CYBER SECURITY FOR GAS MEASURING DEVICES

PRODUCT MANAGEMENT
VERSION 03

Honeywell

PRESENTATION OVERVIEW

1. **Cyber security by Design**

   Honeywell's standard procedures for developing secure products

2. **Implemented security measures**

   Examples

3. **In preparation**

   Component certification according to IEC 62443-4-2 for Gas measurement devices

4. **Example for implementing national security requirements**

   TSA directive (USA)

CYBER SECURITY BY DESIGN

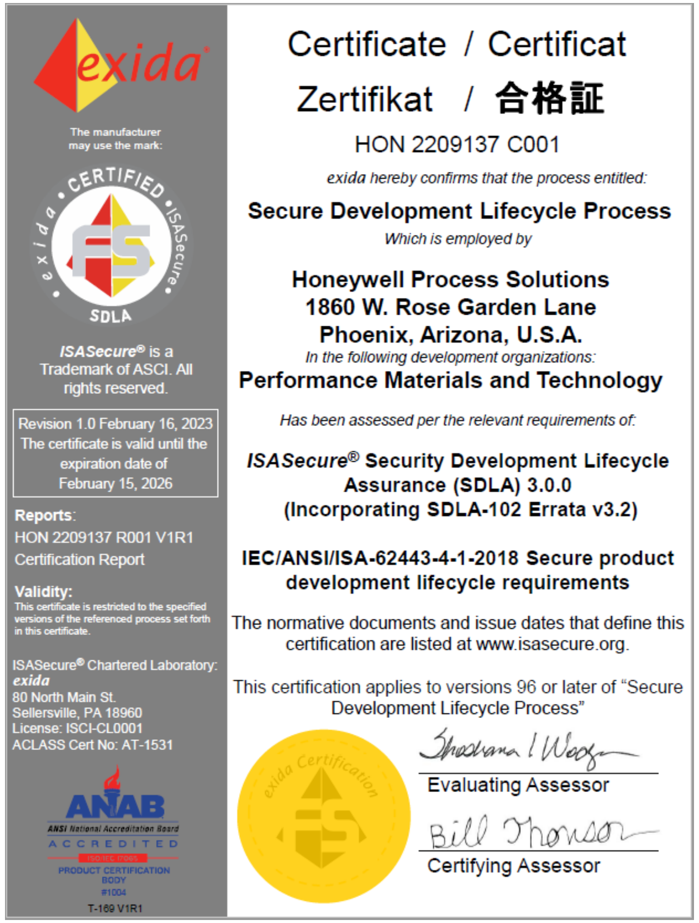
Honeywell's standard procedures for developing secure products

SECURE DEVELOPMENT LIFECYCLE PROCESS

- The Honeywell Process Solution (HPS) Product Security Center of Excellence (CoE) has implemented a Secure Development Life Cycle (SDLC) for all products being developed.
- Aim is to ensure that security is built into HPS systems and not included as an afterthought - security mechanisms and controls are treated the same way as other development items.

SDLC – COMPLIANT TO IEC 62443-4-1

- Honeywell Process Solution (HPS) has achieved a SDLA Certification[1)] for the standard development process that certifies compliance to IEC 62443 Part 4-1: Secure product development lifecycle requirements.
- In addition, HPS uses BSIMM (Building Security In Maturity Model) as an additional framework for security improvement and organizational capability measurement
- The European Union’s General Data Protection Regulation (GDPR) is also supported.



exida

The manufacturer may use the mark:

CERTIFIED • ISASecure • exida •
SDLA

ISASecure® is a Trademark of ASCI. All rights reserved.

Revision 1.0 February 16, 2023
The certificate is valid until the expiration date of February 15, 2026

Reports:
HON 2209137 R001 V1R1
Certification Report

Validity:
This certificate is restricted to the specified versions of the referenced process set forth in this certificate.

