



2023
ODVA

Industry Conference and 22nd Annual Meeting

Industrial Ethernet Security Harmonization Group – Collaboration is Key

Simon Merklin
Endress+Hauser

Simon Merklin

Product Owner Security at Endress+Hauser
Leader of Industrial Ethernet Security Harmonization Group

Mail: simon.merklin@endress.com



- Why implementing security in industrial plants?
- What is the Industrial Ethernet Security Harmonization Group (IESHG)?
- Presentation of the results of the group
- What`s next?
- Wrap-up
- Q&A



2023
ODVA

Industry Conference and 22nd Annual Meeting

Industrial Ethernet Security Harmonization Group – Collaboration is Key

**Why implementing security in industrial
plants? ...and what did we as ODVA achieve
so far?**

Industrial Automation Cybersecurity Definition

- The prevention of
 - Illegal or unwanted penetration of IACSs
 - Intentional or unintentional interference with the proper and intended operation of IACSs
 - Inappropriate access to confidential information in IACS
- Security includes devices, networks, operating systems, applications and other programmable configurable components of the system

Source: ODVA Introduction to CIP Security 2022-05

Why implementing security in industrial plants?

NIS 2



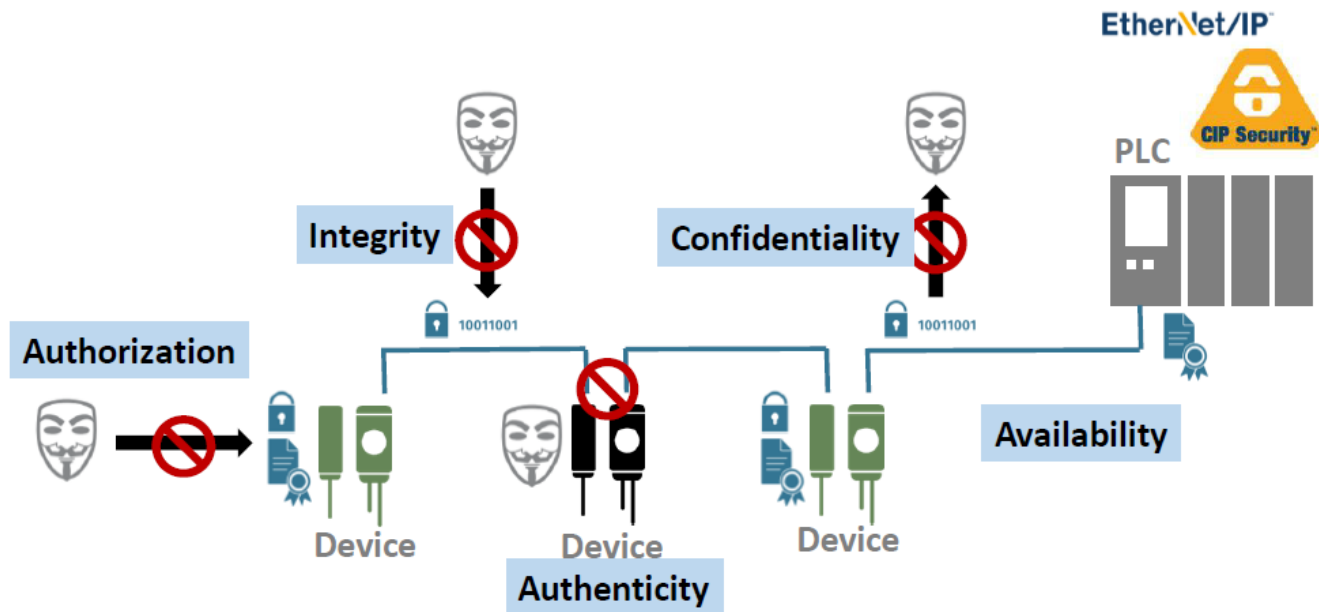
Source: infoguard.ch/

Cyber Resilience Act



Source: digital-strategy.ec.europa.eu/

Cybersecurity properties



Source: ODVA Introduction to CIP Security 2022-05



2023
ODVA

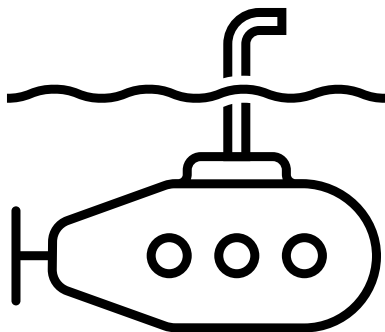
Industry Conference and 22nd Annual Meeting

