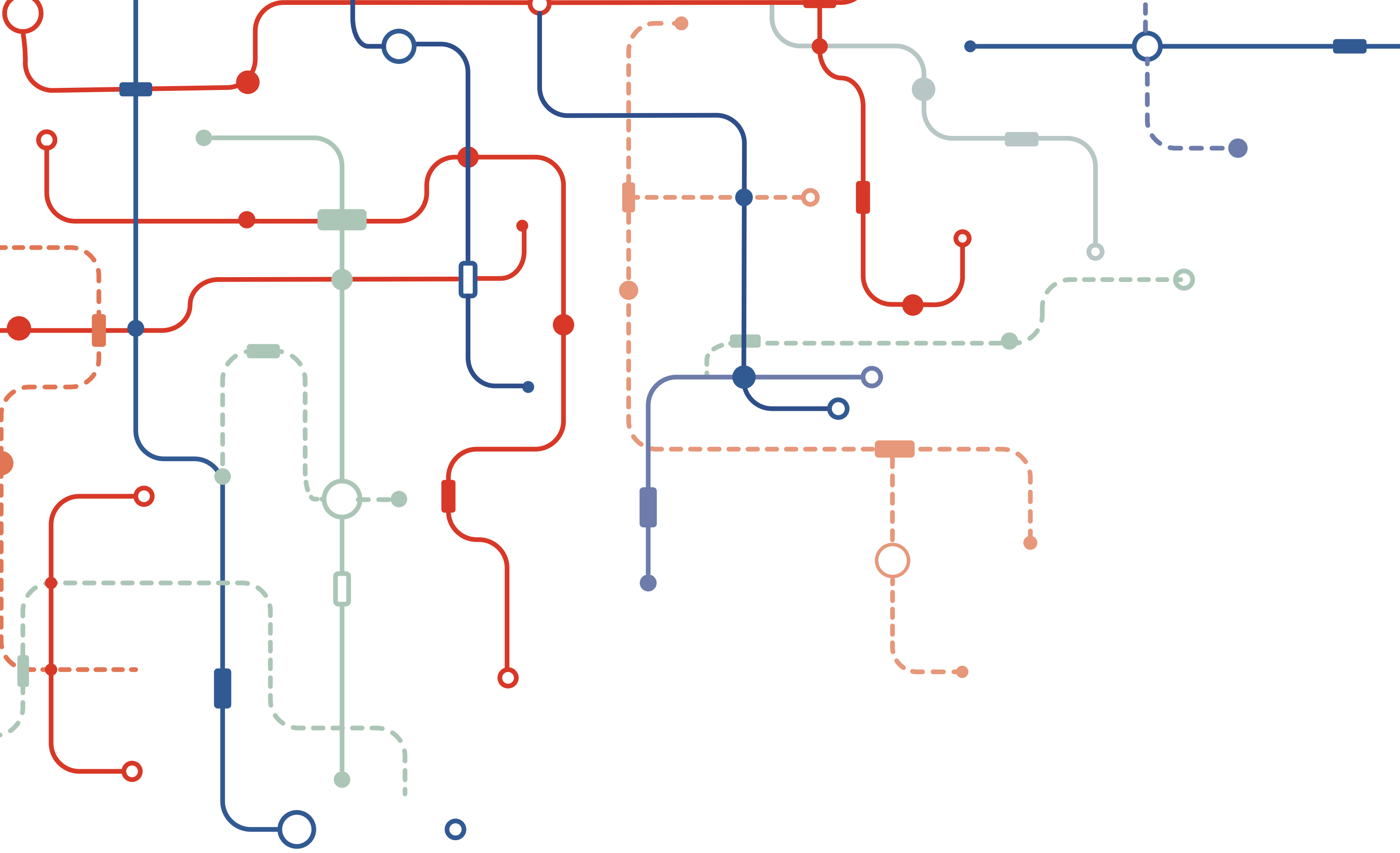
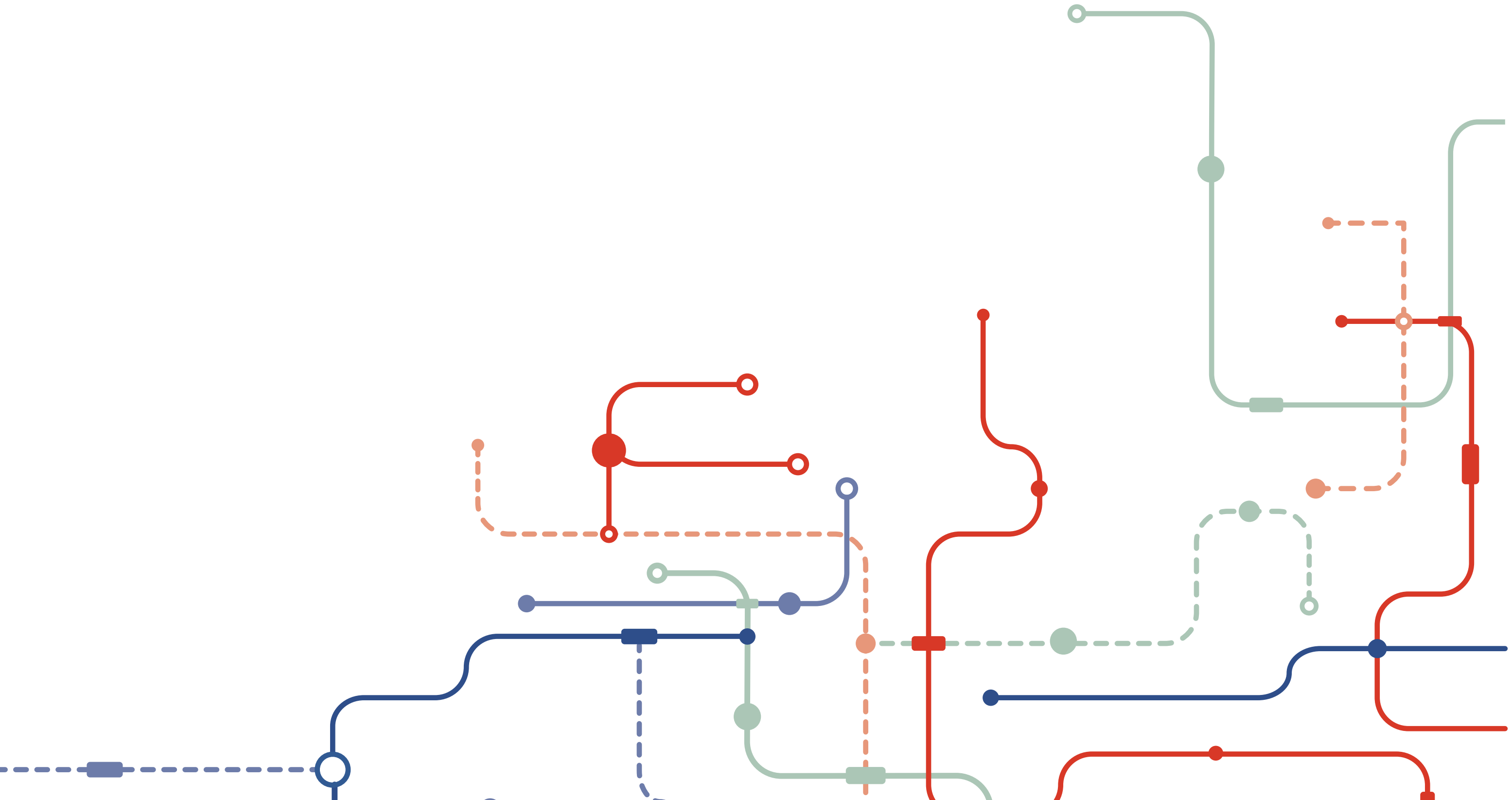