ISASecure® Chartered Laboratory:
exida
80 North Main St.
Sellersville, PA 18960
License: ISCI-CL0001
ACLASS Cert No: AT-1531

ANAB
ANSI National Accreditation Board
ACCREDITED
ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004

T-169 V1R1

Certificate / Certificat
Zertifikat / 合格証

HON 2209137 C001

exida hereby confirms that the process entitled:

Secure Development Lifecycle Process

Which is employed by

Honeywell Process Solutions
1860 W. Rose Garden Lane
Phoenix, Arizona, U.S.A.

In the following development organizations:

Performance Materials and Technology

Has been assessed per the relevant requirements of:

ISASecure® **Security Development Lifecycle Assurance (SDLA) 3.0.0**
(Incorporating SDLA-102 Errata v3.2)

IEC/ANSI/ISA-62443-4-1-2018 Secure product development lifecycle requirements

The normative documents and issue dates that define this certification are listed at www.isasecure.org.

This certification applies to versions 96 or later of “Secure Development Lifecycle Process”

Evaluating Assessor

Bill Thomson
Certifying Assessor

1) https://www.isasecure.org/en-US/End-Users/IEC-62443-4-1-Certified-Development-Organizations
2) A study of current software security initiatives or programs of different organizations across industries, sizes, and geographies.
3) GDPR website

SDLC – WORK PERFORMED BY LIFECYLE PHASE

- Inception: During establishing the scope of the project, security requirements are identified and are added to the project's Requirement Repository.
- Elaboration: Primary objectives are to mitigate critical technical risks and to develop an executable architecture.
- Construction: Design and implementation may identify assets to be added to the Threat Model.
- Transition: Product packages and components are signed using a certificate to ensure that the end user can verify the integrity and authenticity of the product.
- Any Time (lifecycle phase independent): At any time, when an anomaly is fixed, it is determined if the fix could affect the security of the product. If so, the anomaly and its fix is analyzed to determine how to address any security issues.

SDLC – SECURITY ROLES

- Security Architect (Project role): Guide the team on architectural requirements from a security standpoint as well as provide design guidance based on a good working knowledge of cyber-security.
- Security Tester (Project role): Have an understanding of cyber security attacks and special training on using security testing tools.
- Master Security Architect (Organizational role): They are responsible for providing consulting and mentoring to Security Architects; providing final approval on threat models; and determining resolutions for unmitigated security issues encountered by the Security architect.
- Master Security Tester (Organizational role): Responsible for providing consulting and mentoring to Security Testers and providing guidance on Security testing tools.