Industrial Ethernet Security Harmonization Group – Collaboration is Key

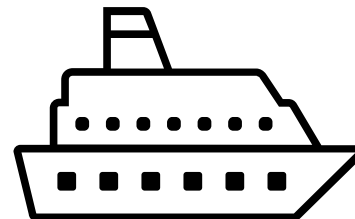
**What is the IESHG? ...and why should you
care?**

What is the IESHG?

Before SPS fair 2022



After SPS fair 2022



Explaining the setup

- Collaboration between ODVA, FieldComm Group, OPC Foundation and PROFIBUS & PROFINET International
- ODVA participants of IESHG:
- Jack Visoky
- Joakim Wiberg
- Simon Merklin (independent lead)



How we collaborate

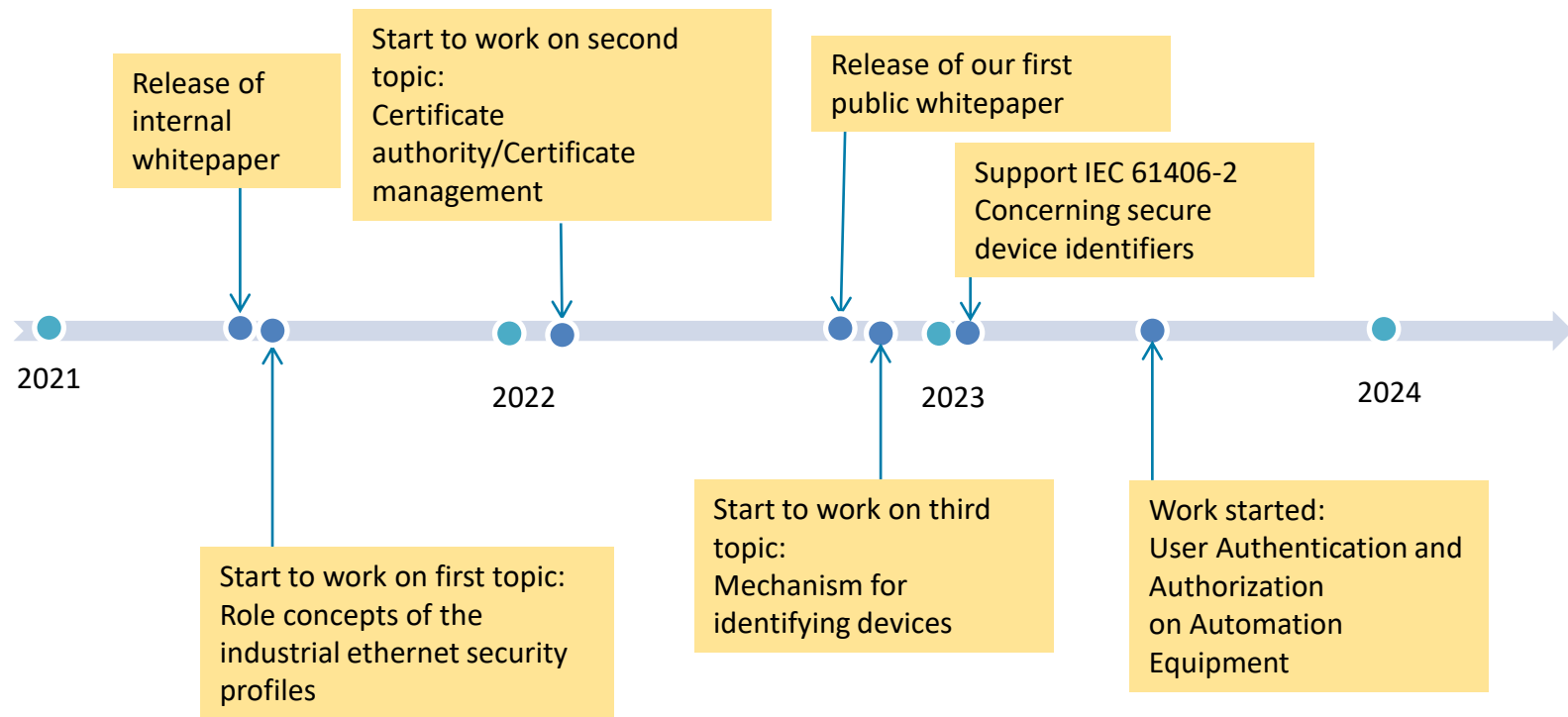
- Online Meetings
- Bi-weekly meetings
- The results of the group are circulated in the SDOs



