CYBER SECURITY FÜR GASMESSGERÄTE

PRODUKTMANAGEMENT
VERSION 04

Honeywell

AGENDA

1. **Cyber Security by Design**
   Honeywells zertifizierter Prozess für die Entwicklung sicherer Produkte

2. **Was bedeutet das für den Anwender?**
   Beispiele für Sicherheitsmaßnahmen
   Umgesetzte Maßnahmen in enCore-Geräten

3. **In Vorbereitung**
   Komponenten-Zertifizierung nach IEC 62443-4-2

CYBER SECURITY BY DESIGN

Honeywells zertifizierter Prozess für die Entwicklung sicherer Produkte

Honeywell

SECURITY DEVELOPMENT LIFECYCLE (SDLC)

- Honeywell Process Solution (HPS) hat für die Produktentwicklung einen sog. „Security Development Life Cycle“ (SDLC) eingeführt.
- Damit wird gewährleistet, dass Sicherheits-aspekte von Anfang an in die Entwicklung integriert und nicht erst nachträglich berücksichtigt werden – Sicherheitsmechanismen und -kontrollen werden im Entwicklungsprozess genauso behandelt wie andere Elemente.

SDLC – KONFORM MIT IEC 62443-4-1

- Honeywell Process Solution (HPS) hat eine SDLA-Zertifizierung[1)] für den Standardentwicklungsprozess erhalten, die die Einhaltung der Anforderungen der IEC 62443 Teil 4-1: ‚Secure Product Development Lifecycle‘ bescheinigt.
- Darüber HPS BSIMM (Building Security In Maturity Model) als zusätzlichen Rahmen für die Verbesserung der Sicherheit und die Messung der organisatorischen Fähigkeiten verwendet.
- Die General Data Protection Regulation (GDPR) der Europäischen Union wird ebenfalls unterstützt.


exida

The manufacturer may use the mark:

exida CERTIFIED ISASecure 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
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”

exida Certification

Evaluating Assessor

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 – AKTIVITÄTEN IM ENTWICKLUNGSPROZESS

- Konzept: Während der Festlegung des Projektumfangs werden die Sicherheitsanforderungen ermittelt und in die Anforderungen des Projekts aufgenommen.
- Entwurf: Hauptziele sind die Minimierung kritischer technischer Risiken und die Entwicklung einer geeigneten Architektur.
- Konstruktion: Beim Entwurf und bei der Implementierung werden möglicherweise Maßnahmen ermittelt, die dem Bedrohungsmodell hinzugefügt werden müssen.
- Einführung: Produktpakete und Komponenten werden mit einem Zertifikat signiert, um sicherzustellen, dass der Endbenutzer die Integrität und Authentizität des Produkts überprüfen kann.

SDLC – AKTIVITÄTEN WÄHREND DER LEBENSZEIT

- Wird eine Produktanomalie behoben, erfolgt zu jedem Zeitpunkt eine Überprüfung, ob die Behebung die Sicherheit des Produkts beeinträchtigen könnte.
- Ist dies der Fall, werden die Anomalie und ihre Behebung analysiert, um festzulegen, wie etwaige Sicherheitsprobleme zu behandeln sind.

SDLC – ROLLEN IM ENTWICKLUNGSPROZESS

- Security Architect (Projektrolle): Er leitet das Team bei der Festlegung der Architekturanforderungen unter Sicherheitsaspekten an und stellt auf der Grundlage der Cybersicherheit Leitlinien für den Entwurf bereit.
- Security Tester (Projektrolle): Besitzt hohes Verständnis von potenziellen Cybersicherheitsangriffen und eine spezielle Ausbildung in der Verwendung von Sicherheitstools.
- Master Security Architect (Organisatorische Rolle): Ist verantwortlich für die Beratung und Betreuung des Security Architects, für die endgültige Genehmigung von Bedrohungsanalysen und für die Festlegung von Lösungen für nicht behobene Sicherheitsprobleme, auf die der Sicherheitsarchitekt stößt.
- Master Security Tester (Organisatorische Rolle): Verantwortlich für die Beratung und Betreuung von Security-Testern und -Testtools.

