LEGIC

Whitepaper

Establishing Trust in the Industrial IoT - Security by Design

Anthony Fitze, Carl Fenger, LEGIC Identsystems

In industrial environments, mass deployment of sensors and the ability to securely collect and process data from fixed and mobile assets increases efficiency and enables better business decisions. It makes it easier to streamline processes, reduce errors, support auditing and enforce quality control.

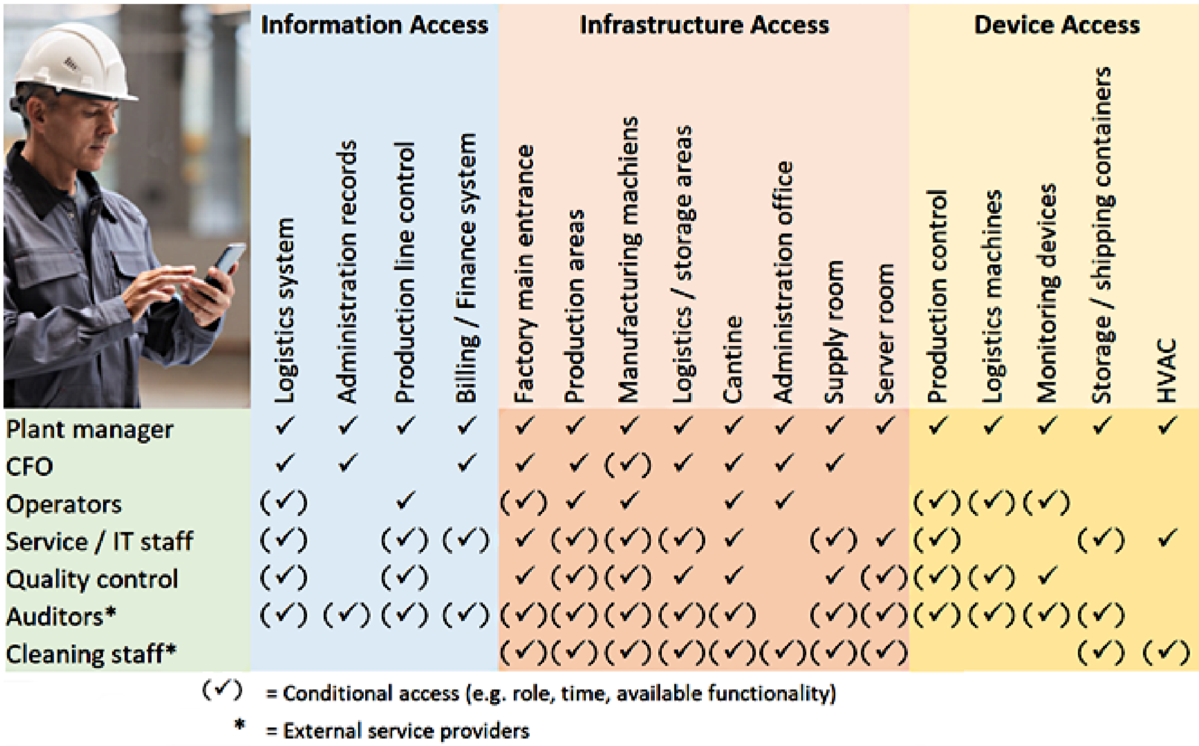
The common denominator: Trust

Connecting sensors to the internet is not enough. Improving processes via the "Industrial Internet of Things (IIoT)" depends on a common denominator: **Trust**. If users, sensors and their interactions cannot be trusted, the results can be costly and even catastrophic, especially where volatile assets and safety are involved, which is often the case.

The Three Pillars of Trust in the IIoT

Being able to trust in IIoT data relies on linking authenticated users with trusted sensors/objects so that their interactions are reliable, transparent and accountable. Accomplishing this relies on three principles:

1. **Accountability:** users must be authenticated and accountable before gaining access to sensors or infrastructure. Access permissions must be assigned based on roles, training and authorizations plus context-based criteria such as time and location. Permissions must be autonomously enforced, both **online** and **offline**, to minimize human error and support 24/7 operation. All activities must be transparent and auditable.