Mission of the IESHG

- Our mission is the harmonization of cyber security strategies and concepts, so that end users do not face unnecessary complexity when using security concepts in their automation systems.
- This group will work out which concepts can be harmonized and how these concepts will be harmonized.
- A harmonization is conceivable for a wide variety of topics, such as common security recommendations for customers or sharing of security tools of the associations.

Roadmap of IESHG






2023
ODVA

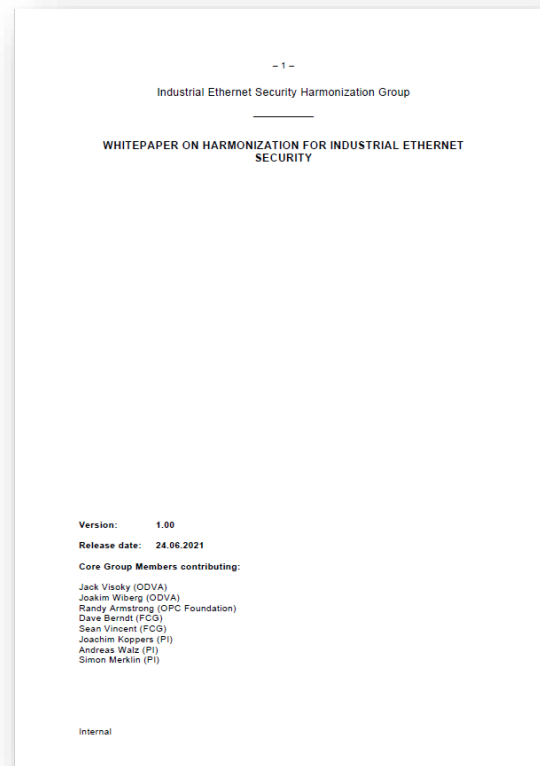
Industry Conference and 22nd Annual Meeting

Industrial Ethernet Security Harmonization Group – Collaboration is Key

IESHG deliverables

Results of internal whitepaper

- 
- Role concepts of the industrial ethernet security profiles
 - Certificate authority/Certificate management
 - Mechanism for identifying devices (cryptographical identities)
 - High level requirements scheme for devices that utilize industrial ethernet security profiles
 - Integrity and authenticity checks of devices and applications
 - Introductory material for end user motivation and architecture view



Role concepts of the industrial ethernet security profiles

- **Content:**
A crucial part of the access management of industrial ethernet communication are the role concepts that are used to restrict access to only those actors who need and are trusted with the access. For example, a maintenance engineer should have a different level of access permission than an administrator of a plant.
- **Goal:** The group defines a basic set of roles with corresponding definitions that can be used by all associations

Result of role concept evaluation

- The SDOs have different roles that can be grouped into meta-roles.
- However, the harmonization of these roles is not being pursued for the time being, as the roles are too heterogeneous.
- The meta-roles are defined and can be built upon.