SDLC – KEY WORK PRODUCTS

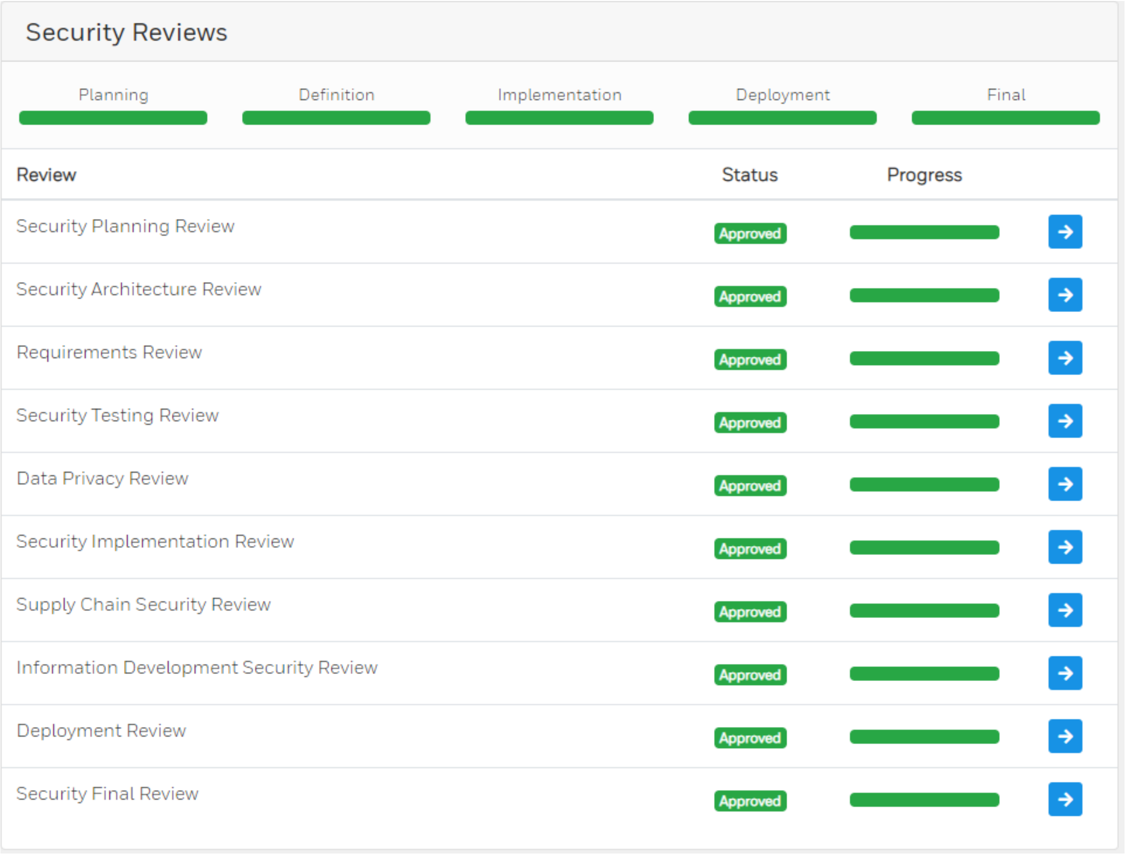
- Requirements Repository: Security Requirements and Non-Functional Requirements that are based on Master Security Requirements (MSR). The security requirements relevant for the project are selected and added to the project’s requirement repository.
- Software Architecture Document: Includes information about how the system is architected to fulfill a set of Architecturally Significant Requirements which may include security requirements that need special handling in the architecture.
- Threat Model: Security map of the level of risk in the application
  - Security assets: Defining the location of potential attacks
  - Threats: Information on how the system might be misused
  - Controls: Mechanisms to mitigate the possible threats; additional requirements or architecture and design elements to be implemented and tested as part of standard product development.

SDLC – KEY WORK PRODUCTS

- Static Code Analysis Reports: Used to mitigate implementation-level security risks. They are created and analyzed for each system build.
- Test Plan - Security Verification Testing: Includes a section on Security Verification Testing which includes a list of test targets and security verification test types (e.g., Penetration Testing) that are planned to be performed in each iteration.
- Security Test Evaluation Summary: Describes the results of the security tests.
- Security Documentation Checklist: When writing user documentation, a security checklist is used to ensure that appropriate security information is included for each of the information types that make up the User Assistance deliverables.
- Change Request: Impact Analysis of a change request identifies whether security is impacted either by the change requested or by the fix.

SDLC – SECURITY FINAL REVIEW & CTO SIGNOFF

- After the individual security reviews, a final review is conducted and submitted to the CTO for approval.
- All products and service offerings containing software or firmware must obtain cybersecurity approval of the CTO prior to being placed into production of offered for customer use.



Security Reviews

Planning	Definition	Implementation	Deployment	Final
🟩	🟩	🟩	🟩	🟩

Review	Status	Progress	
Security Planning Review	Approved	🟩	→
Security Architecture Review	Approved	🟩	→
Requirements Review	Approved	🟩	→
Security Testing Review	Approved	🟩	→
Data Privacy Review	Approved	🟩	→
Security Implementation Review	Approved	🟩	→
Supply Chain Security Review	Approved	🟩	→
Information Development Security Review	Approved	🟩	→
Deployment Review	Approved	🟩	→
Security Final Review	Approved	🟩	→

A product cannot be launched without final CTO Signoff

SECURITY OF THIRD-PARTY COMPONENTS

- Honeywell ensures that the product development life-cycle processes for components from a third-party supplier conform to the SDLA security requirements when developed specifically for Honeywell or have an impact on security or require ISA Secure certification.
- The Security architect must verify that suppliers meet the same SDLC levels as HPS prior to engaging them in a development effort based on the criteria above.

