HONEYWELL DIGITAL PRIME™ TWIN SECURITY

Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

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

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

Honeywell

TABLE OF CONTENTS

PURPOSE OF THE DOCUMENT

1

This document describes the security mechanisms implemented in Honeywell Digital Prime™ Twin offering.

The following are the different security levels implemented across various layers of the architecture:

- **Transport**
- **User access control**
- **Storage**
- **Infrastructure accessibility**

1.1 AUDIENCE OF THE DOCUMENT

This document is intended for customers, architects, and other essential personnel seeking insights into the security controls implemented in this solution.

OVERVIEW

2

2.1 DATA COLLECTION OVERVIEW

Honeywell Digital Prime™ Twin was developed with an awareness of our customers' concerns regarding the collection and visibility of data from the control system. There are two scenarios in Honeywell Digital Prime™ Twin where changes occur in the data collection sets.

Scenario 1
In this scenario, the user is required to share asset configuration, control engineering configuration, displays, server runtime, and non-CEE configuration (e.g., SCADA) that user has configured on Experion and TPS systems deployed in L2 & L3 control systems. However, Honeywell Digital Prime™ Twin does not need to collect any process runtime data, domain configurations, login names or passwords, and MAC addresses.

Scenario 2
In this scenario, the user is required to share the Experion® Server image created using Experion® Backup and Restore (EBR) with Honeywell. As this image is a replica of the entire hard disk of the Experion® server node, it includes user logins and passwords, domain information, MAC addresses, and IP addresses. Additionally, customer user email address information is utilized for authentication and access to sitespecific data. This data, along with the 18-digit Salesforce Account number, is collected during site and user provisioning (see to the Authentication and Authorization section below for more details).

ARCHITECTURE AND DATA FLOW

3

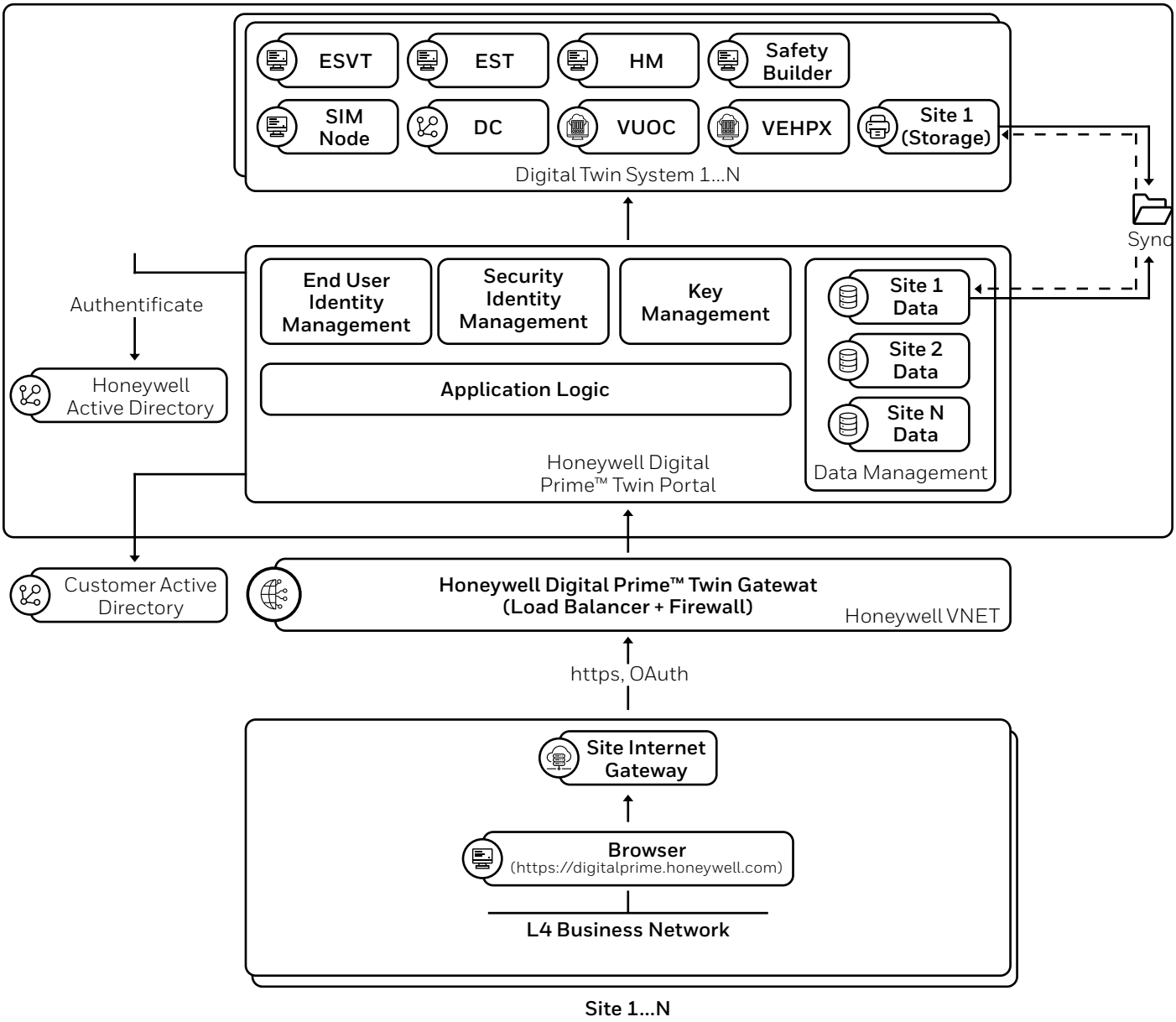
The current software release is constructed on the Microsoft Azure Cloud Platform as the backend infrastructure.