SDLC – PRODUKTE IM ENTWICKLUNGSPROZESS

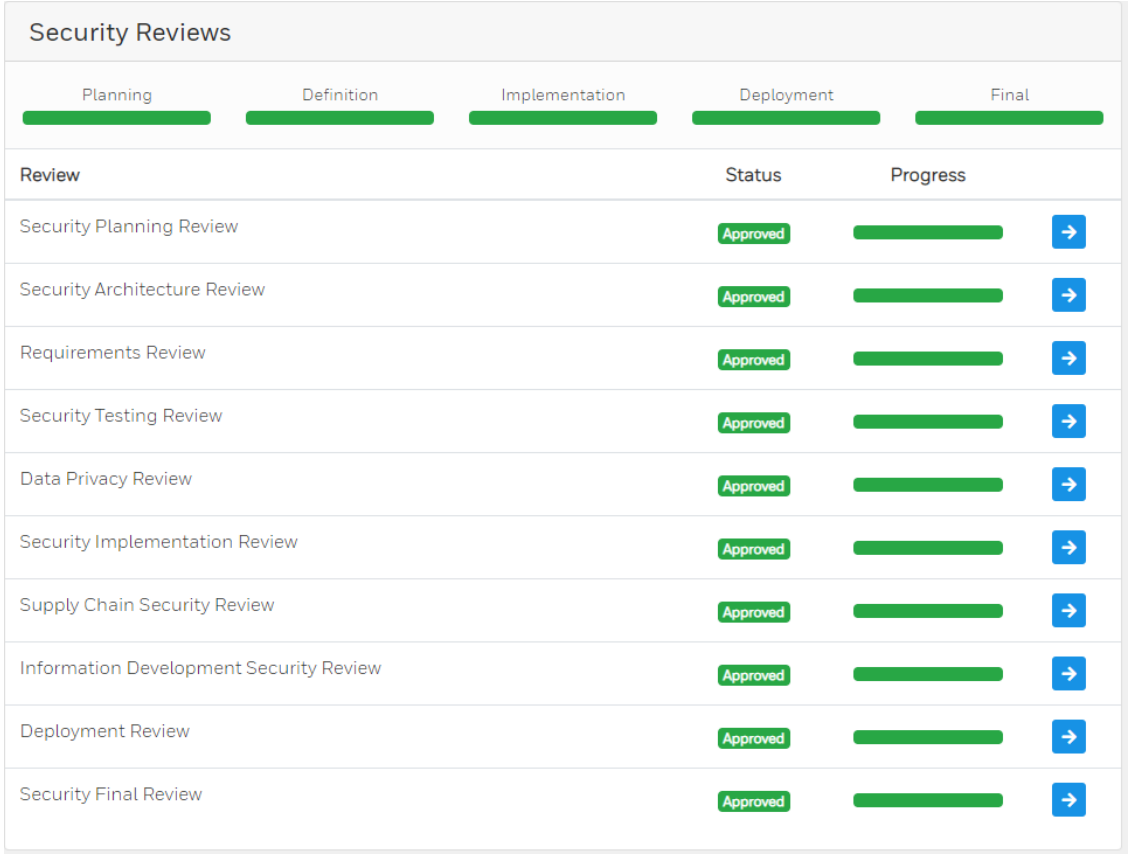
- Anforderungs-Repository: Sammlung von Sicherheitsanforderungen und nicht-funktionale Anforderungen, die auf den Master Security Requirements (MSR) basieren. Die für das Projekt relevanten Sicherheitsanforderungen werden ausgewählt und in das Anforderungs-Repository des Projekts aufgenommen.
- Softwarearchitektur-Dokument: Enthält Informationen darüber, wie die Systemarchitektur aufgebaut ist, um Sicherheitsanforderungen zu erfüllen, die in der Architektur besonders behandelt werden müssen.
- Bedrohungsmodell: Analyse und Bewertung des Risikoniveaus der Anwendung
  - Schwachstellen: Definition der potenziellen Angriffspunkte.
  - Bedrohungen: Identifikation, wie das System missbraucht werden könnte.
  - Maßnahmen: Mechanismen zur Risikominimierung der möglichen Bedrohungen; zusätzliche Anforderungen oder Architekturelemente, die implementiert und getestet werden müssen.