# Security for Industrial Plant



# TABLE OF CONTENTS

## Introduction / Definition

### What is an Industrial Programmable Logic Controller (IPLC)?

Industrial Programmable Logic Controllers (IPLCs) are an integral part of Automated Production Systems (APS). They are designed to produce quality products at a cheaper cost and with fewer human operations. IPLCs first appeared at the end of the 1960s to meet demands from the automotive industry for increased adaptability in their control systems.

Reduced electronic costs then made it possible to replace hard-wired logic (electromagnetic relays and pneumatic systems) by programmable logic (microprocessors).

Figure 1 - Assembly line using IPLCs

This paved the way for the first Industrial Programmable Logic Controllers, a kind of computer adapted to the relatively constrictive world of industry: dust, humidity, temperature, vibrations, simple programming language required for user-friendly operations (implementation, troubleshooting by non-IT specialists), upgradable hardware.

Figure 2 -Examples of Industrial Programmable Logic Controllers (IPLC)

Today it is impossible to imagine a production system that does not include automated systems and thus the use of IPLCs. IPLC have multiple and varied fields of application: automotive, industrial chains (industrial robots), packing (moving objects onto palettes or other items, etc.), wood sawing and machining, machine-tools (drilling, punching), etc.

Safety IPLCs fulfil a safety function, i.e. for lifts, railways or dangerous machines.

To summarize, IPLCs are electronic programmable devices designed to control industrial processes using sequential processing: they send commands to the pre-actuators (Operative Part) using input data (Command Part), instructions and computer programs.

Industrial players connect their IPLCs to networks with a view to increasing productivity and production flexibility.

### IPLC networks

Different types of network exist, depending on the type of "communication" exchange and the level at which it takes place (field, plant, etc.):

- Ground network: used for sensor interconnection, measuring devices, etc.
- Computer network: used to interconnect computers.

CIM (Computer Integrated Manufacturing) can be used when segmenting automatic controls at different levels: sensor/actuator (level 0), automatic control (level 1), monitoring (level 2), data processing (levels 3 and 4) by combining the volume/performance pair.

IPLC manufacturers create networks and buses in line with their needs. As such, a bus or network can be assigned to each level:

- "Sensor bus", simple, single actuators and sensor buses
- "Device bus", bus and networks for IPLC periphery: variable speed drives, robots, axles, etc.
- "Field bus", communication networks between processing units: Industrial Programmable Logic Controllers, supervisors, numerical control, etc.

Local Industrial Network, to establish communication between the IPLC and the data processing environment.

In this way, since the objective is to control and manage the production, the IPLCs are now connected to mini-computers and a monitoring logic controller (see Figure 4).

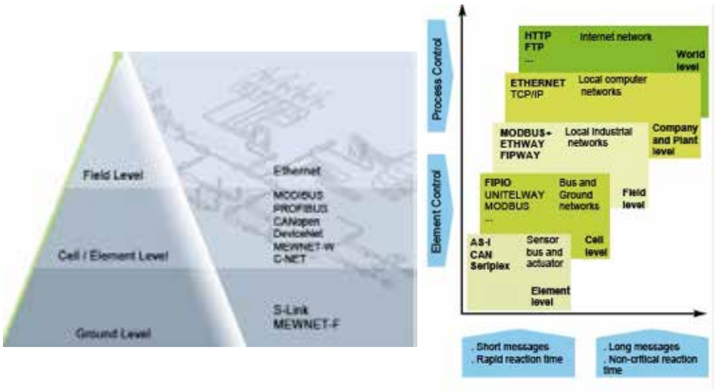


Figure 3 - Network of Panasonic and Schneider Electric IPLCs

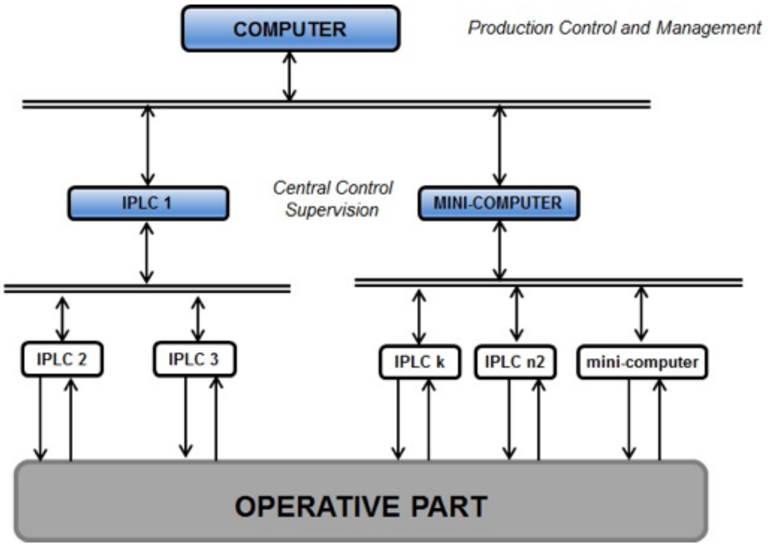


*Figure 4 - Example of a two-level (ground and field) IPLC network (control structure and production management).*

As shown on Figure 4, most networks are owners, apart from that connecting the automatic control environment to the data processing environment: the standardized Ethernet network.