The primary touchpoint between the site and the Cloud is:

- **Honeywell Digital Prime™ Twin web portal:**
  The front end is accessible using secure authentication protocols.
  - Using this user interface, users can upload the Experion® system configuration data.

The diagram below illustrates the overall architecture and data flow mechanism implemented in the Honeywell Digital Prime™ Twin software.

MULTI TENNANT AZURE INFRASTRUCTURE



The table below provides a concise description of the components shown in the diagram

COMPONENT	DESCRIPTION
Honeywell Digital Prime™ Twin Gateway	• Gateway to Honeywell Digital Prime™ Twin Application • It has Firewall and Load Balancer
Honeywell Active Directory	• Honeywell Active Directory is where end-user account information is stored and provides SSO capability
Customer Active Directory	• Customer Active Directory is where end-user account information is stored and provides SSO capability
Data Management	• Secure store for storing data for each site in isolation • Securely manages data management
Honeywell Digital Prime™ Twin System	• Digital Twin system, hosting Experion® Systems • Isolated network of Experion® System, Safety System, and Windows System as Honeywell Digital Prime™ Twin of Plant • Multi-tenancy
Security Identity Management	• Cloud service used to secure all internal communication • Securely authenticates inter-service communication
Key Mgt	• Cloud service to securely store secret keys • Access controlled by a separate set of credentials
End User Identity Mgt	• Used for authentication and authorization of end users
End User UI (User Interface)	• Front end UI visible to external users via browser • Securely communicates with backend services

KEY SECURITY ELEMENTS

4

The Honeywell Digital Prime™ Twin software rigorously enforces "Defense in Depth" security principles to ensure security at each progressive level of connectivity, data flow, storage, access control, infrastructure and accessibility.

Data encryption serves as a comprehensive capability integrated into the software at each point an module across the overall architecture layers.

The security controls built into the software follow stringent Honeywell standards and practices and are reviewed at multiple levels to ensure compliance with Honeywell practices. The subsequent sections in this document describe these controls in more detail.