VULNERABILITY MANAGEMENT

- Cyber security vulnerabilities are reported to the HPS Product Security Group through two primary methods: internal disclosure and external disclosure.
  - Internal discovery of cyber security vulnerabilities is typically triggered by: Security Assessments or security testing, Threat Models, Static Code Analysis and code reviews or Design or Architectural Reviews
  - External discovery of cyber security vulnerabilities is typically triggered by: Black hat or white hat security researchers, Hackers, Customers, Media coverage
- Vulnerabilities are managed via defect reports which are logged into Honeywell's defect management systems and prioritized to identify the release in which a resolution or fix will be available.

IMPLEMENTED SECURITY MEASURES

Examples

COMPLEX PASSWORDS + LOGIN ATTEMPTS

- Security gap : Short (up to 5 digits long) and simple (numeric) PINs were often implemented in gas measurement devices. These do not sufficiently protect the device from unauthorized access.
- Solution: In addition to requiring long (usually greater than 8 characters) and complex (alphanumeric + special characters) passwords (or secrets), the number of failed authentication attempts for a subscriber's account needs to be limited.
- Example: Secrets according to NIST SP 800-63B - Authentication and Lifecycle Management

Ensure that someone is who they say they are before granting access

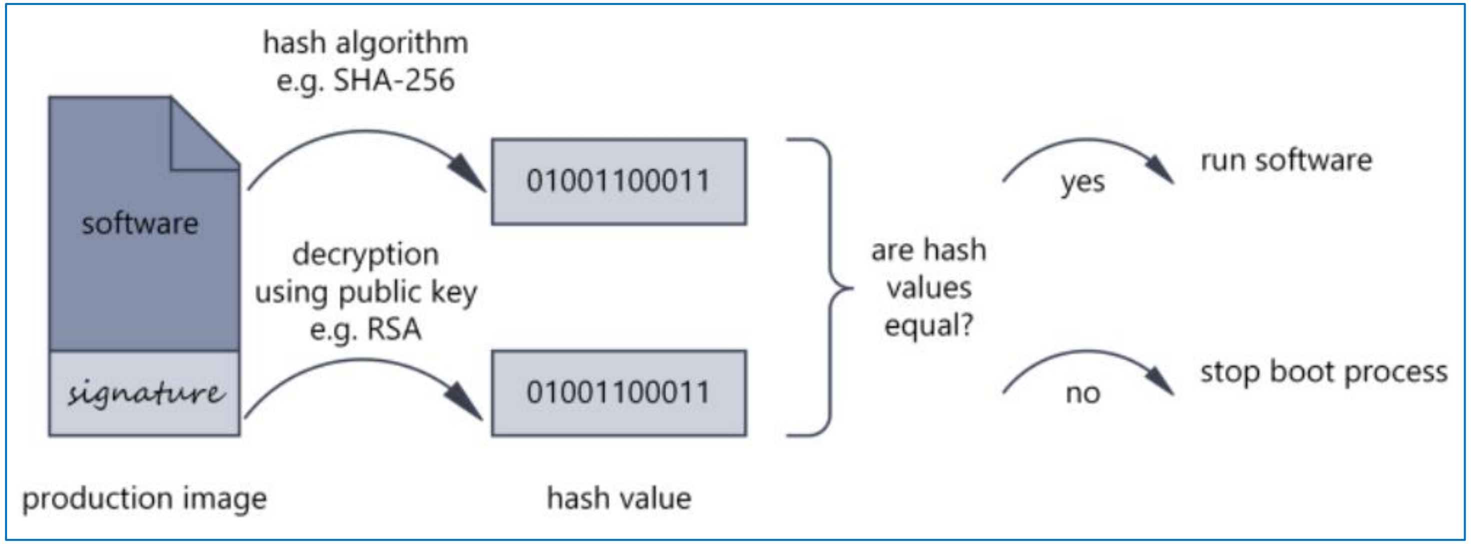
ENCRYPTED DATA COMMUNICATION

- Security gap: Data including access information such as device passwords, PIN for SIM cards, etc. are transmitted as plain text and can be both eavesdropped and manipulated without the user being able to detect this.
- Solution: Encrypted data transmission ensures that no third party can eavesdrop or tamper with any message
- Example: Transport Layer Security (TLS).
  A cryptographic protocol for encrypted data transmission providing privacy (confidentiality), integrity and authenticity using certificates between two or more communication partners.

Protect data from eavesdropping and tampering

SECURE BOOT

- Security gap: Remote update functions allow devices to be kept up to date without the need for a visit to the station. But how do you guarantee that a device is only using firmware that is intended for it and has not been tampered with?
- Solution: Firmware authenticity verification mechanism using a cryptographic algorithm.