Engineer




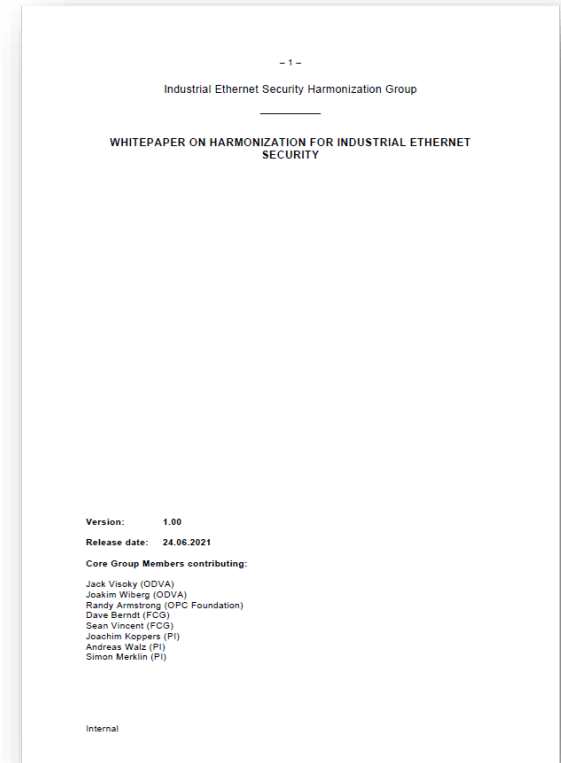
Admin



Supervisor

Results of internal whitepaper

- 
- Role concepts of the industrial ethernet security profiles
 - Certificate authority/Certificate management
 - Mechanism for identifying devices (cryptographical identities)
 - High level requirements scheme for devices that utilize industrial ethernet security profiles
 - Integrity and authenticity checks of devices and applications
 - Introductory material for end user motivation and architecture view



Certificate authority/ Certificate management

- Content:
Certificate management and the corresponding authorities will play a central role in future automation infrastructures. The certificates are a building block to achieve the security goals integrity, authenticity and confidentiality.
- Goal: The goal of this guideline is to establish a framework for a common terminology that needs to be established in the market.

Whitepaper Certificate authority/Certificate management



Industrial Ethernet Security Harmonization Group
FAQ ON INDUSTRIAL ETHERNET SECURITY CONCEPTS

PROFIBUS & PROFINET International (PI)
10.527 Follower:innen
3 Wochen

Industrial Ethernet Security Harmonization Group

The major standards development organizations (#SDOs) OPC Foundation, PROFIBUS & PROFINET International (#PI), ODVA, and FieldComm Group have announced the release of the first Whitepaper of their joint working group, the Industrial Ethernet Security Harmonization Group (#IESHG).

Read the #whitepaper here: <https://lnkd.in/eZSuaXa>

Übersetzung anzeigen
60 1 Kommentar • 6 direkt geteilte Beitr

Gefällt mir
Kommentar
Teilen
Senden

Kommentar hinzufügen ...



ARC Advisory Group
Member Log-in Europe

HOME | BLOG | INDUSTRIAL ETHERNET SECURITY HARMONIZATION GROUP (IESHG) PUBLISHES FIRST WHITEPAPER

Industrial Ethernet Security Harmonization Group (IESHG) Publishes First Whitepaper

NOVEMBER 29, 2022 BY CHANTAL POLSONETTI
CATEGORY: COMPANY AND PRODUCT NEWS



Security is a top priority for industrial automation users. The onus is on solution providers and product suppliers to provide solutions that make it practical for IA users to manage large networks of devices with security enabled by default.

The OPC Foundation, PROFINET International, ODVA and FieldComm Group have formed the Industrial Ethernet Security Harmonization (IESHG) joint working group to help address this challenge by finding ways to agree on common terminology and solutions. The goal of the working group is the alignment of industrial ethernet security concepts so that end users have less complexity when using security in their automation systems.