By adopting global standards such as Ethernet and TCP/IP, it is now possible, for any authorized person, using Extranet, Intranet and Internet, to access data from a IPLC in real-time, from any location.

In this way, many remote services are available, such as: access to IPLC data bases, diagnosis of the IPLC controller and its configuration, graphics editors used to visualize and control process data, alarm reports, etc.

In the same way, it is also possible to redistribute this data to other persons by email or using web forms. In short, these networks establish an embedded human-machine interface in real-time.

As shown on Figure 4, most networks are owners, apart from that connecting the automatic control environment to the data processing environment: the standardized Ethernet network.

By adopting global standards such as Ethernet and TCP/IP, it is now possible, for any authorized person, using Extranet, Intranet and Internet, to access data from a IPLC in real-time, from any location.

In this way, many remote services are available, such as: access to IPLC data bases, diagnosis of the IPLC controller and its configuration, graphics editors used to visualize and control process data, alarm reports, etc.

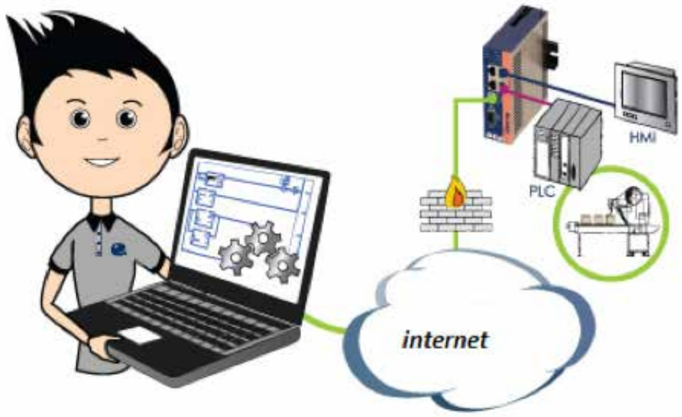


*Figure 5 - Using the Internet to control IPLCs remotely*

In the same way, it is also possible to redistribute this data to other persons by email or using web forms. In short, these networks establish an embedded human-machine interface in real-time.

## Security

Network interconnectivity engenders a wide range of risks in terms of the security of the entire network.

### Authentication

In industrial environment, in fact, about 25% of all reported data security breaches are the result of malicious insider activity. For example, during IPLC maintenance, when diagnostic tools are connected to fix, or update the IPLC software, personnel can access the secure data.

To prevent this, human intervention must be locked out to eliminate the possibility of data manipulation or the installation of malicious modifications.

This "new" remote maintenance entails the risk of malicious takeover via the Internet, if an "unauthorized" person gains access to the monitoring command. Steps must be taken to control access to the monitoring consoles via the network.

In this way, several IPLCs from a single network must then be authenticated, thus blocking access to any uninvited "newcomers" (for example).

Finally, to manage console user rights, access to the monitoring console must be controlled independently from the network: who is trying to connect? What rights do they have for this console?

In an Industrial infrastructure where plants are no longer operating in a stand-alone mode but are interconnected like in a SCADA (Supervisory Control And Data Acquisition) infrastructure, it's mandatory that each of the final element in the factory (e.g. sensors, robot actuator, motors…) to be security authenticated and can securely communicate with the supervisory control system. It is as important that the final element can make sure that the command it receives is really coming from a trusted sender.

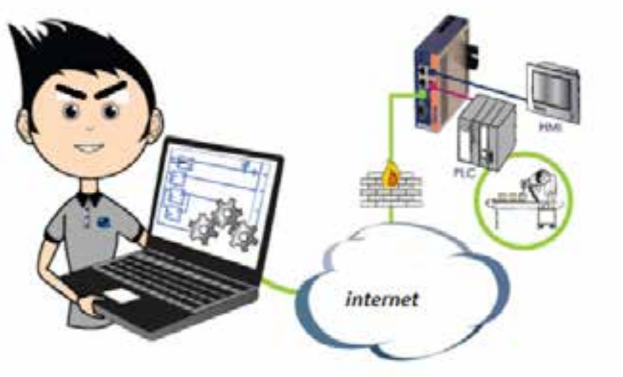


*Figure 6 - It is possible to control IPLCs remotely and with malicious intent via the Internet*

Consequently, security requirements are as follows:

1. Mutual Authenticating between IPLCs, final element and supervisory control system through an Ethernet network (or similar) and owner network
2. Mutual authentication of the monitoring console on the network with the IPLC
3. Mutual Authentication between the technician and its maintenance console
4. Securing data that is transmitted across the network

Both levels of the network affected by these risks can be identified on Figures 7 and 8 below:

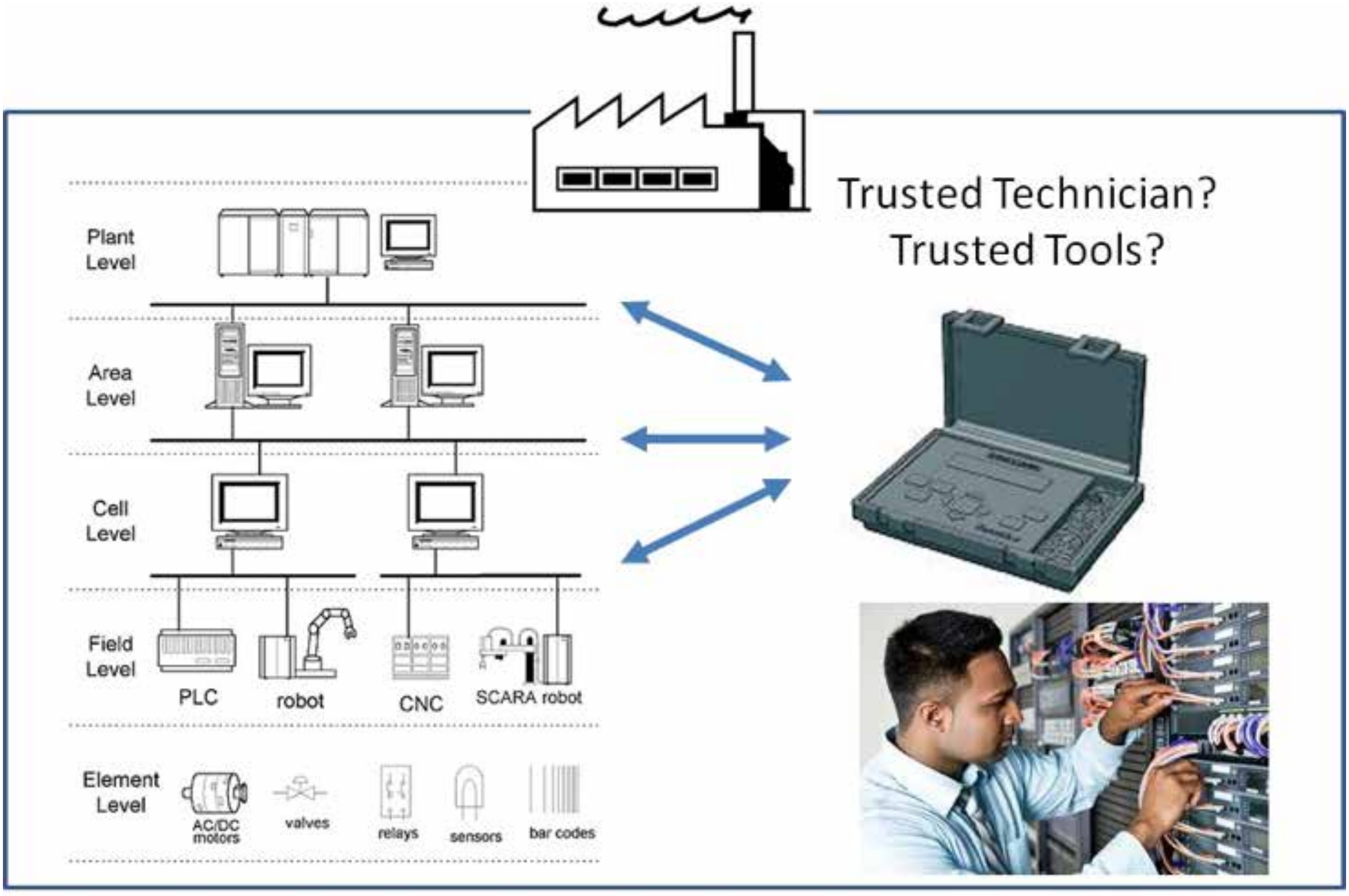


*Figure 7 - Structure of a multiple-level IPLC structure: human operation at field level*

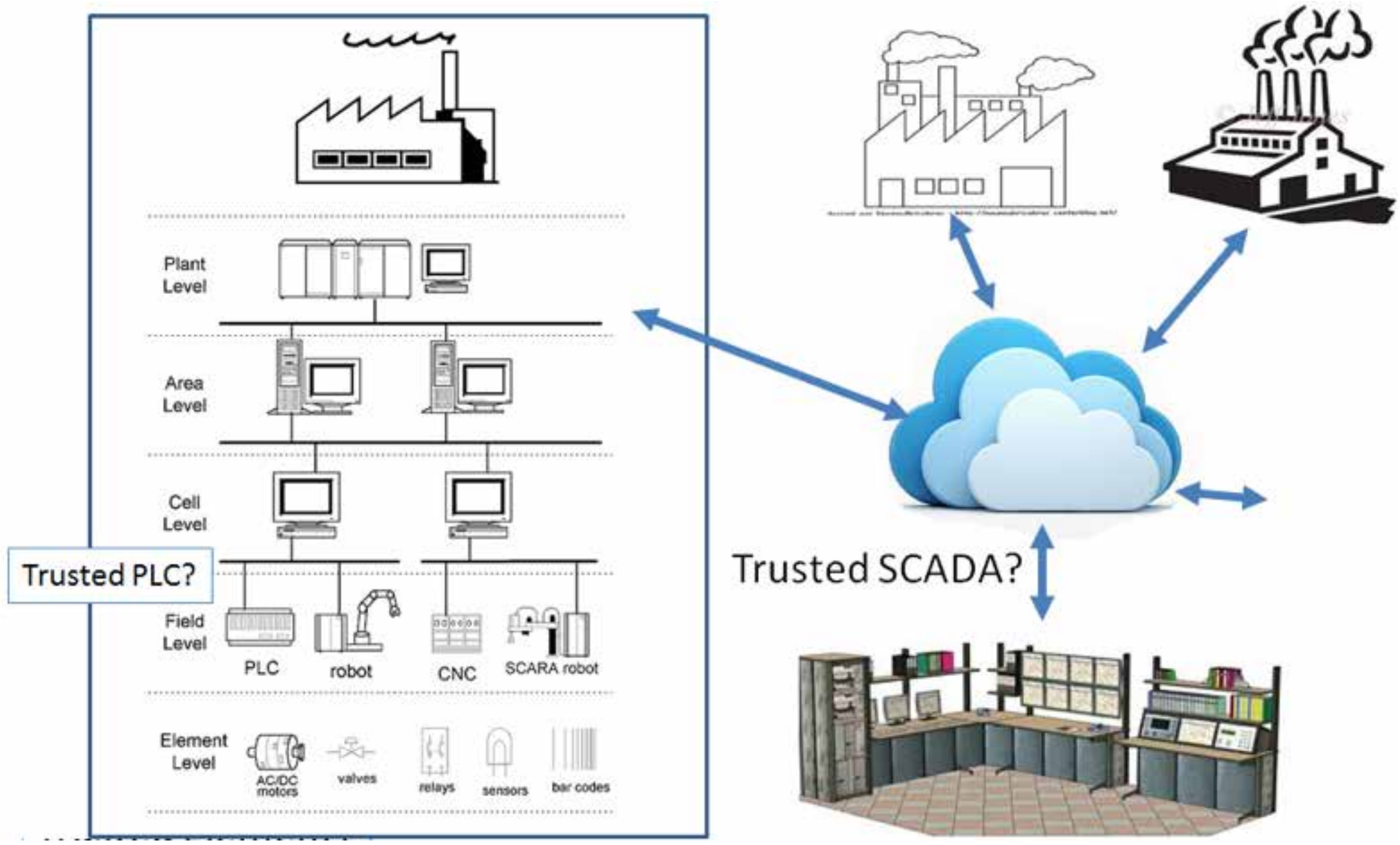


*Figure 8 - Structure of a multiple-level IPLC structure: human operation at Plant level*

### Securing Communication

As described in chapter 1.2, IPLC network are based on Ethernet or Internet technologies and protocols. These protocols provide a selection of proven secure communication solutions.

MACsec is the IEEE security protocol designed for strong hop-to-hop security, low latency and high throughput for 1G, 10G, 40G, and 100G Ethernet. It protects Layer 2 of the OSI model, consisting of two parts:

- Data plane protocol - IEEE802.1AE
- Control plane protocol - IEEE802.1X-2010 (MKA)

The performance advantages of the MACsec protocol are based on its data encryption algorithm. The MACsec data plane uses the robust, highly scalable AES-GCM crypto cipher; the scalability to support multiple operations in parallel enables very high throughput configurations. The other important advantage of MACsec is that because it operates at Layer 2, all higher levels are protected transparently to application software.