Ensure that the device only starts firmware that is trusted

IN PREPARATION

Component certification according to
IEC 62443-4-2 for Gas measurement devices

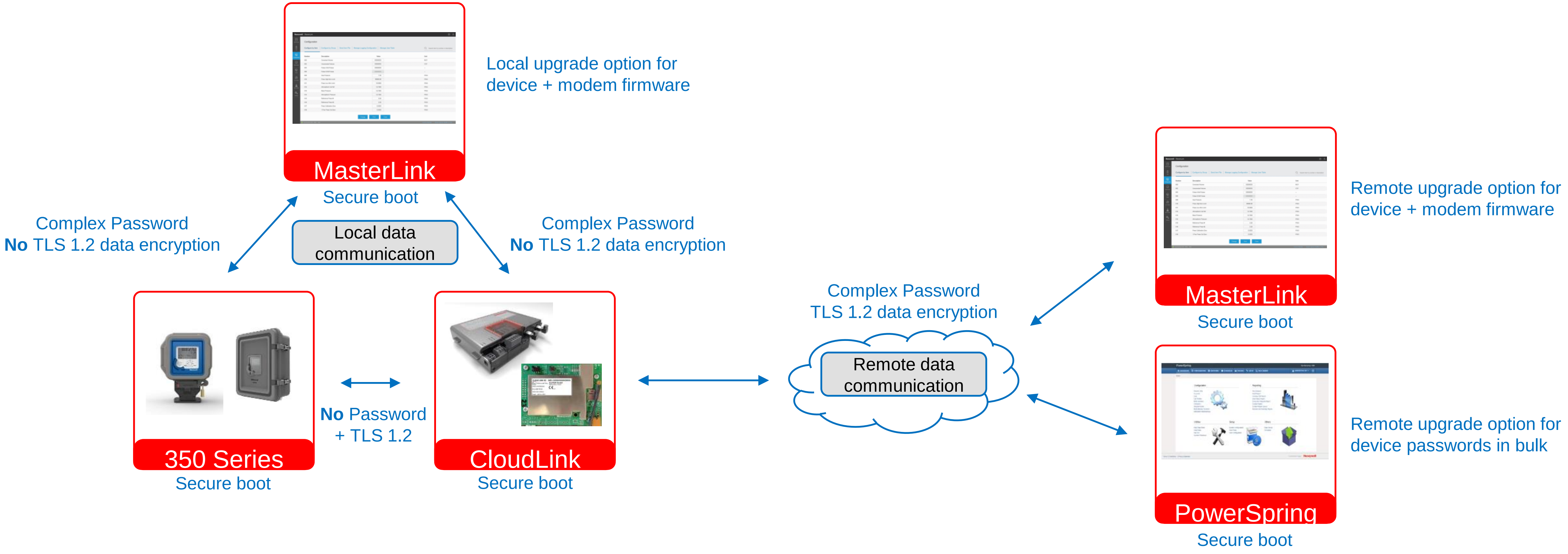
COMPONENT CERTIFICATION ACC. IEC 62443

- More and more customers and authorities are asking for secure measurement devices, but without providing an exact definition or naming a standard.
- Therefore, it is difficult for us as a manufacturer to specify the required measures and for the user to assess the implemented level of security.
- We decided to achieve a to achieve a component certification according to IEC 62443-4-2 (secure industrial automation and control systems) for the Honeywell Gas measurement products.

EXAMPLE FOR IMPLEMENTING NATIONAL SECURITY REQUIREMENTS

TSA directive (USA)

TSA COMPLIANT ECOSYSTEM



MasterLink

Secure boot

Local upgrade option for device + modem firmware

Complex Password
No TLS 1.2 data encryption

Local data communication

Complex Password
No TLS 1.2 data encryption

350 Series

Secure boot

No Password
+ TLS 1.2

CloudLink

Secure boot

Complex Password
TLS 1.2 data encryption

Remote data communication

MasterLink

Secure boot

Remote upgrade option for device + modem firmware

PowerSpring

Secure boot

Remote upgrade option for device passwords in bulk

Complex password:

- Hash passwords are stored and exchanged between devices and PC software independent from the used password complexity (also for current PINs).
- Password verification is done in the encrypted format.

TLS 1.2 data encryption:

- Use is not mandatory (switched on/off)

FEATURES PER PRODUCT

Feature	CloudLink 100	CloudLink 110	CloudLink 5G	350 series	MasterLink	PowerSpring
Complex Password	Yes	Yes	Yes	Yes	Yes	Yes
Secure Boot	Yes	Yes	Yes	Yes	Yes	Yes
TLS 1.2 Server[1)]	No	No	Yes	NA	NA	Yes
TLS 1.2 Client[2)]	No	No	Yes	NA	Yes	Yes

[1)] TLS Server: TLS server will validate the incoming connection by verifying certification used by the TLS client.

[2)] TLS Client: TLS client will go and connect to TLS server; TLS client will share the supported TLS encryption algorithm to TLS server.

COMPLEX PASSWORD

Guideline for creating complex password

- Minimum 8 characters length
- Maximum 15 characters length
- At least one special character
- At least one numeric
- At least one capital letter

Password throttling (already in place in EC350)

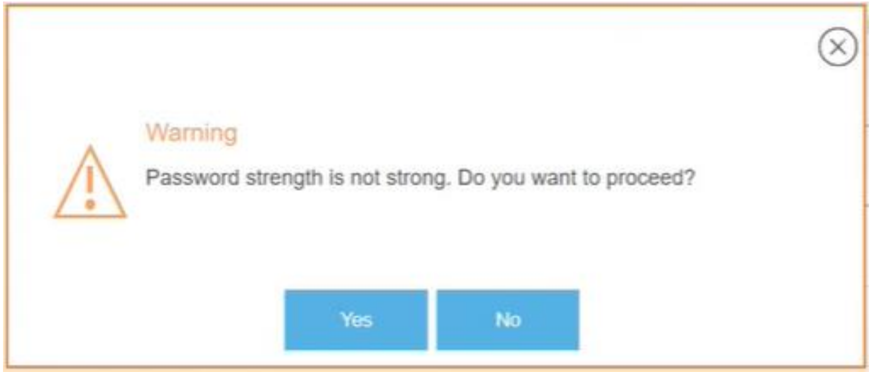
- After entering an incorrect password three times continuously, the user must wait 3 minutes before entering the password again.
- After entering an incorrect password three more times, the user must wait 5 minutes. This goes until 25 minutes and the user will be locked.
- In this case, the Admin must generate a new password for the user to login again.