The security mechanisms implemented can broadly be classified as follows:

- **Encryption:** Encryption is implemented at all levels of the software, right from communication and transport pipelines to storage in the cloud. It is one of the fundamental building blocks of the security architecture to secure data at various levels of transport and storage, as follows:
- **Transport Level:** This refers to all connections established within the software, both within services running in the Cloud as well as between the on-premises data upload agent and the Cloud. The security mechanisms implemented at the transport level ensure that connections are properly authenticated, secure and encrypted.
- **Authentication and Authorization:** Authentication and authorization are implemented at all levels of the software, including end-user access, service access, storage access, and communication. Authenticated and authorized access also ensures that only minimal and required permissions are given to any entity in the software. The Honeywell Forge Identity Management platform is used for customer identity management, and the Honeywell Digital Prime™ Twin software implements a rigorous authorization flow that ensures that end users do not gain access to unauthorized information.
- **Data Backup and Disaster Recovery**
- **Virtual machine security:** Virtual machines hosting the customer data are hosted in Azure. These machines are completely isolated and accessible only to Honeywell Administrators for virtual infrastructure management, and only end-users can login to them using Windows log-in accounts, which are again created and managed by end-users. VMWare's VSAN Encryption provides encryption and key management for virtual machines located in data centers. The embedded Key Management Service stores encryption keys, policies, and configuration for virtual machines with the VSAN Storage policy.
- Rubrik for Backup.
- The isolated network and the outside network can't communicate with the internal VM network, and vice versa, except for the sync service.

DATA ENCRYPTION

5

Data encryption is a critical aspect of security in the overall architecture of the Digital Prime™ Twin solution and is addressed at every communication tier of the software and at the storage level as well.

The subsequent sections of this document address encryption in the context of each specific section and sub-section.

Given the critical nature of this security control, it is worthwhile to call this out specifically. Encryption occurs at two primary levels:

TRANSPORT LEVEL ENCRYPTION:

This refers to data in transit between the site and the cloud, as well as between internal cloud and application services in the Honeywell Private Network. All connections and communication are encrypted using SSL with certificates. All secrets needed for secure communication are securely stored and protected in an Azure Key Vault in the cloud.

STORAGE LEVEL ENCRYPTION:

This refers to data at rest in persistent cloud storage. Persistent storage refers to long-term storage. All storage systems enforce encryption policies as per Honeywell standards.

TRANSPORT LEVEL SECURITY

6

All data in transit is encrypted. This section covers the security mechanisms implemented to secure these layers.

6.1 CLOUD SERVICE CONNECTIVITY

Cloud service connectivity refers to the communication between the application business services and the connections established between them. This includes connections to service endpoints and to message brokers to exchange real-time messages. This section describes the security mechanisms implemented for communication between application services to exchange information and make API calls. The following points are applicable to connections established between services in the cloud:

Digital Prime™ Twin Application is protected within its own isolated network:

- Services are not accessible outside the Honeywell network.
- Special permissions are required, even for administrators, to access services.
- All communication between services takes place within the Honeywell network.

All service communication is secure and encrypted over SSL:

- Service communication is always authenticated using Azure Active Directory.
- Using SSL is mandatory for all communication, otherwise connections are rejected.

Message brokers for service communication are access-controlled and in the Honeywell network:

- Message broker services can be managed only by authorized Honeywell administrators.
- The brokers have robust access controls implemented through Shared Access Signature (SAS) policies.
- SAS policies on message brokers grant only the bare minimum permissions required.

Service communication credentials are securely stored in the Azure Key Vault:

- Connection strings and secrets for communication are kept in the Azure Key Vault.
- Access to the Key Vault is restricted and controlled through Azure AD and certificates.
- Key Vault Access Policies define the bare minimum permissions required.

VM Security

STORAGE LEVEL SECURITY

7

Storage level security refers to the mechanisms used to secure access to site data in the Cloud. All data at rest in the Honeywell Digital Prime™ Twin Cloud is encrypted.

Data storage is physically separated with a separate database for each site:

- Database separation ensures complete data isolation for each site.

Data in Azure storage accounts are always encrypted at rest:

- The Azure platform encryption feature is used to encrypt all storage files at rest.

Data storage on disk at rest is always encrypted and backed up:

- External disks can only be managed by authorized Honeywell administrators.
- All disks are encrypted with Azure Disk Encryption services.