SDLC – WICHTIGE ARBEITSPRODUKTE

- Bericht der statischen Codeanalyse: Statische Codeanalysen werden verwendet, um Sicherheitsrisiken auf Implementierungsebene zu vermindern. Sie werden für jeden Systemaufbau erstellt und analysiert.
- Testplan für Sicherheitstests: Enthält eine Liste der Testziele und der Arten von Sicherheitstests (z.B. Penetrationstests), die in jeder Iteration durchgeführt werden.
- Zusammenfassung der Sicherheitstests: Beschreibt die Ergebnisse der Sicherheitstests.
- Checkliste für Dokumentation: Bei der Erstellung der Benutzerdokumentation wird eine Sicherheitscheckliste verwendet, um zu gewährleisten, dass die erforderlichen Sicherheitsinformationen für den Anwender enthalten sind.

SDLC – ABSCHLUSS & CTO-ABNAHME

- Nach den einzelnen Prozessschritten wird eine abschließende Überprüfung durchgeführt und dem CTO (Chief Technology Officer) zur Genehmigung vorgelegt.
- Alle Produkte, die Software oder Firmware enthalten, müssen vom CTO im Hinblick auf die Cyber-sicherheit genehmigt werden, bevor sie in die Serienproduktion gehen.



Keine Produkteinführung ohne die Freigabe durch den CTO

KOMPONENTEN VON LIEFERANTEN

- Honeywell stellt sicher, dass die Produktentwicklungsprozesse für Komponenten, die speziell für Honeywell entwickelt werden, Auswirkungen auf die Sicherheit haben oder eine ISA Secure-Zertifizierung erfordern, ebenfalls die SDLA-Sicherheitsanforderungen erfüllen.
- Der Sicherheitsarchitekt muss sich vergewissern, dass die Lieferanten die gleichen SDLC-Stufen wie HPS erfüllen, bevor er sie auf der Grundlage der oben genannten Kriterien mit der Entwicklung beauftragt.

SCHWACHSTELLEN-MANAGEMENT

- Cybersicherheitsschwachstellen werden der HPS-Produktsicherheitsgruppe über zwei Hauptmethoden gemeldet: interne und externe Mitteilungen.
  - Die interne Aufdeckung von Cybersicherheitsschwachstellen wird in der Regel ausgelöst durch: Sicherheitsbewertungen oder Sicherheitstests, Bedrohungsmodelle, statische Code-Analysen und Code-Reviews oder Design- oder Architektur-Reviews.
  - Die externe Aufdeckung von Sicherheitslücken erfolgt in der Regel durch: Black Hat oder White Hat Hacker, Kunden, Sicherheitsorganisationen (z.B. NIST, BSI).
- Schwachstellen werden über Fehlerberichte verwaltet, die im Honeywell Fehlerverwaltungssystemen erfasst und nach Prioritäten geordnet werden, um die Version zu ermitteln, in der eine Lösung oder Behebung verfügbar sein wird.

WAS BEDEUTET DAS FÜR DEN ANWENDER?

Beispiele für Sicherheitsmaßnahmen

Umgesetzte Maßnahmen in enCore-Geräten

Honeywell

KOMPLEXE PASSWÖRTER + ANMELDEVERSUCHE

- Sicherheitslücke: Kurze (bis zu 5 Ziffern lange) und einfache (numerische) PINs wurden oft in Gasmessgeräten implementiert. Diese schützen das Gerät nicht ausreichend vor unberechtigtem Zugriff.
- Abhilfe: Neben der Forderung nach langen (in der Regel mehr als 8 Zeichen) und komplexen (alphanumerische + Sonderzeichen) Passwörtern (oder Geheimnissen) muss die Anzahl der fehlgeschlagenen Authentifizierungs-versuche für das Konto eines Teilnehmers begrenzt werden.
- Beispiel: Geheimnisse gemäß NIST SP 800-63B - Authentifizierung und Lifecycle Management