Secure operation due to Complex password & exponential lockup feature

COMPLEX PASSWORD

Using complex passwords

- Initial login is done with default password (numeric).
- User should change the simple password to a complex password.
- Also, the User IDs should be adjusted.
- The user receives a message in MasterLink if the selected password does not meet the NIST requirements.



Warning

Password strength is not strong. Do you want to proceed?

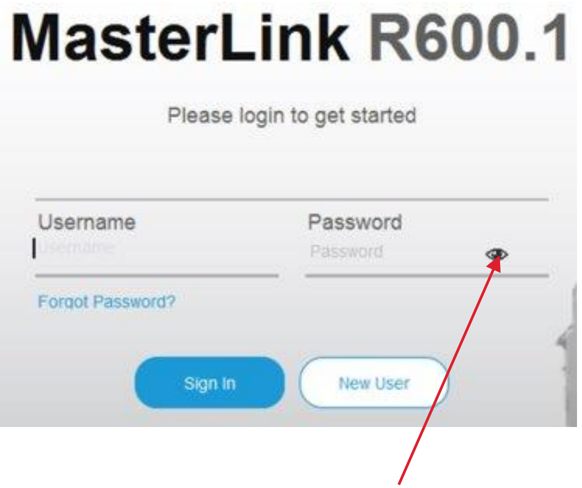
Technical details

- Hash password is calculated using SHA256 encryption method
- Nowhere in the system is the plain password stored.
- Verification is done in the encrypted format.

Use of complex passwords is the responsibility of the customer

COMPLEX PASSWORD

‚Show password‘ function available



MasterLink R600.1

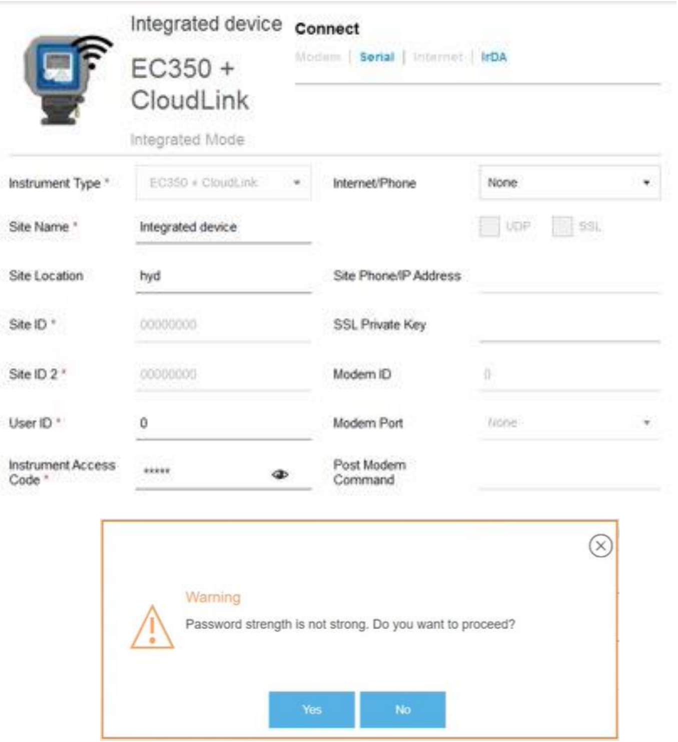
Please login to get started

Username	Password
Username	Password

Forgot Password?