	Information Access				Infrastructure Access								Device Access				
	Logistics system	Administration records	Production line control	Billing / Finance system	Factory main entrance	Production areas	Manufacturing machiens	Logistics / storage areas	Cantine	Administration office	Supply room	Server room	Production control	Logistics machines	Monitoring devices	Storage / shipping containers	HVAC
Plant manager	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CFO	✓	✓		✓	✓	✓	(✓)	✓	✓	✓	✓						
Operators	(✓)		✓		(✓)	✓	✓		✓	✓			(✓)	(✓)	(✓)		
Service / IT staff	(✓)		(✓)	(✓)	✓	(✓)	(✓)	(✓)	✓		(✓)	✓	(✓)			(✓)	✓
Quality control	(✓)		(✓)		✓	(✓)	(✓)	✓	✓		✓	(✓)	(✓)	(✓)	✓		
Auditors*	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)		(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	
Cleaning staff*					(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)				(✓)	(✓)

(✓) = Conditional access (e.g. role, time, available functionality)

* = External service providers

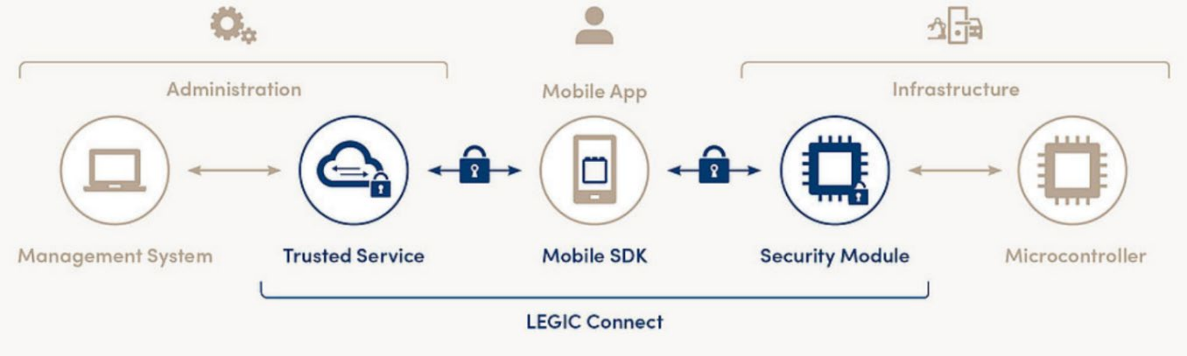
Trusted Users example: managing access to information, infrastructure and devices based on user credentials

2. **Security:** equipment must be configured and accessed by authorized users onsite. As sensors at the edge are the most vulnerable component of an IIoT system, physical hardware-level security must be implemented in the form of an embedded **Secure Element** for hosting of cryptographic keys and user permissions.

3. **Transparency:** all interactions between users and devices must be trustable, auditable and transparent to authenticated users. At the same time, they must not be visible to, nor subject to interception by unauthorized parties either at the sensor, along local area networks, air interfaces or over the public internet.

Security by Design: LEGIC Connect mobile credentialing platform for IIoT system users

LEGIC Connect is a mobile credentialing platform that securely distributes mobile credentials or other data to registered iOS or Android smartphones or tablets anytime, anywhere and instantly at the touch of a button.



The s

establishing trust and accountability in user/sensor /infrastructure interactions. The system can be easily integrated into existing infrastructure and applications, enabling service operators to manage user permissions and send/receive data securely from/to smartphones and sensors. For details see www.legic.com/connect

A secure gatekeeper at the IIoT edge

With a secure, end-to-end IIoT platform based on Mobile Credentialing, Managed Encryption and Secure Element technologies, accountability, security and transparency can be achieved. This is particularly relevant for

- Logistics automation:
  It ensures secure, transparent and auditable movement of goods within as well as between facilities by securing access and logging user/asset interactions.
- Building management:
  It links persons with a verified identity to enable trusted monitoring of building assets and interactions between users and doors, HVAC systems, security and fire systems, etc.
- Industrial equipment:
  It authenticates persons and enables secure dynamic permissioning to ensure trusted interactions with equipment and infrastructure. Protocolled usage data can be collected per user. Updating of permissions can be performed in real-time and over-the-air.

Introducing Mobile Credentialing in the IIoT

The LEGIC XDK Secure Sensor development Evaluation Kit is a universal programmable sensor device & prototyping platform for developing trusted IoT applications based on Mobile Credentialing. It enables secure sensor configuration and readout via mobile devices which can also be configured in real-time from the cloud. With 8 MEMs sensors, built-in Secure Element for storage of cryptographic keys/whitelists and RFID/NFC/Bluetooth/Wi-Fi communications, it enables rapid prototyping of secure, touchless, sensor based IoT applications.

For more details visit: www.legic.com/iot or email info@legic.com

*LEGIC will be exhibiting at: **IoT Solutions World Congress** in Barcelona 31. Jan – 2. Feb 2023 Gran Via Venue Hall 4 / F671 and*
***ISC West** in Las Vegas 29 – 31 March 2023 Booth 2045*