Web

The following Honeywell web sites may be of interest to Process Solutions customers.

Honeywell Organization	WWW Address (URL)
Corporate	<a href="http://www.honeywell.com">http://www.honeywell.com</a>
Honeywell Process Solutions	<a href="http://hpsweb.honeywell.com">http://hpsweb.honeywell.com</a>

## Contacts

---

### Telephone





Contact us by telephone at the numbers listed below.

<b>Location</b>	<b>Organization</b>	<b>Phone</b>
United States and Canada	Honeywell IAC Solution Support Center	1-800-822-7673
Europe	Honeywell TAC-EMEA	+32-2-728-2704
Pacific	Honeywell Global TAC - Pacific	1300-300-4822 (toll free within Australia) +61-8-9362-9559 (outside Australia)
India	Honeywell Global TAC - India	+91-20-2682-2458
Korea	Honeywell Global TAC - Korea	+82-2-799-6317
People's Republic of China	Honeywell Global TAC - China	+86-10-8458-3280 ext. 361
Singapore	Honeywell Global TAC - South East Asia	+65-6580-3500
Taiwan	Honeywell Global TAC - Taiwan	+886-7-323-5900
Japan	Honeywell Global TAC - Japan	+81-3-5440-1303
Elsewhere	Call your nearest Honeywell office.	

---

## Symbol Definitions

The following table lists those symbols used in this document to denote certain conditions.

Symbol	Definition
	<p><b>CAUTION:</b> Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury. It may also be used to alert against unsafe practices.</p> <p><b>CAUTION</b> symbol on the equipment refers the user to the product manual for additional information. The symbol appears next to required information in the manual.</p>
	<p><b>WARNING:</b> Indicates a potentially hazardous situation, which, if not avoided, could result in serious injury or death.</p> <p><b>WARNING</b> symbol on the equipment refers the user to the product manual for additional information. The symbol appears next to required information in the manual.</p>
	<p><b>WARNING, Risk of electrical shock:</b> Potential shock hazard where HAZARDOUS LIVE voltages greater than 30 Vrms, 42.4 Vpeak, or 60 VDC may be accessible.</p>
	<p><b>ESD HAZARD:</b> Danger of an electro-static discharge to which equipment may be sensitive. Observe precautions for handling electrostatic sensitive devices.</p>



# Contents

<b>1.</b>	<b>ABOUT THIS GUIDE</b> .....	<b>13</b>
1.1	Intended audience.....	13
1.2	How to use this guide.....	13
1.3	Related documents.....	13
<b>2.</b>	<b>HONEYWELL WIRELESS OVERVIEW</b> .....	<b>15</b>
2.1	Key Features and benefits.....	15
2.2	About Honeywell Wireless Services.....	15
2.3	Wireless system overview.....	15
2.4	Wireless components.....	15
2.5	Wireless Server Tools (software package).....	16
2.6	About the Key Server Node.....	16
2.7	Wireless Installation Overview.....	16
2.8	For more information.....	17
	Current standards for wireless in automation and control environment.....	17
	About ISA SP-100.....	17
	Honeywell references.....	17
<b>3.</b>	<b>WIRELESS SITE PLANNING</b> .....	<b>19</b>
3.1	Site survey tasks.....	19
3.2	Site considerations.....	19
3.3	Radio Frequency Survey.....	19
3.4	Hazardous Location requirements.....	19
3.5	Wireless Device Placement.....	19
3.6	Key Server and Authentication Device.....	20
3.7	Wireless installation requirements.....	20

<b>4.</b>	<b>WIRELESS NETWORK PLANNING .....</b>	<b>21</b>
4.1	Network planning guidelines.....	21
4.2	Wireless network architecture topology examples.....	21
4.3	Wireless network redundancy requirements and implementation .....	21
4.4	About the Network Analysis Tool .....	21
<b>5.</b>	<b>WIRELESS SECURITY PLANNING.....</b>	<b>23</b>
5.1	Security planning checklist .....	23
5.2	Network protection: protected against deliberate attack or human error by: 23	
5.3	Industrial Wireless Security Features .....	23
5.4	About device authentication.....	23
5.5	About security keys.....	23
5.6	About the Key Server .....	23
5.7	Wireless Security Requirements.....	24
5.8	Secure Wireless Architecture.....	24
5.9	Mitigating wireless security threats.....	24
<b>6.</b>	<b>ABOUT WIRELESS COMMUNICATIONS .....</b>	<b>25</b>
6.1	Communication for a wireless network infrastructure .....	25
6.2	Industrial Wireless network is developed as a multi-use wireless network. 25	
6.3	Wireless Primary Protocols.....	25
6.4	Wi-Fi and Gateway protocols .....	25
6.5	IP addressing iNodes .....	25
6.6	Wireless Data Access.....	26
6.7	Monitoring Data Access.....	26
6.8	Control Data Access.....	26