INDUSTRIAL ETHERNET

Industrial Ethernet Security Harmonization Group

FAQ ON INDUSTRIAL ETHERNET SECURITY CONCEPTS



Version 1.0 | September 19, 2022

FAQ ON INDUSTRIAL ETHERNET SECURITY CONCEPTS

Content

Disclaimer

Preamble

- 1 Introduction and scope
- 2 General concepts and terms
 - 2.1 Evolution of security in industrial automation plants
 - 2.2 Public-key cryptography and digital certificates
 - 2.3 Public-key infrastructure (PKI)
 - 2.4 Certificate Authority (CA)
 - 2.5 Registration Authority (RA)
 - 2.6 Certificate Revocation Mechanism and Certificate Revocation Lists (CRL)
 - 2.7 Certificate Chains
 - 2.8 Certificate hierarchies in an industrial environment
 - 2.9 Trust Lists
 - 2.10 Why are different types of Certificates needed?
 - 2.11 Different types of certificates
 - 2.11.1 Device certificates need business level trust relationship
- 3 Certificate Management Tool
 - 3.1 General
 - 3.2 Workflows of a Certificate Manager
 - 3.2.1 Register/Unregister devices and applications
 - 3.2.2 Request Certificate
 - 3.2.3 GetTrustList
 - 3.2.4 Check Revocation Status
- 4 Miscellaneous
 - 4.1 Glossary
 - 4.2 Abbreviations
 - 4.3 Version History

What kind of device certificates are described in an industrial environment?

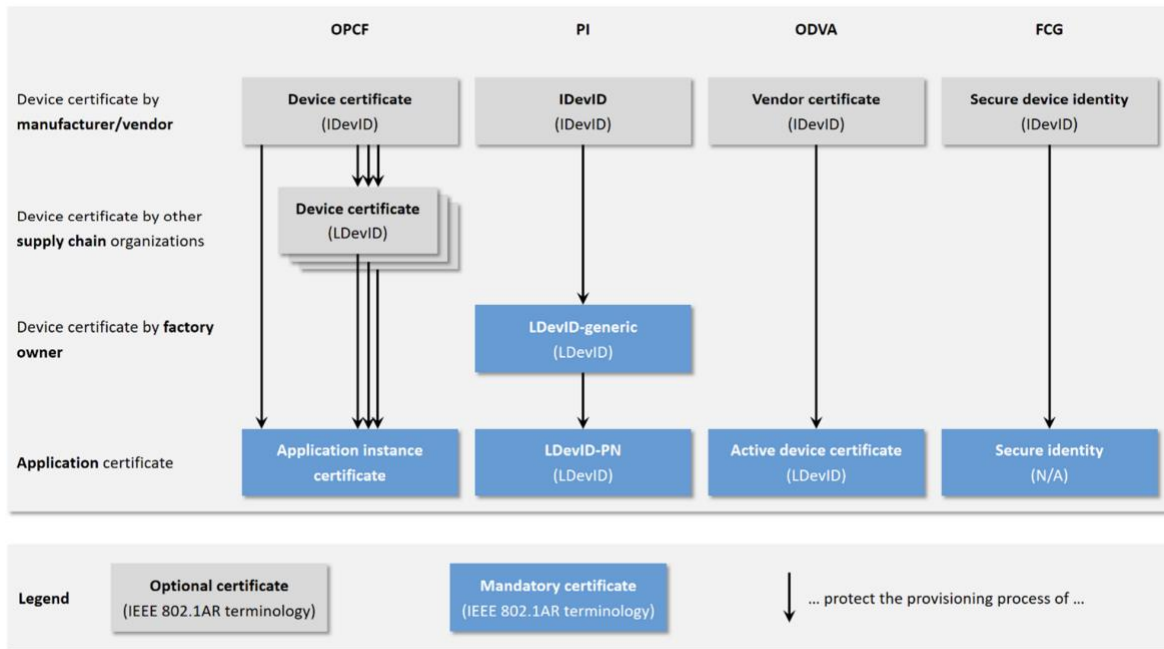
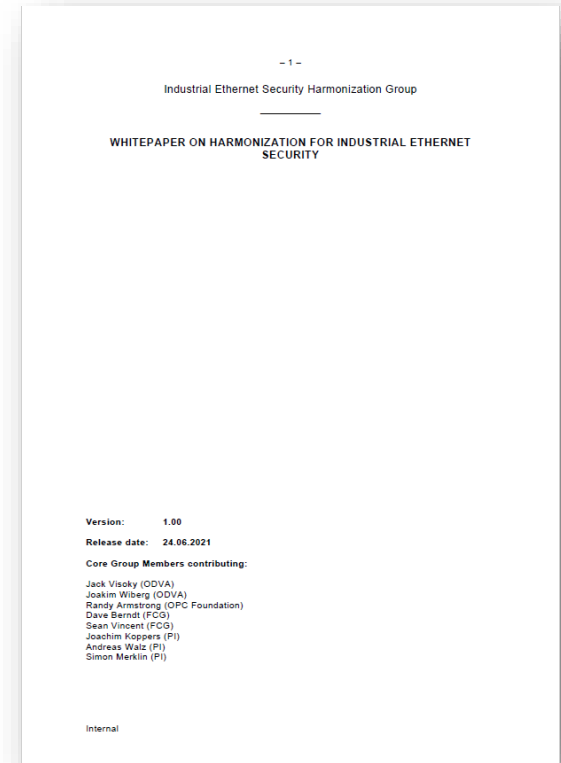