The actual use case of the node typically dictates the criteria for selecting the leveraged secure communication protocol – for example, in “SCADA” deployments where the communication model typically follows the client-server model, protocols such as SSL/TLS or DLTS are used, while in “full mesh”-type networks a network level security protocol such as IPsec is more applicable.

All three security protocols that are mentioned above can use the earlier introduced and proposed suggested PKI authentication in a standardized way. This guarantees the IoT nodes’ seamless integration into and interoperability with the existing standard network infrastructure.

While the data rates to and from an individual node are typically limited in IPLC network deployments, the constrained nature of the host devices may pose implementation challenges in the context of cryptographically secured communications. To limit the amount of CPU cycles used for cryptography on the general purpose processing unit of the host, and to reduce power consumption of the device during crypto operations, it is likely beneficial to offload the symmetric and asymmetric cryptographic algorithms to specialized silicon. When executed on hardware the common symmetric encryption algorithms (such as AES and 3DES) and asymmetric algorithms (such as RSA and ECDSA) are faster and more power- efficient (which is important in power-constrained and battery-powered devices) compared to software implementations.

## Solutions Offered by WISeKey

### WISeKey Unique Root of Trust Model

A Root of Trust (RoT) is the basis for a global end-to-end security solution. A RoT serves as a common trust anchor, which is recognized by the operating system (OS) and applications, to ensure the authenticity, confidentiality and integrity of on-line transactions. With the cryptographic RoT embedded in the device, the IoT product manufacturers can use PKI (Public Key Infrastructure) technologies to secure interaction among objects and between objects and people.

WISeKey has a unique positioning to offer a consistent security system from the RoT to back-ofice. WISeKey is the trusted operator of the International Organization for the Security of Electronic Transaction (OISTE) Global Root. The OISTE Foundation is working with the UN and International Organizations since 1999 in line with the United Nation's Sustainable Development Goals which include giving everyone a legal identity by 2030. Swiss neutrality, security, and privacy laws allow operations without geo-political or governmental constraints. The RoT is the only one available outside NATO. It is located in a military grade bunker located in the Swiss Alps.

### Certificate Authority

Based on Trusted Root Keys, the Certificate Authority (C.A.) creates a digital certificate for each individual device which uniquely and strongly identify the device. A C.A. can also generate digital certificates to secure communications or control applications.

WISeKey can support a corporate Sub C.A. under WISeKey's Root of Trust model

WISeKey Certificate Management System is also compatible with third party C.A. based on Microsoft or Enterprise Java Beans Certificate Authority (EJCBA) open source C.A.

### Use of Digital Certificates

The digital certificate is used to identify and authenticate devices during their entire life. Only trusted devices can connect to secure networks.

Digital certificates, for instance SSL certificates, can also be used to secure communication channels from devices to gateways/routers, and from gateways/routers to servers.

WISeKey also offers solutions to control the device's firmware integrity at initial stage (bootloader) and during upgrades in the field.

For the best security, digital certificates can be loaded in tamper resistant secure chips in WISeKey secured premises. These chips are then integrated in the IoT devices to become the concrete hardware foundation upon which the security subsystem is built upon.

WISEKEY proposes to create an Identity for each device connected. The identity is provided in the form of digital certificate. For the devices that are in the factories (e.g. PLC) or in the field (e.g. programming consols).

### Certificate Management System (CMS)

The WISeKey Certificate Management System (CMS) is a software tool with user friendly interface that allows the complete management of the digital certificates during the whole life of the IoT device, from the manufacturing to the field.

The status of the certificates can be checked or changed at any time by the administrator. They can for instance be remotely revoked, or frozen.

The optional message broker allows to authenticate and validate the messages coming from the different IoT devices and transfer only trusted messages to the IoT platform of our customer. The WISeTrustIoT framework can be integrated into customer IoT platform easily as the customer does not need to implement additional security mechanisms. When the Message Broker is integrated in customer premises the solution offers end-to-end security from the IoT device to the customer back-office.

The WISeKey CMS also includes secure provisioning solutions to help maintain a consistent high system security, even when the IoT device is in an unsecured environment (contract manufacturers, in the field). Devices configuration and firmware upgrades are made easy and secure at any time.

WISeKey CMS can be installed in customer premises, bur for the ones not willing to deploy their own infrastructure, WISeKey can provide trusted services from any of its local secure datacenters in Switzerland, USA, India or China. The managed platform can be accesses through a browser and a web-service API.

## Security Module

WISekey recommends to store the secure assets (Digital certificate and associated Device private keys) in a security Module.

A Security Module provides an extremely high level of protection, existing specifically for the purpose of performing its pre-programmed security routines. These cryptographic services and functions, executed in a physically small, hardened environment, include low-level cryptographic methods and algorithms needed for authentication and data encryption/decryption as well as secure storage of essential data items (private keys, CA and user certificates, user credentials and configuration data). This enables highly trusted methods of mutual authentication between system components to effectively block attacks on security network.

WISeKey propose Security Modules in the form of a physical companion chip (VaultIC products).

VaultIC is a product family of tamper resistant security modules to be used as a companion chip to the IoT-device host processor). VaultIC embeds configurable cryptographic tool boxes for Authentication, Confidentiality and Integrity executed in a secure environment. The tool box is proposing a variety of standard and NIST recommended algorithms and key lengths (e.g. ECC, RSA, ECDSA, AES, SHA,..). VaultIC embeds on-chip tamper resistant data storage capabilities (NVM) for keys, certificates and customer data. VaultIC also features a True Random Number Generator to guarantee the entropy needed for high-level cryptographic services (not achievable in software).

The VaultIC low-power consumption profile makes it a viable solution to meet the limited power budgets of the embedded IoT nodes.

VaultIC comes with middleware including secure boot, secure firmware update for IoT devices and a secure communication (SSL/TLS) stack.