- 7. WIRELESS MAINTENANCE PLANNING .....27**
- 7.1 Pre-configuring local access to field devices for an emergency (..... 27**
- 7.2 Device Power Failure Recovery and Authentication - references ..... 27**
- 7.3 Device Replacement and Authentication - references ..... 27**
- 7.4 List of references for each of the Wireless components ..... 27**

## **Tables**

**Error! No table of figures entries found.**

## **Figures**

**Error! No table of figures entries found.**



# 1. About this Guide

## 1.1 Intended audience

- Defined users
- Prerequisite skills (knowledge of Open Standard protocols like MODBUS and OPC, basic knowledge of wireless system and techniques, basic knowledge of security protocols such as boot strapping, establishing a secure session)

## 1.2 How to use this guide

## 1.3 Related documents

- Provide references to other Knowledge Builder documents that contain related topics and supporting information for this guide.
- List other sources if applicable



## 2. Honeywell Wireless Overview

*(Honeywell is Making Industrial Wireless Real Presentation) (Wireless Infrastructure & Tools System Requirements & Functional Solutions)*

### 2.1 Key Features and benefits

- State of the Art Security System - WPA2, AES-based, Device Authentication
- Reliable Communications – High Speed Mesh, Tolerant Sensor Radio
- Good Power Management – Designed for ~10 Year Sensor Battery Life (Rain or Shine)
- Open – Via PKS Advantage Program
- Multi-speed Monitoring – 1 Second Latency
- Multi-functional – Integrated 802.11 Network for Handhelds & Sensors
- Scalable – Start Small (1 Gateway & 1 Sensor) and Grow
- Global Solution – 2.4 GHz Based
- Quality of Service – Provides Optimized Performance
- Multi-protocol – Universal Wireless – Connects to Any System
- Control Ready – Redundant, Managed Message Routes

### 2.2 About Honeywell Wireless Services

- Provides site assessments and implementation for wireless.

### 2.3 Wireless system overview

- Show complete system with callouts to major components and subsystems (each of which is explained in subsequent sections)

All the devices and infrastructure required to communicate wireless information back to and through a single WSG (inclusive of configuration tools and devices) or WSG redundant pair (*Wireless Infrastructure & Tools System Requirements & Functional Solutions*)

- Wireless sensors and actuators
- Wireless network infrastructure nodes or iNodes
- Wireless system gateways
- Wireless device configuration tools

### 2.4 Wireless components

Describe each component and it's purpose:

- Wireless Configuration Node (Key server, directory server)

## 2. Honeywell Wireless Overview

### 2.5. Wireless Server Tools (software package)

---

- Authentication Device
- OPC Server
- iNode
- WSG node
- Mesh network
- Sensor/actuator nodes
- Wireless Builder for commissioning

## 2.5 Wireless Server Tools (software package)

- XP or 2003 Server PC platform is required to run the software
- Wireless Builder to configure and troubleshoot the devices and gateways
- Key Server and associated UI to commission devices and manage network security
- Directory Server for automatic wireless address assignment
- Network Diagnostic Tool for network troubleshooting and network maintenance (developed by 3eTI)
- OPC Server to provide open access to all device data
- (Tentative) Data Collection Tool and associated UI for maintaining a history of network performance and displaying long-term network statistics

## 2.6 About the Key Server Node

- Importance of maintaining high security for Key Server: Compromise of the Key Server jeopardizes the security of the entire network, it is vital that such scenarios are prevented. The communications to the Key Server must be over a secure channel.
- Availability: System depends on Key Server. The Key Server should be able to handle all requests and should have minimum latency.
- Maintenance: Physical access to the Key Server should be limited and must be secure. See *Wireless System Implementation and Administration Guide* for additional information.