Sicherstellen, dass eine Person diejenige ist, die sie vorgibt zu sein

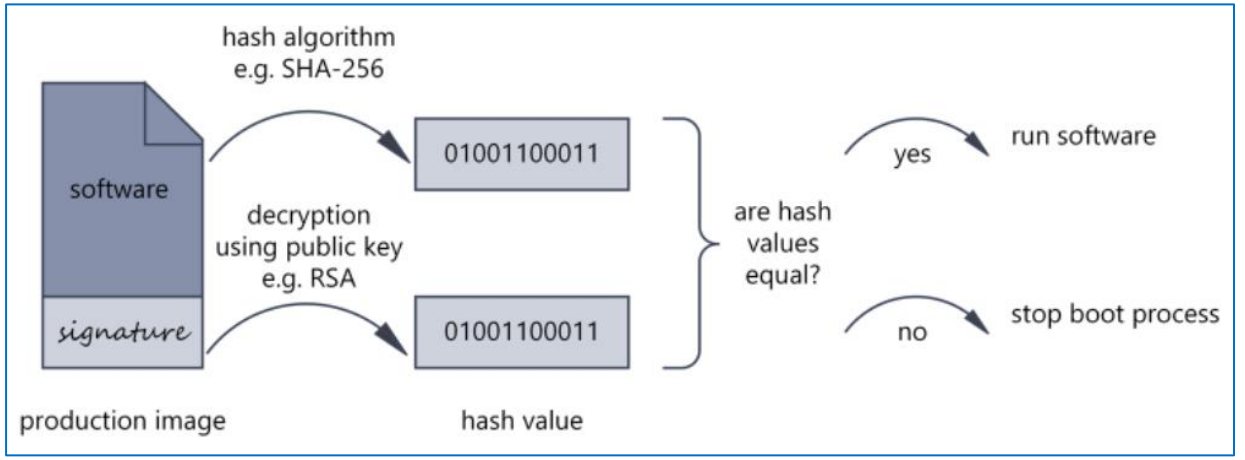
VERSCHLÜSSELTE DATENKOMMUNIKATION

- Sicherheitslücke: Daten einschließlich Zugangsinformationen wie Gerätepasswörter, PIN für SIM-Karten usw. werden im Klartext übertragen und können sowohl abgehört als auch manipuliert werden, ohne dass der Nutzer dies erkennen kann.
- Abhilfe: Verschlüsselte Datenübertragung stellt sicher, dass kein Dritter eine Nachricht abhören oder manipulieren kann
- Beispiel: Transport Layer Security (TLS). Ein kryptografisches Protokoll zur verschlüsselten Datenübertragung, das die Vertraulichkeit, Integrität und Authentizität mit Hilfe von Zertifikaten zwischen zwei oder mehreren Kommunikationspartnern gewährleistet.

Schutz der Daten vor Abhören und Manipulation

SECURE BOOT

- Sicherheitslücke: Mit Hilfe von Fernaktualisierungsfunktionen können die Geräte auf dem neuesten Stand gehalten werden, ohne dass ein Einsatz in der Station erforderlich ist. Aber wie wird sichergestellt, dass ein Gerät nur die vorgesehene Firmware verwendet und diese nicht manipuliert wurde?
- Abhilfe: Mechanismus zur Überprüfung der Authentizität der Firmware mit Hilfe eines kryptografischen Algorithmus.



Sicherstellen, dass das Gerät nur Firmware startet, die vertrauenswürdig ist

SICHERES BETRIEBSSYSTEM

Mitbewerber: Windows CE

Was ist Windows CE?

Windows CE, auch bekannt als Windows Embedded Compact oder Windows Embedded CE, ist ein Betriebssystem, das für Windows Embedded-Geräte entwickelt wurde. Das Windows CE Betriebssystem versorgt seit mehr als 20 Jahren Industrie-, Medizin- und eine Vielzahl anderer Geräte. Microsoft lizenziert Windows CE an Originalgerätehersteller (ORIGINAL Equipment Manufacturers, OEMs), die ihre eigenen Benutzeroberflächen und Benutzeroberflächen ändern und erstellen können, wobei Windows CE die technische Grundlage dafür bietet. Die aktuelle Version von Windows Embedded Compact unterstützt x86- und ARM-Prozessoren mit board support package (BSP) direkt.

Wann ist das Ende des Lebens für Windows CE?