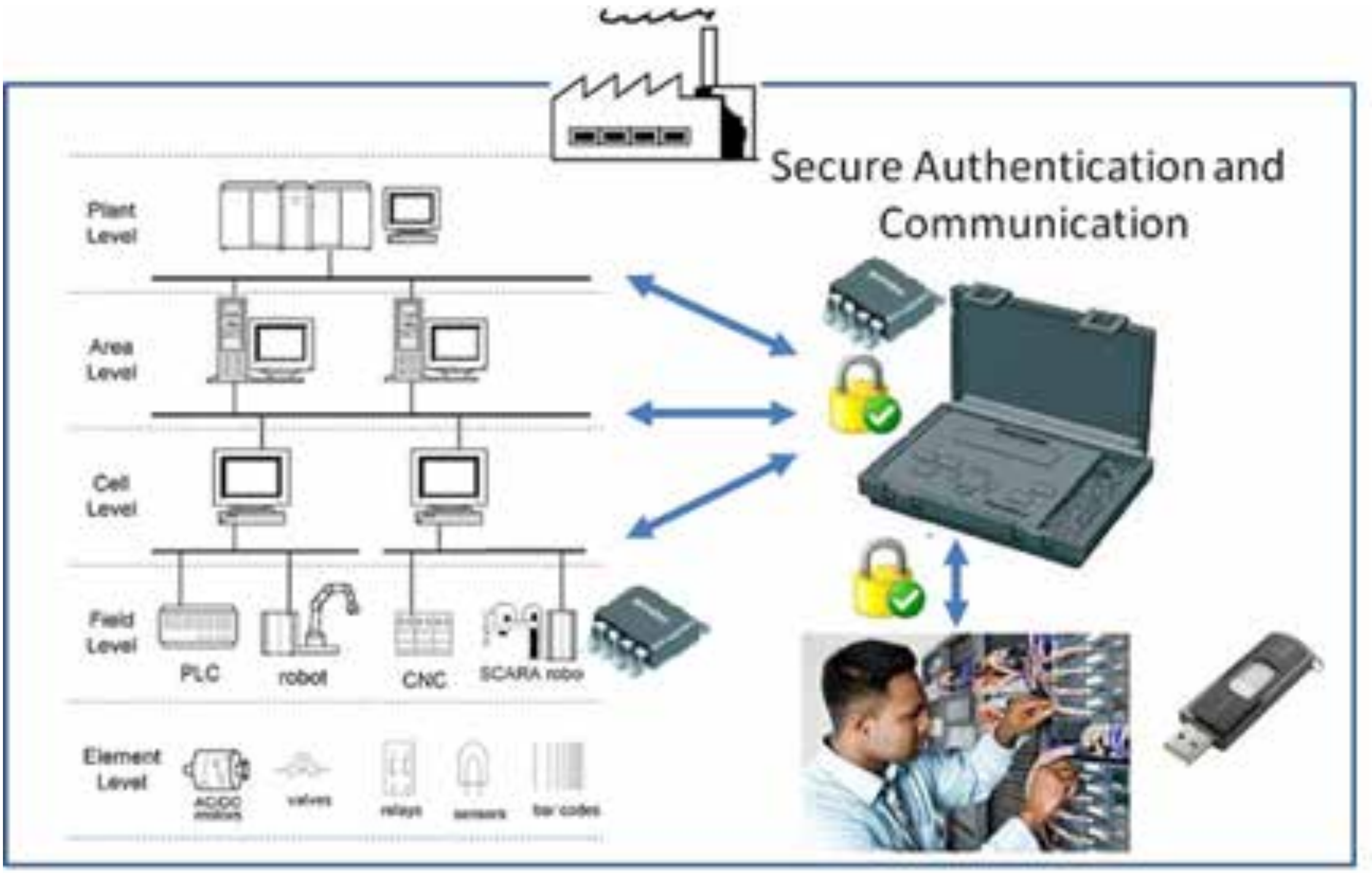


*Figure 9 - Structure of a multiple-level IPLC structure: securing data at field level*

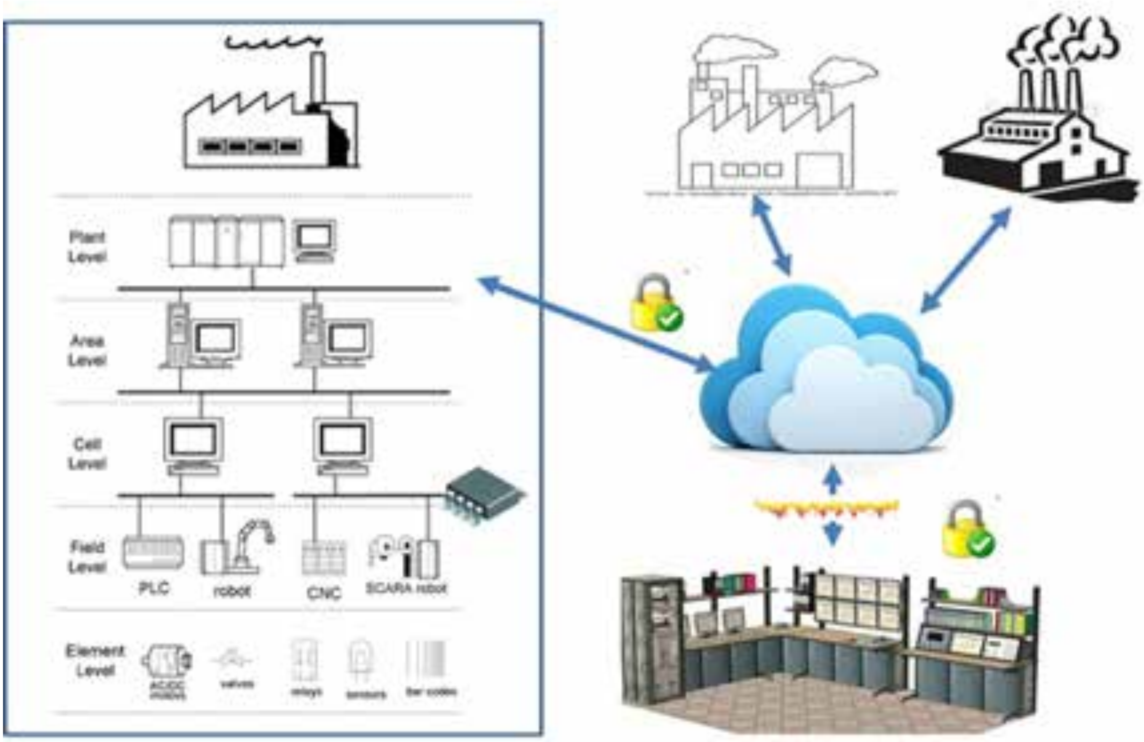


*Figure 10 - Structure of a multiple-level IPLC structure: securing data at plant level*

Secure Modules, such as WISeKey's VaultIC, provide multiple advantages when compared with software-based security, including:

- Crypto keys and other security materials are stored in the under the control of secure hardware, beyond the reach of any software attack
- Protection against physical attacks, also referred to as tamper-resistant
- Digital signature and verification like ECDA are performed within the Secure Module
- True Random Number Generation is performed within the Secure Module hardware, delivering true randomness that is vital for high quality generation of encryption keys – software alone is limited to Pseudo Random Number Generation, weakening encryption and security

VaultIC are certified by the US FIPS 140-2 Level 3 (version 2011) standard.