## 2.7 Wireless Installation Overview

(similar to what is in the Getting Started Guide)

- Install and configure Wireless software
- Configure Authentication Device
- Configure mesh network (configure INodes and Wireless System Gateways and authenticate)
- Configure wireless field devices (power up, authenticate)
- Commission wireless devices into Wireless Builder



## **2.8 For more information**

### **Current standards for wireless in automation and control environment.**

- Reference table of resources for wireless implementation in the automation and control environment.

### **About ISA SP-100**

Instrumentation, Systems and Automation Society's (ISA) SP-100 initiative defines a set of standards and recommends best practices for implementing wireless systems in the automation and control environment.

Wireless usage classifications

### **Honeywell references**

- Preparing for Industrial Wireless Whitepaper



## 3. Wireless Site Planning

### 3.1 Site survey tasks

Checklist of items that are usually considered when performing a site survey

### 3.2 Site considerations

- Site environmental considerations
- Throughput considerations
- Coverage area
- Mobility requirements

### 3.3 Radio Frequency Survey

- Required before installation
- Determine area of coverage, line of sight, physical and transient barriers
- Determine antenna and access point selection and location based on application and protocol standard selection
- Determine wired network access and power access requirements for antenna and access points

### 3.4 Hazardous Location requirements

- all electrical equipment installed within a hazardous location must utilize one, or a combination of, the following protection techniques:

- Intrinsic Safety (Division 1 or 2; Zone 0, 1 or 2)
- Explosionproof (Division 1 or 2; Zone 1 or 2)
- Purged and Pressurized (Division 1 or 2; Zone 1 or 2)
- Powder Filled (Zone 1 or 2)
- Oil Immersion (Zone 1 or 2)
- Increased Safety (Zone 1 or 2)
- Encapsulation (Zone 1 or 2)
- Nonincendive / Nonsparking (Division 2; Zone 2)

**Note:** Verify necessity of section. If it is necessary, each wireless device manual also needs to specify any location requirements.

### 3.5 Wireless Device Placement

- Inode (environment, antenna placement, grounding)

### **3. Wireless Site Planning**

#### **3.6. Key Server and Authentication Device**

---

- WSG (environment, antenna placement, grounding)
- Wireless field devices (environment, antenna placement, grounding)

### **3.6 Key Server and Authentication Device**

- Security and location
- Restricting access to the Key Server and the Authentication Device

### **3.7 Wireless installation requirements**

- All wireless devices must be installed by trained personnel (see Hardware Engineering for wording).
- Wireless standards & compliance (references)

## **4. Wireless Network Planning**

### **4.1 Network planning guidelines**

### **4.2 Wireless network architecture topology examples**

*(Wireless Field Trial Presentation)*

- Minimum system
- Maximum system

### **4.3 Wireless network redundancy requirements and implementation**

### **4.4 About the Network Analysis Tool**

- Similar to Ethernet Sniffer, handheld
- Uses and purpose (refer to tool documentation for operating instructions) – checklist of items



## 5. Wireless Security Planning

### 5.1 Security planning checklist

### 5.2 Network protection: protected against deliberate attack or human error by:

- Provable device identity
- Authorization of communications relationships, usually by automatic derivation from configuration database
- Automatic key management
- Inference, logging & reporting of possible attack

### 5.3 Industrial Wireless Security Features

- Authentication device
- Security Keys
- Key Server

### 5.4 About device authentication

- Adding nodes to the wireless network requires device authentication.
- No device that has not been properly authenticated can join the Wireless network.
- Rule applies to all wireless devices, iNodes and gateways

### 5.5 About security keys

- security architecture depends on 3 types of keys
- Bootstrap Key (BK): Initial key used only for deployment, transmitted “in the clear” over short-range medium (IR) – per node
- Key Encryption Key (KEK): Protected key used to identify trusted nodes and for key distribution – per node
- Session Key (SK): Periodically updated key used for normal secure operations - per communicating pair, or per communicating group

### 5.6 About the Key Server

- The Key Server is the center of trust. All nodes trusted by the Key server are also trusted by any other node in the network
- If the key server is compromised then the entire system is compromised

## **5. Wireless Security Planning**

### **5.7. Wireless Security Requirements**

---

## **5.7 Wireless Security Requirements**

- Confidentiality (prevent eavesdropping)
- Integrity (prevent injection of false/tampered data)
- Source authentication (securely identify senders and receivers)
- Replay protection (prevent injection of pre-recorded data)
- Resistance to denial-of-service attacks

## **5.8 Secure Wireless Architecture**

- Topology diagram of secure system

## **5.9 Mitigating wireless security threats**

- Eavesdropping (Initial keys are transmitted out of band. Following keys are encrypted.)
- Spoofing (Authentication device (AD) attests to validity of new device. An authenticated message validates the Key Server.)
- Man-in-the-middle (Authenticated messages – source is known.)
- Subverted manufacturing/distribution (No keys available at manufacturing time, address modification threats by statistical inspection especially for high-security sites).
- Human threat factors (Simple deployment mechanism, automated key updates, high-security sites establish stringent procedures with cross checks, and audit compliance).