Show Password

Hint if PW is to be saved with insufficient complexity



Integrated device

EC350 + CloudLink

Integrated Mode

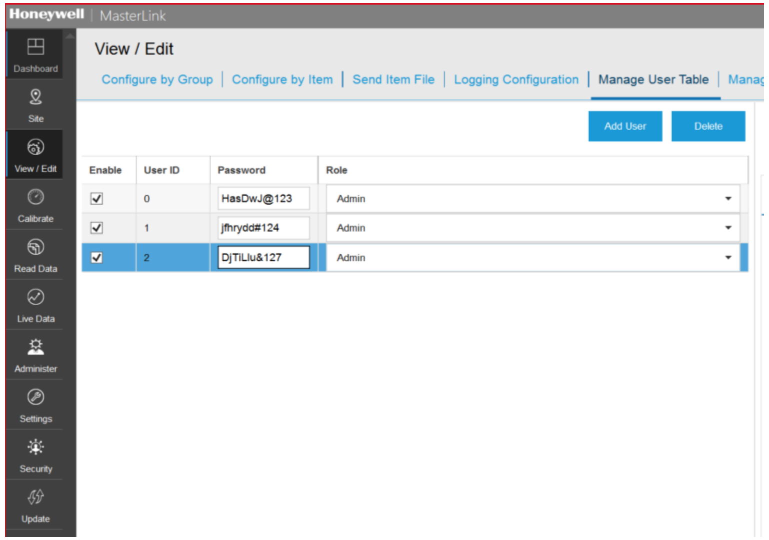
Connect

Instrument Type *	EC350 + CloudLink	Internet/Phone	None
Site Name *	Integrated device		□ UDP □ SSL
Site Location	hyd	Site Phone/IP Address	
Site ID *	00000000	SSL Private Key	
Site ID 2 *	00000000	Modem ID	0
User ID *	0	Modem Port	None
Instrument Access Code *	*****	Post Modem Command	

Warning

Password strength is not strong. Do you want to proceed?

User table with complex passwords



View / Edit

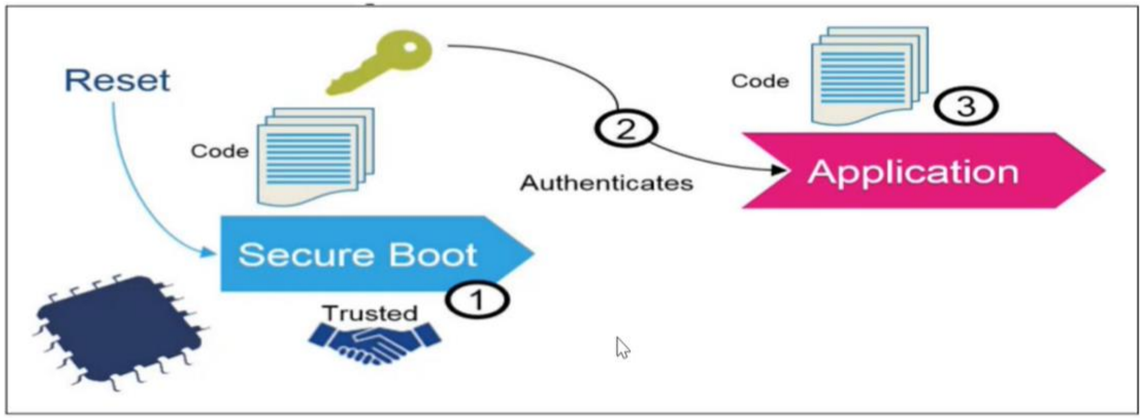
Configure by Group | Configure by Item | Send Item File | Logging Configuration | Manage User Table | Manag
Add User
Delete

Enable	User ID	Password	Role
☑	0	HasDwJ@123	Admin
☑	1	jfhrydd#124	Admin
☑	2	DjTiLlu&127	Admin

Entering has not changed, but system hint if complexity is not sufficient

SECURE BOOT

1. On each Power-On, the Secure Boot Loader will take control of the MCU to ensure that the current running application is not compromised (Corrupted FW, Incorrect application).
2. Boot loader authenticates current running application by calculating the hash of application and compared to stored hash in memory.
3. If Authentication is successful, then only control is passed from Boot Loader to Application for execution.



THANK YOU

Honeywell