Hardware Security provided by a VaultIC module is recognized by international standards, based on a certified "common criteria" hardware platform, and used by banks and government organizations.

In this architecture, IPLC authentication relies solely on VaultIC. It is therefore possible to assign VaultIC a "genuine" IPLC and then place it on another ("fake") IPLC. Server data can thus be accessed without this tactic being "perceived" by the server. VaultIC must therefore bind with its "host" through mutual authentication. Since the host is not in a secure environment, it must be possible to "hide" the Host authentication keys somewhere in its internal memory and to retrieve them whenever necessary. This is the function provided by Secure Binding.

### Authentication of user through USB key

This key contains the secret authentication keys, stored in the key's tamper-proof "vault": VaultIC. Access to these keys is protected by an access key (password, PIN code, etc.).

*Figure 11 - Authentication USB key based on VaultIC405*

The authentication protocols used by VaultIC are based on standards (Global Platform SCP02, SCP03, Microsoft Mini-driver) that use DES or AES secret keys.

Server authentication of the programmer in possession of an authentication USB could therefore be performed and the programmer could be assigned access rights, even remotely, whether via his console or a computer.

Remote authentication is possible on the Internet using secure communication standards (TLS, SSL), compatible with VaultIC modules.

Security can be enhanced by combining two or three authentication factors like USB key unlocking thanks to a password and/or a biometric verification like finger print or a one time password (generated based on internal real time clock).

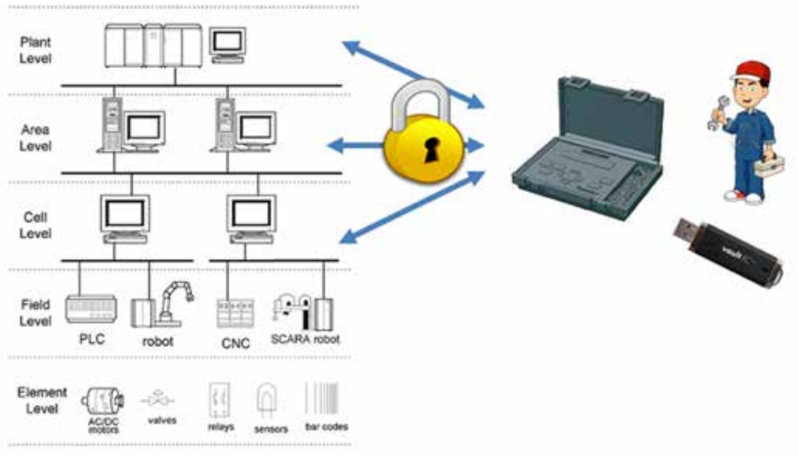


*Figure 12 - Using an authentication USB key on a programming console*

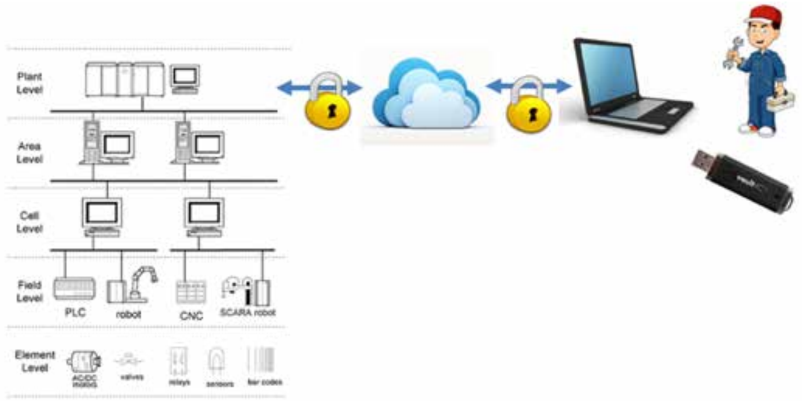


*Figure 13 - Using an authentication USB key on a programming console*

## Acronyms

| | |
|---|---|
| AES | Advanced Encryption Standard |
| APS | Automated Production System |
| CA | Certificate Authority, entity that issues digital certificates |
| CC | Common Criteria |
| CPU | Central Processing Unit |
| CIM | Computer Integrated Manufacturing |
| CMS | Certificate Management System |
| DES/3DES | Data Encryption Standard |
| ECC | Elliptic Curve Cryptography: is an approach to public-key cryptography |
| ECDSA | Elliptic Curve Digital Signature Algorithm. Cryptographic Algorithm based on ECC used for digital signature. |
| EJCBA | Enterprise Java Beans Certificate Authority |
| FIPS | Federal Information Processing Standard |
| IoT | Internet of Things |
| IPLC | Programmable Logic Controller |
| IPSec | Internet Protocol Security |
| Minidriver | Windows Smart Card Mini Driver |
| NIST | The National Institute of Standards and Technology. A USA measurement standards laboratory, issuing the FIPS 140 Publication Series |
| OITSTE | Organization for the Security of Electronic Transaction https://oiste.org/ |
| PKI | Public Key Infrastructure https://en.wikipedia.org/wiki/Public_key_infrastructure |
| PKCS#11 | Public-Key Cryptographic Standards |
| ROT | Root of Trust. The foundation for cryptography. |
| RSA | Stands for Ron Rivest, Adi Shamir and Leonard Adleman: Initial of inventors of this Cryptographic Asymmetric Algorithm |
| SCP02 | GlobalPlatform Secure Channel Protocol 2 |
| SCP03 | GlobalPlatform Secure Channel Protocol 3 |
| SSL | Secure Sockets Layer. Secure transportation protocol replaced by TLS |
| TLS | Transport Layer Security. A secure transportation protocol |
| USB | Universal Serial Bus |
| VPN | Virtual Private Network |
| Windows CSP | Microsoft Smart Card Base Cryptographic Service Provider |