## 6. About Wireless Communications

*(Wireless Infrastructure & Tools System Requirements & Functional Solutions)*

### 6.1 Communication for a wireless network infrastructure

- Open system communications supported by the wireless network infrastructure falls into two categories (Communication with control system for data access, Communication with controllers for control)
- Data access applications use OPC for data access.
- Controllers that need wireless data use Modbus.

### 6.2 Industrial Wireless network is developed as a multi-use wireless network.

It allows different types of wireless devices to share the same infrastructure. The system can be used in one of the three modes depending on the installation

- Sensor network mode
- Wireless worker mode
- Mixed mode

### 6.3 Wireless Primary Protocols

- IP addressing with the subnets or IP address ranges set up (large supernetted addresses vs. smaller supernetted addresses vs. Single class "C" subnets) depending on Customer PCN policies.
- Honeywell's Mesh Network is meant to plug-in to some other DCS or application and should follow IP addressing rules of the application (or DCS) Any meaningful DCS policy should work for Honeywell's Mesh Network.

### 6.4 Wi-Fi and Gateway protocols

- CDA (Honeywell proprietary protocol for populating the OPC Server database)
- SNMP
- HTTPS
- Sensor/actuator nodes communicate with iNode using FHSS radio link.

### 6.5 IP addressing iNodes

- Fixed addressing is preferred for the iNodes.
- Need to make sure that the same node always gets the same address whenever it is rebooted.

## 6. About Wireless Communications

### 6.6. Wireless Data Access

---

- During iNode or gateway replacement, the replacement box needs to get the same IP address as the box being replaced.

## 6.6 Wireless Data Access

Wireless sensor data can be accessed for two main purposes – to provide information and to participate in automatic control scheme. Non-EPKS approach to solve these two needs is based on OPC for data access and Modbus for control. While it is possible to use Modbus for data access as well, it is not recommended since only a small subset of wireless data is exposed via Modbus while full access to all device parameters is possible via OPC.

## 6.7 Monitoring Data Access

OPC is de facto standard for SCADA communications. Wireless network relies on OPC to provide open system communication pipe to the wireless sensor data. The concept is illustrated on the following figure:

OPC Server PC also known as Wireless Configuration and OPC Server node is an integral part of the data access solution. OPC Server is collecting wireless device data from gateways using native EPKS CDA protocol. The data is then accessible to any OPC client application via standard OPC DA protocol.

In addition to OPC DA for data access, OPC A&E implementation provides wireless alarms directly to OPC A&E compatible alarm clients. Wireless alarms and events are mapped into OPC without any loss of richness of the device alarming.

Note that OPC server does not reside on the gateway. Current OPC technology makes it virtually impossible to implement it in an embedded environment. Future OPC UA technology may allow moving OPC server function down to the gateway.

## 6.8 Control Data Access

When wireless data is used for control, the open system access protocol of choice is Modbus. Two flavors of Modbus are supported by the wireless gateway – serial and TCP. Serial Modbus protocol is suitable for older controllers while Modbus TCP can be used by new generation of controllers. Modbus server is implemented directly in the wireless gateway as shown on the following figure:

Only a small subset of wireless data is exposed via Modbus protocol. It includes PV of every transducer block with associated PV status and device status bit string. Modbus register mapping is flexible and configurable by the configuration tool.

## **7. Wireless Maintenance Planning**

### **7.1 Pre-configuring local access to field devices for an emergency (**

*Honeywell – Intel Wireless Update Presentation)*

- Purpose of
- Restrictions
- Reference to actual procedure

### **7.2 Device Power Failure Recovery and Authentication - references**

### **7.3 Device Replacement and Authentication - references**

### **7.4 List of references for each of the Wireless components**





**Honeywell**

---

Honeywell International  
Process Solutions  
2500 West Union Hills  
Phoenix, AZ 85027