Figure 2-1 SDO certificate types overview

Results of internal whitepaper

- Role concepts of the industrial ethernet security profiles
- Certificate authority/Certificate management
- Mechanism for identifying devices (cryptographical identities)
- High level requirements scheme for devices that utilize industrial ethernet security profiles
- Integrity and authenticity checks of devices and applications
- Introductory material for end user motivation and architecture view



Mechanism for identifying devices

- Goal: The goal is to create a detailed guideline for manufacturers for IDevIDs in device and to reflect the products origin. Furthermore, a guideline to reflect the product ownership via LDevIDs shall be created.

Vendor production plant



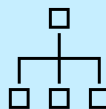
Ethernet device

- Device gets manufactured in vendor production plant
- Initial Device Identifier (IDeVID) are created in the device
- A commonly used standard for IDeVIDs is [802.1AR](#)

Mechanism for identifying devices

Vendor production plant

Vendor CA

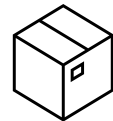


Signing



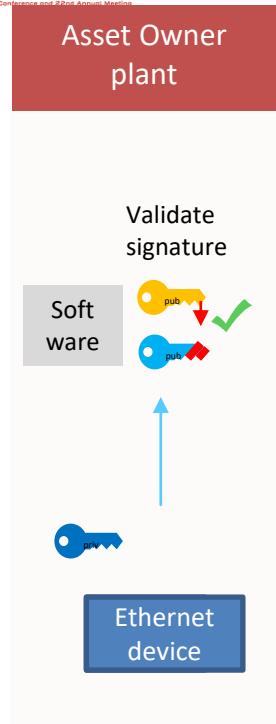
Ethernet device

- The IDeVID of the device gets signed by the Vendor CA private key.