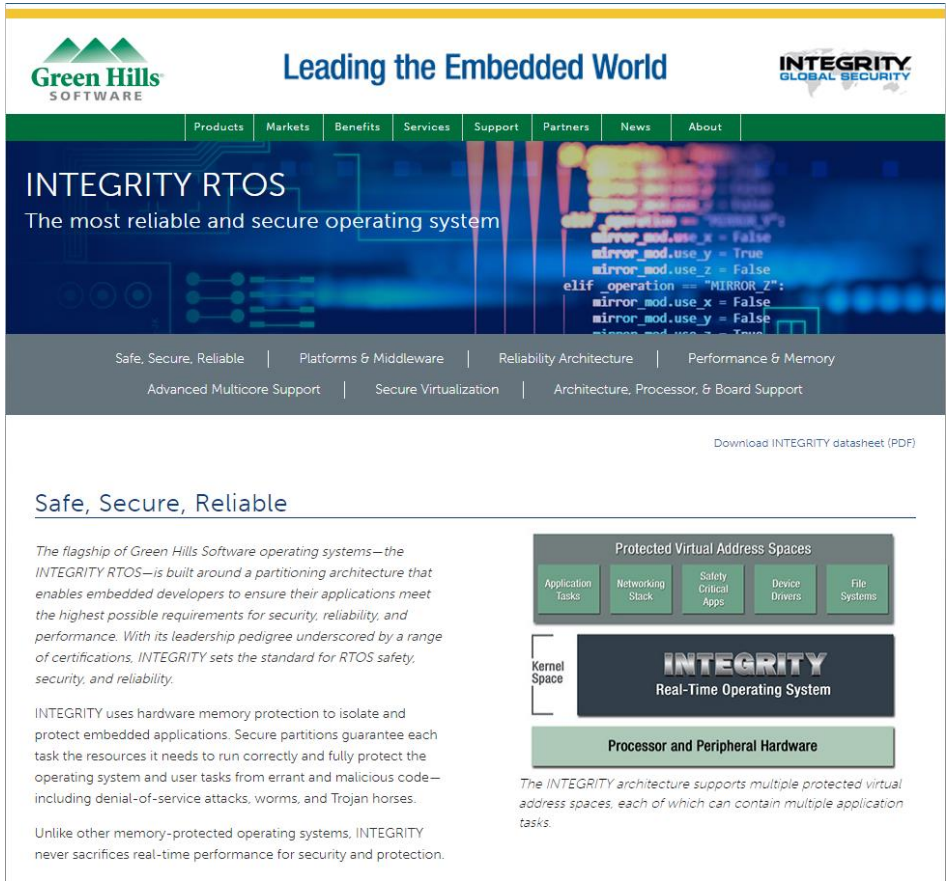
Während Windows CE 2013 das Ende des erweiterten Supports Ende 2023 erreicht, lässt Microsoft den Lizenzverkauf für Windows Embedded Compact 2013 bis 2028 zu. Und natürlich können Windows CE Geräte unbegrenzt weiter verwendet werden.

Bietet Microsoft die Möglichkeit, zusätzlichen Support am Windows CE 2013 nach 2023 zu bezahlen?

Microsoft hat derzeit keine Pläne, über 2023 hinaus erweiterten Support bereitzustellen.

Quelle: https://learn.microsoft.com/de-de/windows/iot-core/windows-ce-migration-faq