The database is not accessible outside the Honeywell private network in the Cloud:

- Virtual machines are hosted in a secure Honeywell network.
- Databases are configured to have only a private IP address within the internal network, and they do not expose any public IP addresses.
- Access to the database virtual machines requires additional administrator credentials.

7.1 SECURE CONNECTIVITY

All connections established between the Cloud services and storage systems, both persistent and transient, are through encrypted connections over SSL. Storage systems are also tightly controlled, and only authorized administrators and applications have access to the systems. All connections to storage systems are controlled within the Honeywell private network. The following points are applicable to connections established with Cloud storage accounts:

Storage infrastructure is accessible only within the Honeywell network:

- The Honeywell network in the Cloud is a private network with very restricted access.
- Access is restricted to authorized Honeywell administrators logged into the network.
- All Honeywell standard security policies and practices are implemented.
- Only applications deployed in the private network can access storage accounts.
- Restrictions on storage permissions are controlled by the global Honeywell security policy.

Connections to Honeywell Digital Prime™ Twin data are encrypted and access controlled:

- Connections are allowed only over HTTPS and SSL with certificates.
- Only authenticated clients can access the data.
- Separate credentials are required for each site since databases are segregated by site.

AUTHENTICATION AND AUTHORIZATION

8

Authentication, Authorization and Access Control have been noted in the preceding sections in the relevant context.

Considering the critical nature of this security control, it is prudent to identify this in a holistic manner as an overarching capability of the Honeywell Digital Prime™ Twin software. Authentication and access control happen at three levels: end users, application services, and storage services. The following points are applicable to authentication and access control:

End users are authenticated and authorized before being granted access to the application:

- Customers need to have an account in https://process.honeywell.com.
- The Honeywell SSO is being used for end user authentication.
- Role based access control (RBAC) for users is provided to user via Honeywell Forge.
- Access to login and key information is strictly limited to authorized personnel only.
- Rigorous authorization checks are enforced at the application level for data separation.
- Authorization policies ensure that users do not access information meant for other sites.
- Site-level authorization is done at all levels, right from the frontend to backend services.

VIRTUAL MACHINE SECURITY

9

To ensure the protection of VMs and data, below are the security measures.

1. NETWORK ISOLATION AND SEGMENTATION:

- We employ vCloud Director's robust network capabilities to create isolated networks for each customer.
- Strict segmentation is implemented, ensuring that VMs within your network are isolated and not directly accessible by VMs from other customers.

2. ORGANIZATION VIRTUAL DATA CENTER (ORG VDC) ISOLATION:

- Each customer is assigned to a dedicated Org VDC, guaranteeing logical separation of resources.
- Resources allocated to organization are isolated and cannot be accessed by other tenants.

3. ROLE-BASED ACCESS CONTROL (RBAC):

- RBAC is utilized to define roles and permissions within the vCloud Director portal.
- Users are assigned specific roles, restricting their actions to customer VMs and preventing unauthorized access to resources owned by other tenants.

4. FIREWALL RULES AND SECURITY GROUPS:

- We implement stringent firewall rules and security groups to control incoming and outgoing traffic at the network level.
- Specific rules are defined to regulate communication between VMs belonging to different customers, ensuring proper isolation.

5. AUTHENTICATION:

- Strong authentication mechanisms for users accessing the vCloud Director portal.

6. ENCRYPTION AT REST AND IN TRANSIT:

- VM disk encryption is in place to secure data at rest within your VMs.
- Secure communication protocols are employed to encrypt data in transit, ensuring the confidentiality of customer information.

9.1 MALWARE SCAN

All traffic to and from virtual machines undergoes malware scanning. If malware is detected, the file gets removed and won't be available.

To ensure the highest level of cybersecurity and to maintain the integrity of the Honeywell Digital Prime™ Twin system, users are required to install the Antivirus software and updates that are utilized at the site. It is critical that malware signatures are updated promptly whenever updates are provided by the Antivirus software vendor.

This structured procedure not only enhances cybersecurity measures but also guarantees that the Honeywell Digital Prime™ Twin remains identical to the plant system in terms of security and operational integrity.