Shipping

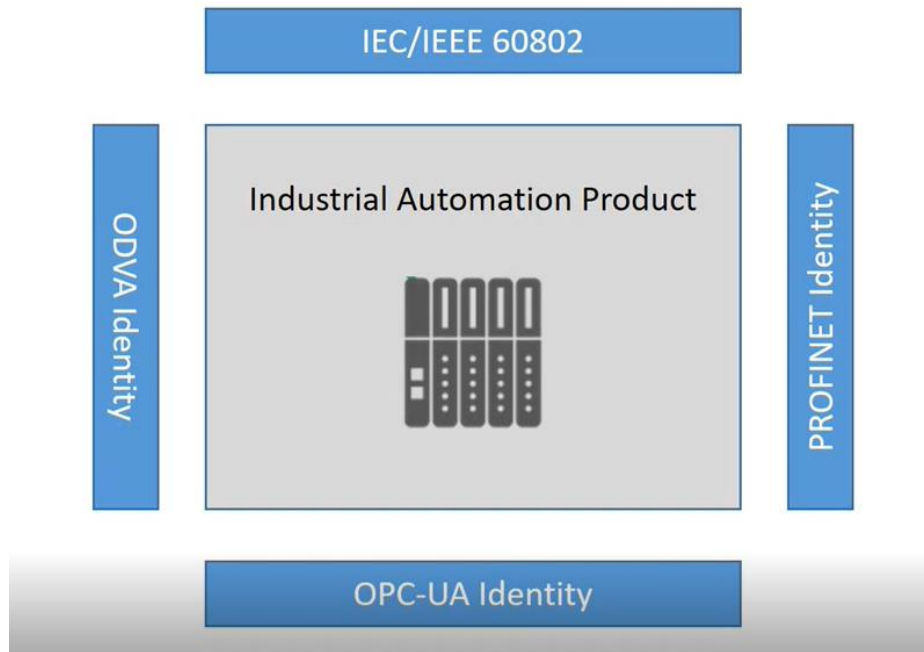
Mechanism for identifying devices



- Asset owner takes possession of the device
- Asset owner validates signature of device's IDevID with the public key of the Vendor CA.

...

Industrial Automation DevID Profile





2023
ODVA

Industry Conference and 22nd Annual Meeting

Industrial Ethernet Security Harmonization Group – Collaboration is Key

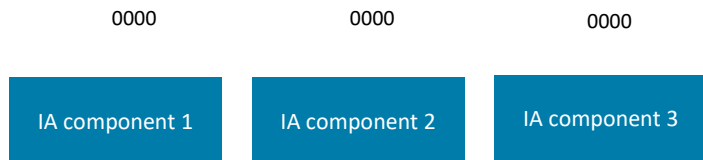
What`s next?

Whats next?

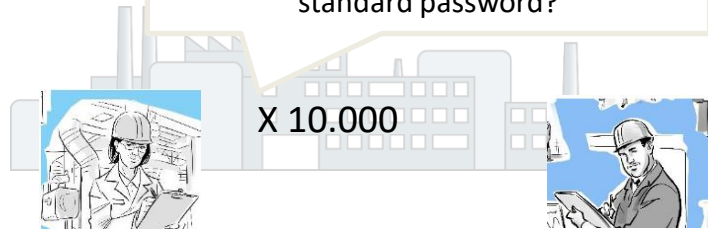
- Today, each SDO, and each product vendor have their own role concepts and authorization mechanisms.
- Some island solutions already emerged to manage the authentication and authorization on each protocol in a centralized way.
- However, all these mechanisms to authenticate and authorize at different protocols will end up to be an administrative nightmare.

New legislation leads to end-user pain

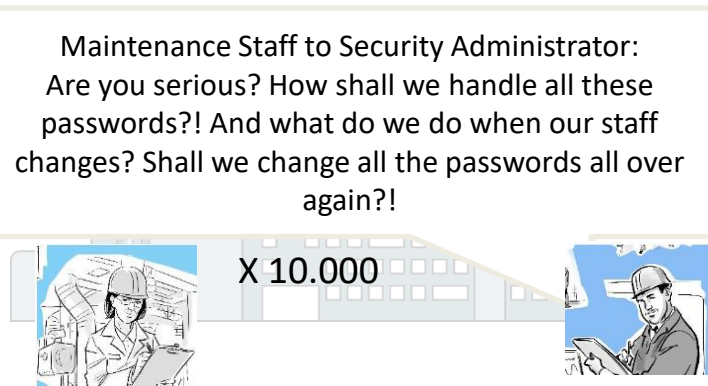
Today: 4-digit PIN



Security Administrator of plant to
Maintenance Staff:
Are you serious? You do not change the
standard password?



Future: individual digital interfaces
with individual
accounts with individual
passwords





2023
ODVA

Industry Conference and 22nd Annual Meeting

Industrial Ethernet Security Harmonization Group – Collaboration is Key

Wrap-up and outlook

Wrap-up and outlook

- Industrial Ethernet Security Harmonization Group is a cross-SDO working group for the harmonization of industrial security topics.
- The first white paper has been published (more will follow)
- The next step will be an SDO-wide definition for device identifiers and centralized user management





2023
ODVA

Industry Conference and 22nd Annual Meeting

- Are there other topics that you would like to see harmonized?
- How do you identify products in your plants today?
- Did you ever have the problem of managing different interfaces in your plant?