HON: Greenhills Integrity



Quelle: https://www.ghs.com/products/rtos/integrity.html

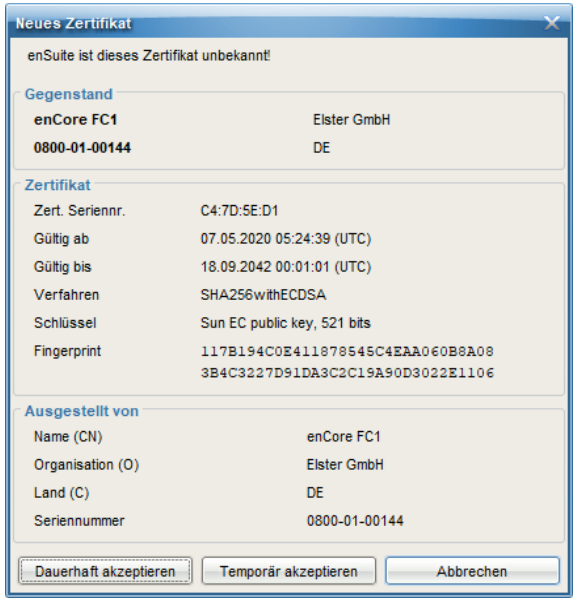
BEHANDLUNG SENSIBLER DATEN

- Sensible Daten = Informationen, die einen Bezug zu einer Person haben (z. B. Email-Adresse) oder Zugangsdaten (z.B. Passworte oder SIM-PIN)
- Bisher:
  - Daten sind in den Parametrierungen enthalten und können von jedem eingesehen werden, der Zugriff auf die Parametrierung hat
- Neu:
  - Daten sind weiterhin Bestandteil der Parametrierung, aber beim Auslesen einer Parametrierung werden sie nur authentifizierten, also angemeldeten Nutzern preisgegeben. Ohne Login kann die Parametrierung weiterhin gelesen werden, die sensiblen Daten sind aber nicht enthalten.
  - Innerhalb des Gerätes werden die sensiblen Daten verschlüsselt gespeichert, Änderungen sind nur mit gültigem Login möglich. Im Änderungslogbuch wird nur die Veränderung mit Zeitstempel, nicht aber alter und neuer Wert protokolliert.
  - In enSuite können beim Export einer gespeicherten Parametrierung und beim Versenden via E-Mail die sensiblen Daten nachträglich entfernt werden.

Besonderer Schutz personenbezogener Daten

VERSCHLÜSSELTE DATENKOMMUNIKATION PER MMS

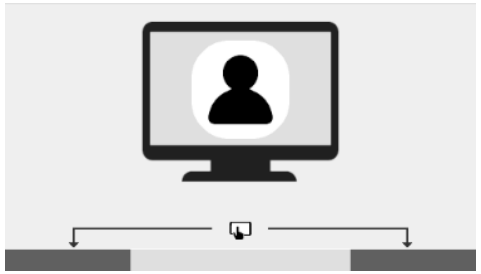
- Netzwerk-Protokoll MMS (Manufacturing Messaging Specification nach ISO 9506 wird zur Parametrierung, Archivabruf etc. genutzt
- Ab FW 03-39 unterstützen die enCore-Geräte das MMS-Protokoll nur noch in Kombination mit einer nach TLS (Transport Layer Security) verschlüsselten Datenübertragung
- enCore-Geräte erzeugen sogenannte selbstsignierte Zertifikate (keine CA im Einsatz)
- Bei der ersten Verbindung mit dem Gerät zeigt enSuite das empfangene Zertifikat an, die Verifizierung erfolgt durch den Anwender

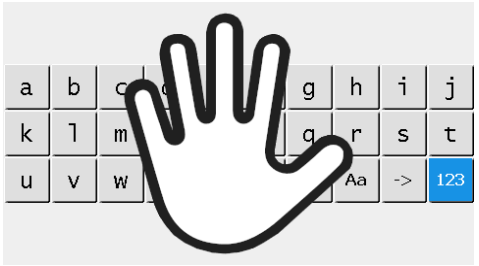


Schutz der Daten vor Abhören und Manipulation

FERNES BEDIENFELD

- Übertragung erfolgt jetzt über verschlüsseltes MMS-Protokoll statt über HTTP und kann damit nicht mehr mit einem Browser abgerufen werden.
- Es kann grundsätzlich nur ein Anwender das Gerät bedienen, die Kontrolle der Sichtbarkeit liegt beim Anwender, u.a.:
  - Findet eine Fernbedienung statt, dann ist die gleichzeitige Bedienung am Gerät nicht möglich und es wird eine Anzeige aufgeschaltet, die erklärt, wie man durch gleichzeitiges Drücken der beiden Funktionstasten die Fernbedienung beenden und die Kontrolle zurückerlangen kann
  - Erfolgt vor Ort eine Eingabe per Tastatur, wird dem entfernten Nutzer diese Eingabe verborgen, da er sonst in der Lage wäre, z. B. die Eingabe eines Passworts mit zu lesen.





Transparenz und Kontrolle der Anwenderaktivitäten

IN VORBEREITUNG

Komponenten-Zertifizierung
nach IEC 62443-4-2

KOMPONENTEN-ZERTIFIZIERUNG NACH IEC 62443

- Immer mehr Kunden und Behörden fordern sichere Messgeräte, ohne jedoch eine genaue Definition zu geben oder eine Norm zu nennen.
- Daher ist es für uns als Hersteller schwierig, die geforderten Maßnahmen zu spezifizieren und für den Anwender, das implementierte Sicherheitsniveau zu bewerten.
- Wir planen eine Komponenten-Zertifizierung nach IEC 62443-4-2 (sichere Industrielle Automatisierungs- und Steuerungssysteme) für die Gasmessgeräte.

THANK YOU

Honeywell