## References

http://www.schneider-electric.com

http://www.panasonic-electric-works.fr

http://fr.wikipedia.org/wiki/Automate_programmable_industriel

http://www.technologuepro.com

http://www.ewon.fr

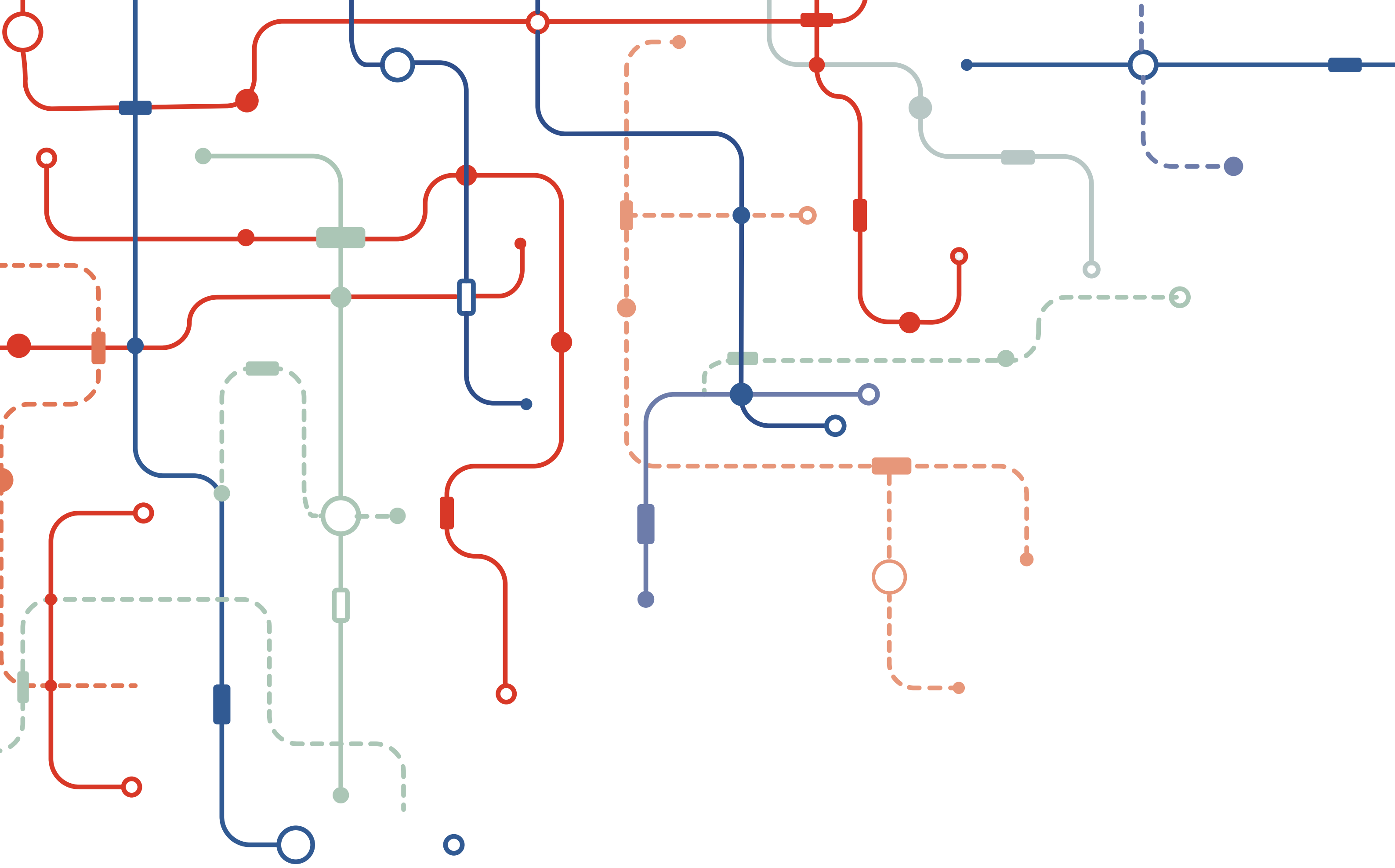
## Disclaimer

All products are sold subject to WISeKey Terms & Conditions of Sale and the provisions of any agreements made between WISeKey and the Customer. In ordering a product covered by this document the Customer agrees to be bound by those Terms & Conditions and agreements and nothing contained in this document constitutes or forms part of a contract (with the exception of the contents of this Notice). A copy of WISeKey's Terms & Conditions of Sale is available on request. Export of any WISeKey product outside of the EU may require an export License.

The information in this document is provided in connection with WISeKey products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of WISeKey products. EXCEPT AS SET FORTH IN WISEKEY'S TERMS AND CONDITIONS OF SALE, WISEKEY OR ITS SUPPLIERS OR LICENSORS ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL WISEKEY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, EXEMPLARY, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF REVENUE, BUSINESS INTERRUPTION, LOSS OF GOODWILL, OR LOSS OF INFORMATION OR DATA) NOTWITHSTANDING THE THEORY OF LIABILITY UNDER WHICH SAID DAMAGES ARE SOUGHT, INCLUDING BUT NOT LIMITED TO CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCTS LIABILITY, STRICT LIABILITY, STATUTORY LIABILITY OR OTHERWISE, EVEN IF WISEKEY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. WISeKey makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. WISeKey does not make any commitment to update the information contained herein. WISeKey advises its customers to obtain the latest version of device data sheets to verify, before placing orders, that the information being relied upon by the customer is current. WISeKey products are not intended, authorized, or warranted for use as critical components in life support devices, systems or applications, unless a specific written agreement pertaining to such intended use is executed between the manufacturer and WISeKey. Life support devices, systems or applications are devices, systems or applications that

(a) are intended for surgical implant to the body or (b) support or sustain life, and which defect or failure to perform can be reasonably expected to result in an injury to the user. A critical component is any component of a life support device, system or application which failure to perform can be reasonably expected to cause the failure of the life support device, system or application, or to affect its safety or effectiveness.

The security of any system in which the product is used will depend on the system's security as a whole. Where security or cryptography features are mentioned in this document this refers to features which are intended to increase the security of the product under normal use and in normal circumstances.



# Contact

## WISeKey SA

**WTC II**
**29, route de Pré-Bois • CP - 853**
**1215 Geneva • Switzerland**
Tel: + 41 (0)22 594 30 00
Fax: +41  (0) 22 594 30 01

## WISeKey Semiconductors

**Arteparc Bachasson • Bât A**
**Rue de la carrière de Bachasson**
**13590 Meyreuil • France**
Tel : +33 (0)4 42 370370
Fax : +33 (0)4 42 370 024

**www.wisekey.com**
***Stay connected with @WISeKey***