CAUTION:

Failure to install and update Antivirus software will result in immediate system shutdown to preserve overall security integrity.

COMPLIANCE CERTIFICATIONS AND STANDARDS

10

Compliance certifications and standards refer to a set of guidelines, regulations, or criteria that organizations must adhere to meet specific industry or regulatory requirements.

Standards are established to ensure that businesses operate in a manner that upholds the principles below:

1. NETWORK ISOLATION AND SEGMENTATION:

- We employ vCloud Director's robust network capabilities to create isolated networks for each customer.
- Strict segmentation is implemented, ensuring that VMs within your network are isolated and not directly accessible by VMs from other customers.

2. ORGANIZATION VIRTUAL DATA CENTER (ORG VDC) ISOLATION:

- Each customer is assigned to a dedicated Org VDC, guaranteeing logical separation of resources.
- Resources allocated to the organization are isolated and cannot be accessed by other tenants.

3. ROLE-BASED ACCESS CONTROL (RBAC):

- RBAC is utilized to define roles and permissions within the vCloud Director portal.
- Users are assigned specific roles, restricting their actions to customer VMs and preventing unauthorized access to resources owned by other tenants.

4. FIREWALL RULES AND SECURITY GROUPS:

- We implement stringent firewall rules and security groups to control incoming and outgoing traffic at the network level.
- Specific rules are defined to regulate communication between VMs belonging to different customers, ensuring proper isolation.

5. AUTHENTICATION:

- Strong authentication mechanisms for users accessing the vCloud Director portal.

6. ENCRYPTION AT REST AND IN TRANSIT:

- VM disk encryption is in place to secure data at rest within your VMs.
- Secure communication protocols are used to encrypt data in transit, ensuring the confidentiality of customer data.

You might have concerns about data security, compliance, and control when managing sensitive information in your Azure VMware Solution private cloud. The procedure of encrypting VMware vSAN Key Encryption Keys (KEKs) using customer-managed keys (CMKs) offers notable advantages that align with your specific concerns and preferences. Let's explore these aspects further:

Key aspects of compliance certifications and standards include:

1. DATA SECURITY AND COMPLIANCE:

- Security breaches and data theft incidents have become a significant concern for organizations. Encrypting KEKs with customer-managed keys provides an additional layer of protection for your vSAN data.
- With CMKs managed in your customer-owned Azure Key Vault, you can ensure that your encryption keys are securely stored and managed according to your organization's compliance requirements.

2. CONTROL OVER DATA ACCESS:

- As a potential customer, you desire control over who can access your vSAN keys. The ability to control Azure access to vSAN keys addresses your concern about unauthorized access to sensitive data.
- By using CMKs, you have the power to manage access permissions and restrict Azure from accessing the KEK. This control further enhances the security posture of your VMware Solution private cloud.

3. CENTRALIZED KEY LIFECYCLE MANAGEMENT:

- Managing encryption keys can be challenging, especially in complex environments. With the ability to centrally manage the lifecycle of CMKs, you gain operational efficiency and streamline key management processes.
- By centralizing key lifecycle management, you can easily rotate keys, update permissions, and comply with security best practices without impacting the productivity of your teams.

4. FLEXIBILITY AND VERSATILITY OF KEY TYPES:

- As a potential customer, you want encryption solutions that align with your specific security needs. The support for various key types and sizes, such as RSA and RSA-HSM with key sizes of 2048, 3072, and 4096, offers the flexibility to choose the appropriate encryption method for your workloads.

  This versatility ensures that your VMware Solution private cloud can accommodate diverse encryption requirements, enabling you to protect different types of data effectively.

PASSWORD

11

Here are the definitions for each action in password settings.

Password reset:
It is recommended that, for security purposes, you reset all the passwords with Experion® and Domain Controller to a strong password or passphrase.

Strong Password:
It is recommended to create a strong password or passphrase that includes a combination of uppercase and lowercase letters, numbers, and special characters.

Password renewal:
It is recommended to regularly renew your password and also recommended not to reuse the passwords.

REFERENCE:
Refer to Experion® Password reset procedure and windows password procedure to the same.

POLICIES, AUDITING AND LOGGING

12

Stringent policy enforcement, real-time security audits, security logs, and alerts are important security controls built into the Honeywell Digital Prime™ Twin software.

Policies are set and enforced by authorized security specialists with deep expertise in securing software at both the infrastructure and application levels. Security, audit, and log policies that are set by specialists at the Honeywell subscription level meet stringent Honeywell security standards and override any policies that may be set in specific applications. Policies set and enforced at the subscription level by a limited set of experts ensure that individual application and product teams do not have the authority to modify or dilute these in any way. Honeywell security standards and practices also mandate that any software must go through a rigorous and comprehensive security review and approval process before it can be released into production. These reviews encompass security at the infrastructure level as well as at the application level and go deep into design elements that have the potential to have an impact on security.

Broadly speaking, auditing and logging are done at two primary levels: at the infrastructure and management level and at the application level. Infrastructure and management level auditing primarily focuses on administrative operations, while application level auditing focuses on the operation of individual application services and components. The following points are applicable to auditing and logging:

Infrastructure and management level auditing

- Logs all activities performed by administrators on all infrastructure resources.
- Provides detailed insight into each action and the impact of each action.
- Logs details of users who perform any administrative action on resources.
- Ensures that only authorized administrators can perform management operations.
- Provides a detailed view into potential security violations on a continuous basis.
- Ensures that all resources are compliant with Honeywell standards on an ongoing basis.
- Provides a comprehensive alerting mechanism for timely alerts on potential threats.
- Provides continuous and detailed insight into the runtime operation of all resources.
- Provides comprehensive querying capabilities to quickly identify and fix any issues.
- Ensures that detailed diagnostic information is available to administrators.
- Provides a centralized security recommendation center for proactive action.
- Implements robust troubleshooting procedures in the event of transient failures.
- Implements resource health monitoring capabilities to enable proactive action.
- Provides highly granular metrics and analytics related to security and system health.
- Provides comprehensive dashboards to administrators to monitor security and health.

Application level logging

- Complements the infrastructure auditing capabilities described above.
- Provides granular logging at the individual application component level.
- Provides well segregated insight into the internal working of components.
- Integrated with infrastructure auditing capabilities to provide a unified view.
- Provides detailed insight into internal faults, errors, and warnings.
- Provides traceability by providing informational logs during operation.

CONCLUSION

13

This document has provided a detailed overview of the comprehensive controls implemented in the Honeywell Digital Prime™ Twin software. The security features built into the software are compliant with standard industry best practices and benchmarks, in addition to being compliant with rigorous standards set by Honeywell. The document is intended to serve as a white paper for parties interested in understanding specific security controls built into Honeywell's Honeywell Digital Prime™ Twin software.

NOTICES

14

14.1 OTHER TRADEMARKS

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

14.2 THIRD-PARTY LICENSES

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third_party_ licenses on the media containing the product.

14.3 DOCUMENTATION FEEDBACK

You can find the most up-to-date documents on the Honeywell Process Solutions support website at: *http://www.honeywellprocess.com/support*

If you have comments about Honeywell Process Solutions documentation, send your feedback via mail to: *hpsdocs@honeywell.com*

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell Technical Assistance Center (TAC).

14.4 HOW TO REPORT A SECURITY VULNERABILITY

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at: *https://honeywell.com/pages/vulnerabilityreporting.aspx*

14.5 SUPPORT

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, *https://www.honeywellprocess.com/en-US/contact-us/customer-supportcontacts/ Pages/default.aspx.*

14.6 TRAINING CLASSES

Honeywell holds technical training classes that are taught by process control systems experts. For more information about these classes, contact your Honeywell representative, or see *https://process.honeywell.com/us/en/services/training*.

Honeywell Process Solutions
2101 City West Blvd, Houston, TX 77042

Honeywell House, Skimped Hill Lane
Bracknell, Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road,
Zhangjiang Hi-Tech Industrial Park,
Pudong New Area, Shanghai 201203

process.honeywell.com

WPR | 441DPH | 09/25

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell