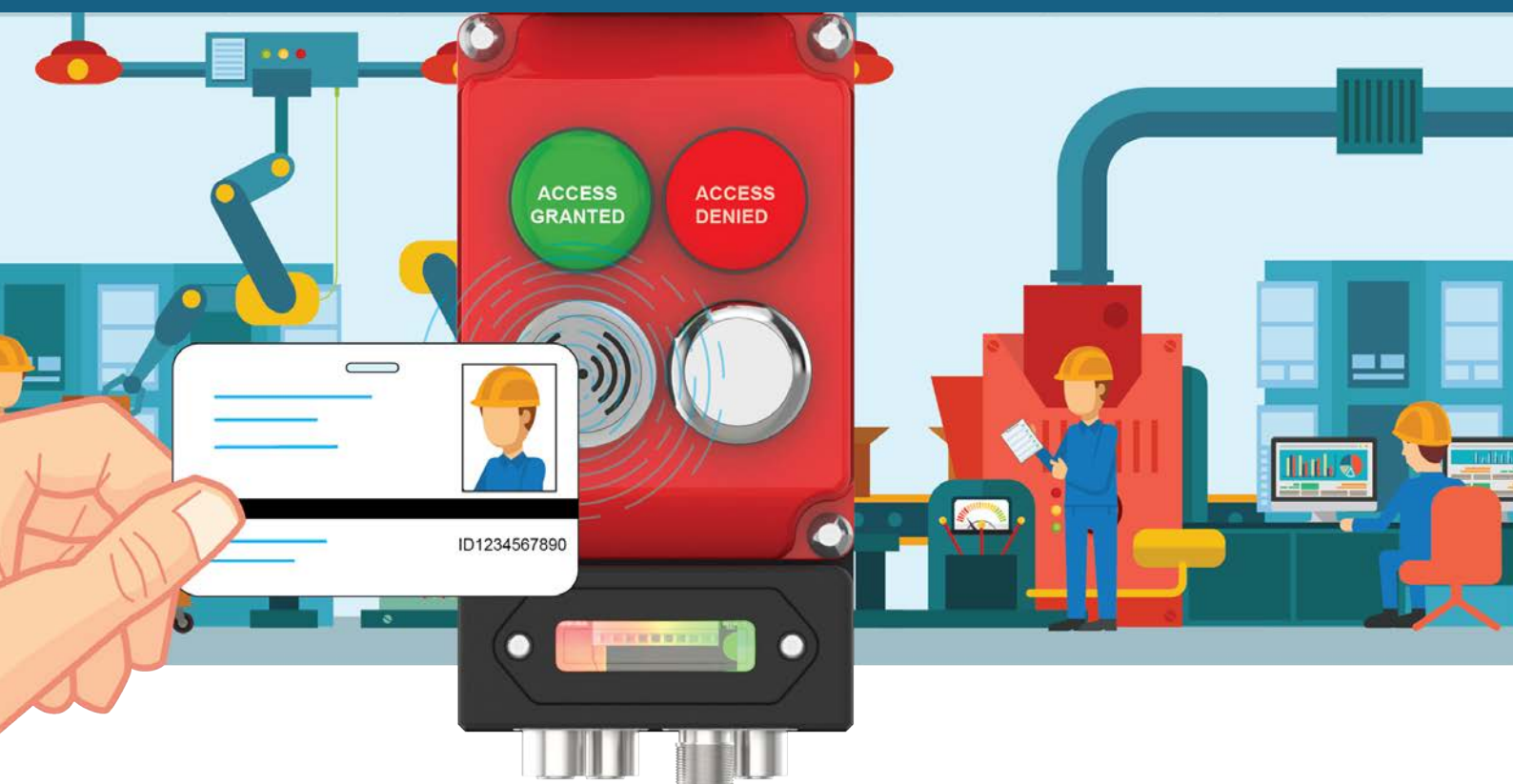


Industrial Access Control



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2018



C

US








Introduction to Fortress:

Fortress designs and manufactures customised safety equipment, protecting lives in hazardous workplaces. Our reputation is as a global provider of robust safety specifications for manufacturing environments.

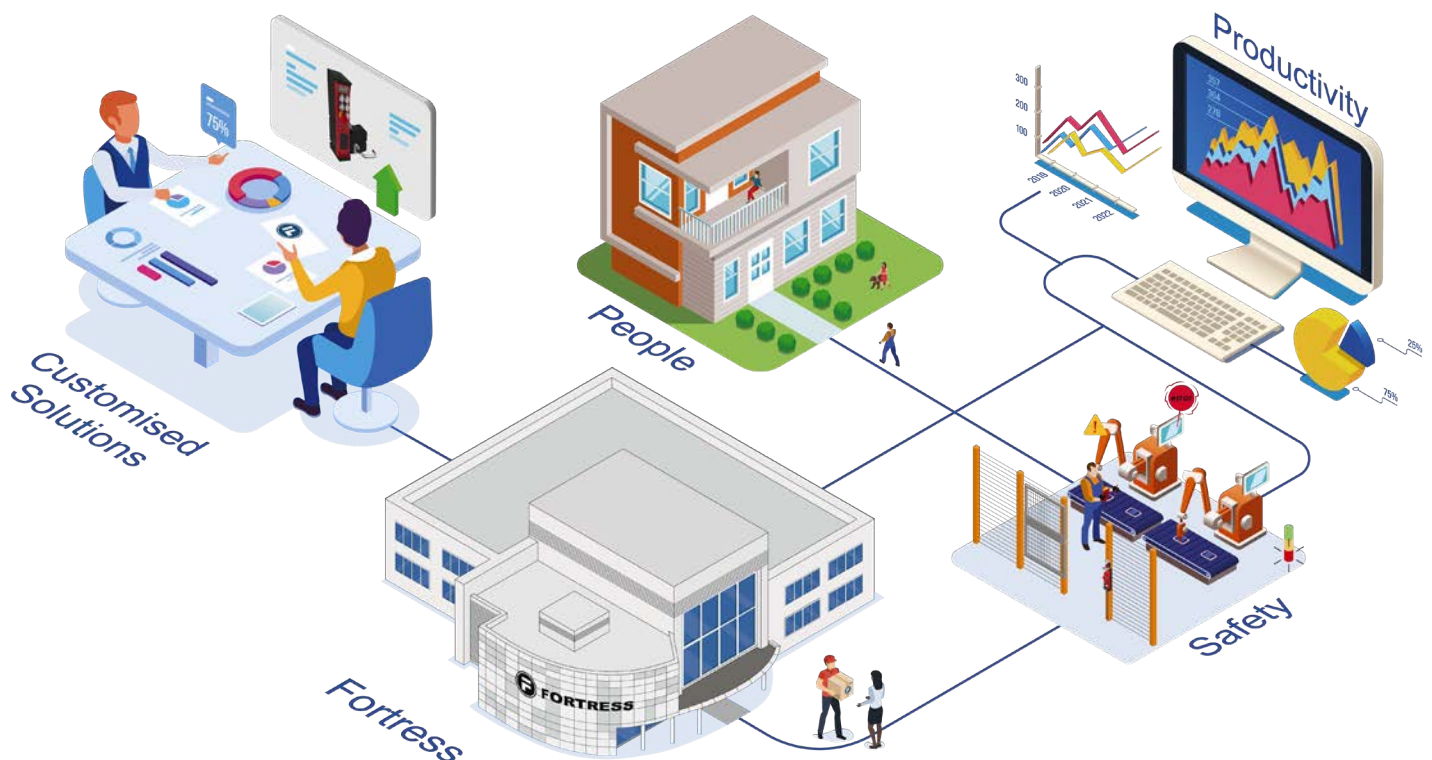
Over the last 40 years, Fortress has become well known in the industry for innovative design, robust engineering and reliability. Headquarters are in Wolverhampton (UK), with supporting offices and manufacturing facilities in the USA, Netherlands, Australia and China, further supported by a global network of trusted distributors and channel partners.

Fortress' current product portfolio includes:

-  **mGard** - The only range of mechanical interlocks independently certified to PLe
-  **amGardpro** - Heavy duty safety gate switches with connectivity and trapped key integration certified to PLe
-  **amGardS40** - Stainless steel IP69K safety gate switches independently certified to PLe
-  **tGard** - Medium duty interlocks with configurable built-in control functionality independently certified to PLd
-  **ncGard** - A range of safety switches with non-contact technology



Saving lives by providing the best safety solutions



Introduction to FRANK

Fortress RFID Access Network Keys

Interlocks control when you can access equipment safely, FRANK controls who can access equipment safely.

By integrating readers to suit the existing site RFID access cards into a Fortress device and providing a software based access approval control system; FRANK can be integrated into automation systems with simple input/outputs to a PLC.

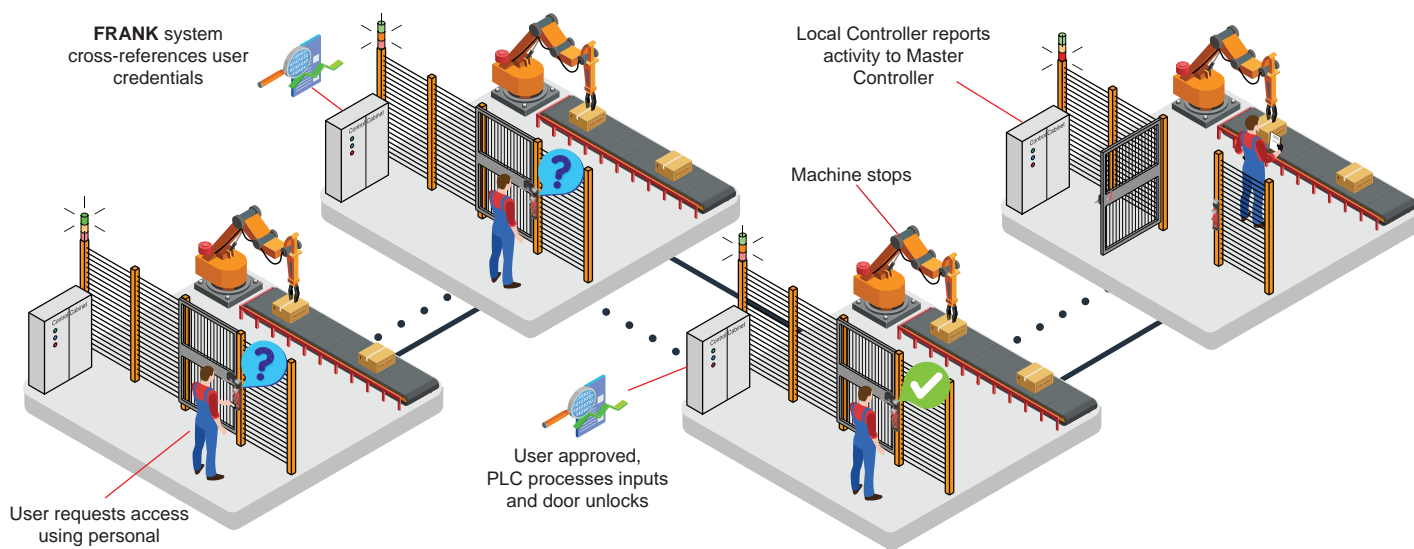
Data of who, when and where from access events is collated to a central point within facilities to allow for viewable events lists and data insights that can support efficiency analysis.

Fortress supports common card types including:

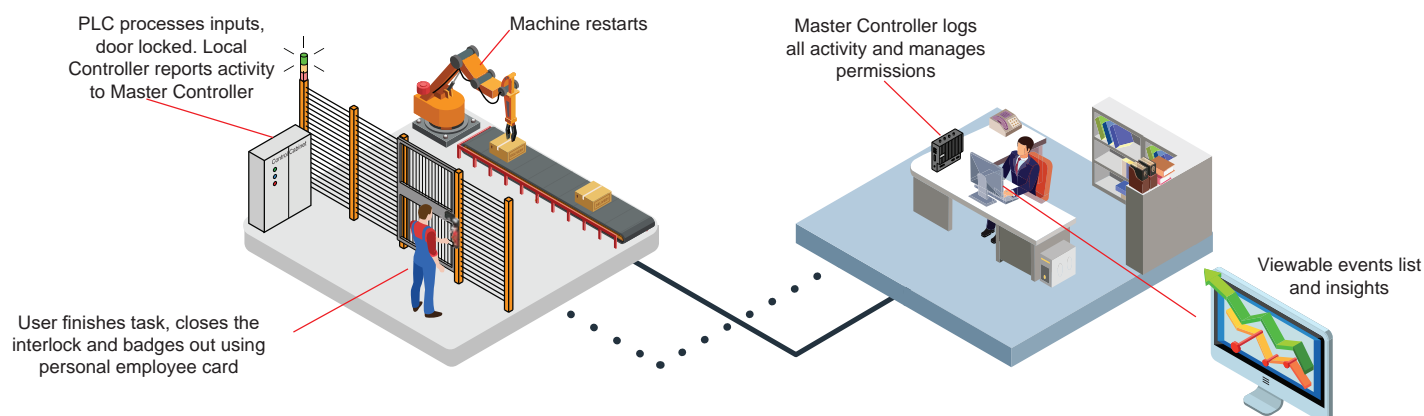
- 13.56MHz ISO 15693
- 13.56MHz With Manufacturer's Specific Protocol
- 13.56MHz ISO 14443A
- 125kHz With Manufacturer's Specific Protocol



Control Access



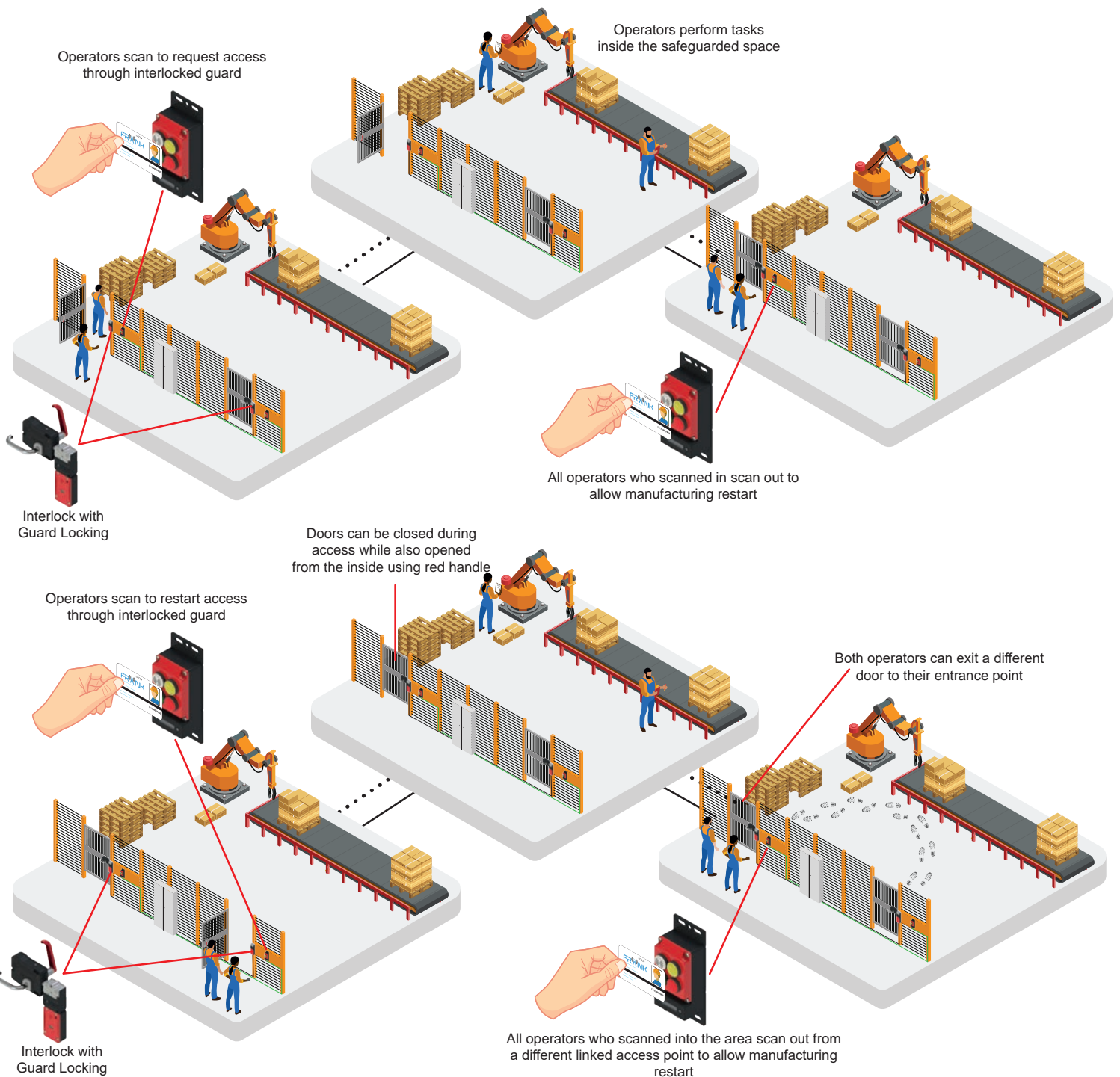
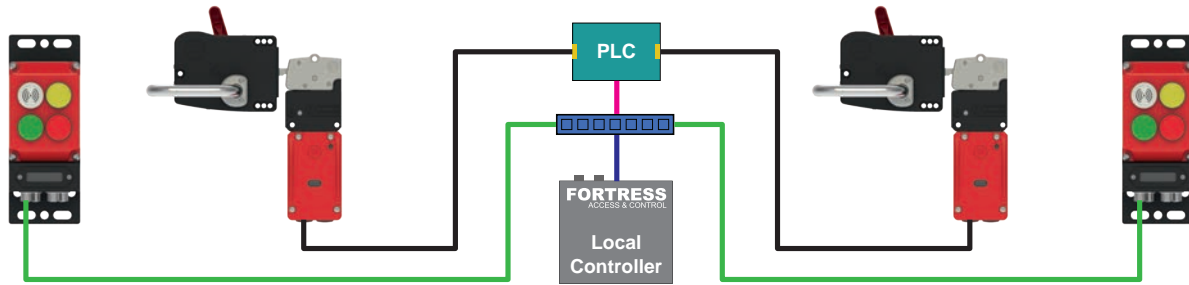
Manage Productivity



Access Control To Large Robotic Handling System

Application Requirement:

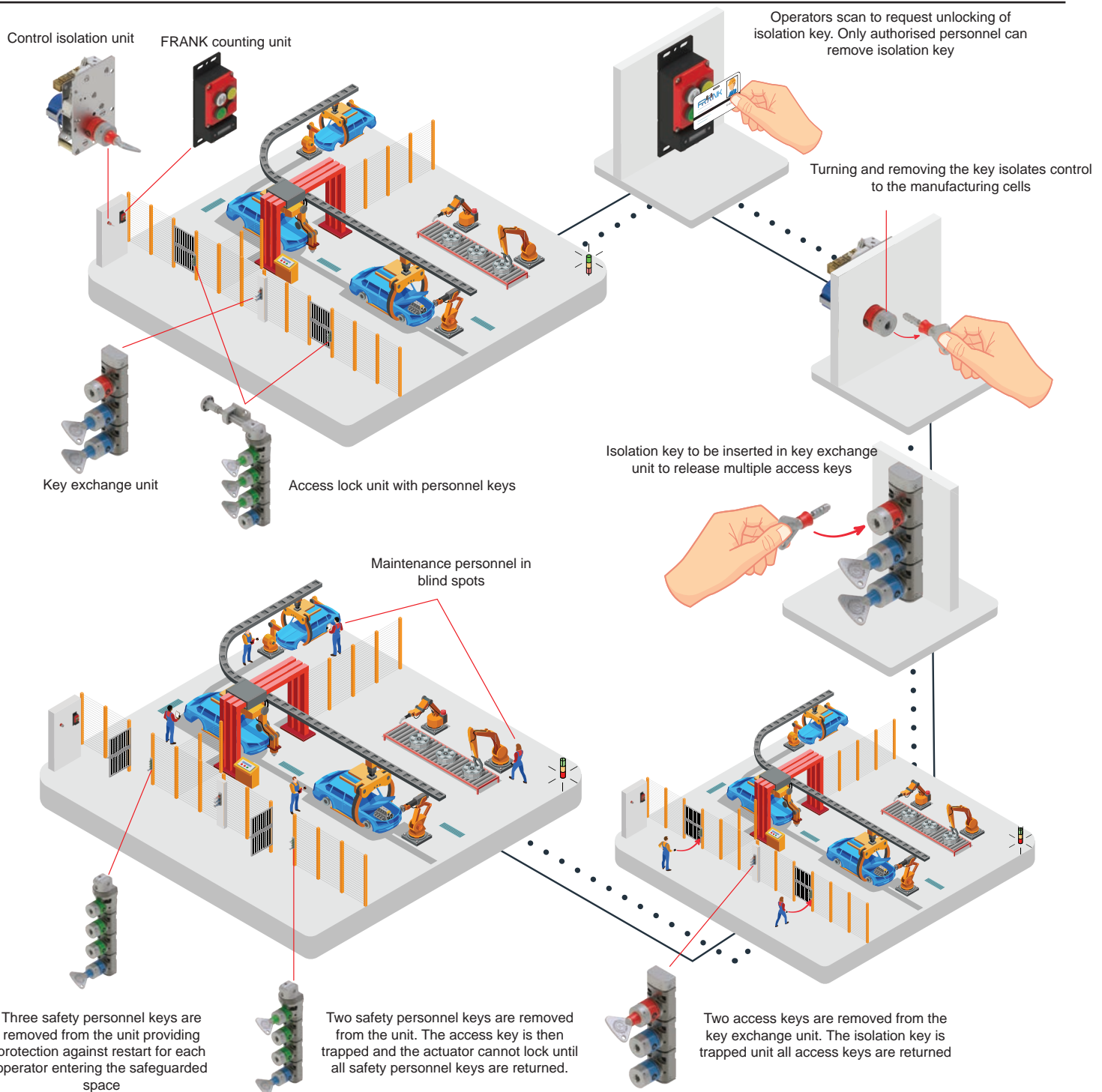
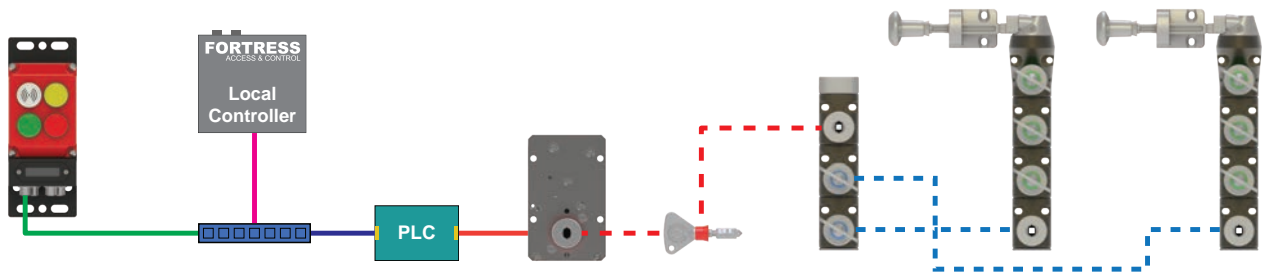
Control access to a large automated area with multiple doors and existing safety system. In addition, employees are permitted to record their entry through one door and exit through another door to the area. Once all employees have signalled they are outside the guarding, the FRANK system reports the area is empty to the PLC and the reset procedure can be undertaken.



Access Control To Component Transfer Line

Application Requirement:

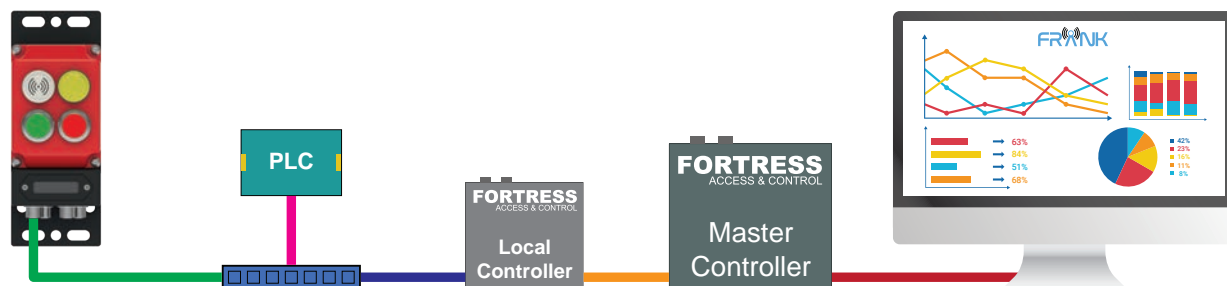
The existing trapped key system fitted in this scenario allows access only when the control system is isolated by a solenoid controlled trapped key device. Door interlocks release 3 personnel keys to prevent restart while operators enter the safeguarded space. RFID badges are used to restrict the start of the trapped key sequence to trained operators.



Brick Manufacturing - Quality Inspection

Application Requirement:

Every hour during brick production, a sample brick must be extracted from the process and tested to ensure the correct clay conditions. The FRANK system automates the record keeping of the brick acceptance/rejection to provide management reporting. Outputs from the FRANK unit can be fed into the machine control system to restart the manufacturing process.



Extracted key system forces personnel key to be carried inside whilst operator collects a brick sample

Interlock closed after brick sample is collected

Operator checks brick

Operator scans to accept / reject brick via pushbuttons

Master controller logs all quality control data

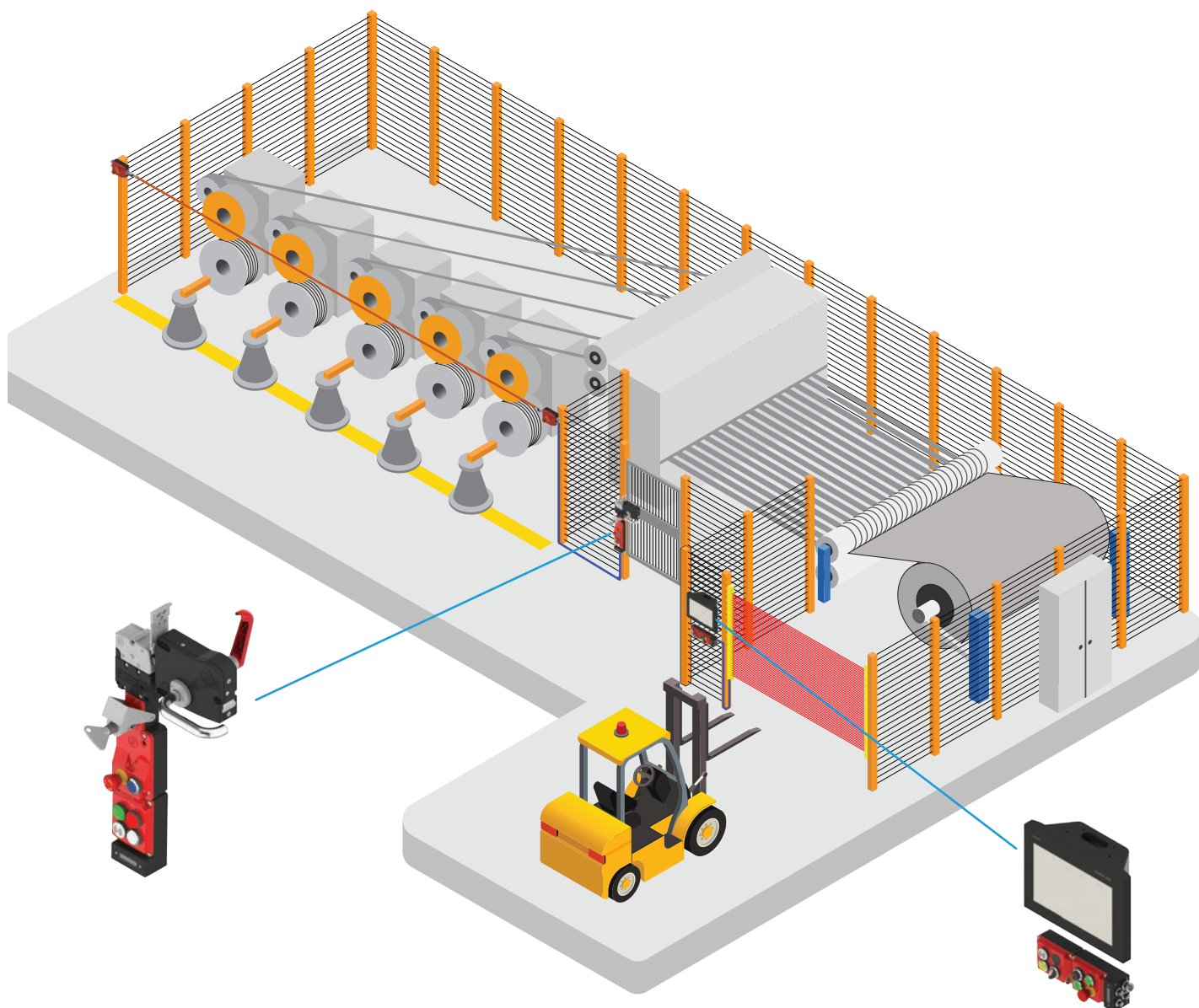
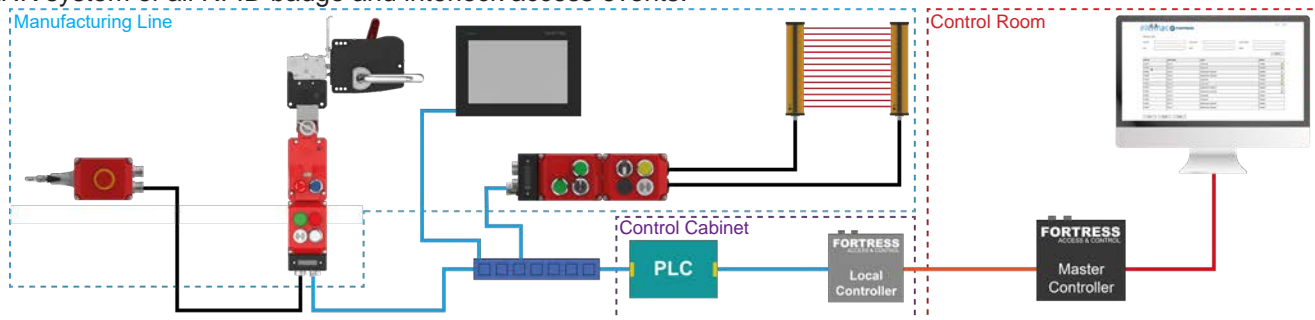
Viewable events list and process audit reports can be generated

FRANK verification unit

Slitting Line Access Control

Application Requirement:

Access to hazardous areas of the slitting line is safeguarded by guard locking devices with the request to enter performed by an authorised employee presenting their RFID badge to the interlock. The FRANK system additionally provides access via RFID badges to the line side HMI restricting process change to only approved employees. Data is collected within the FRANK system of all RFID badge and interlock access events.



FRANK Standard Device Configurations

Counting POD

Standalone RFID reader for integrating badge authentication in PROFINET or EtherNet/IP control networks as an option alongside interlocks.

Preconfigured with indicator lamps to signify 'Access Granted', 'Access Denied' and 'Cell Empty'.

The yellow indicator lamp is included to be programmed to illuminate upon receiving confirmation from the FRANK system that all operators have presented their badge upon exit of the area.



FRANK Interlock

RFID badge reader to suit card type integrated into solenoid controlled interlock.

Single Action Escape Release Handle & Emergency Stop included in configuration as standard.

Available for PROFINET/PROFIsafe or EtherNet/IP with CIP safety networks.



Verification POD

RFID reader configured alongside pushbutton control elements to be used as a supporting device to a quality inspection system.

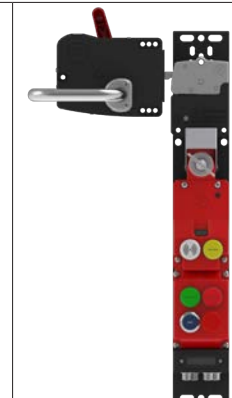
Pushbuttons can be programmed to become active to restart the process only after an authorised operator has conformed the process status.



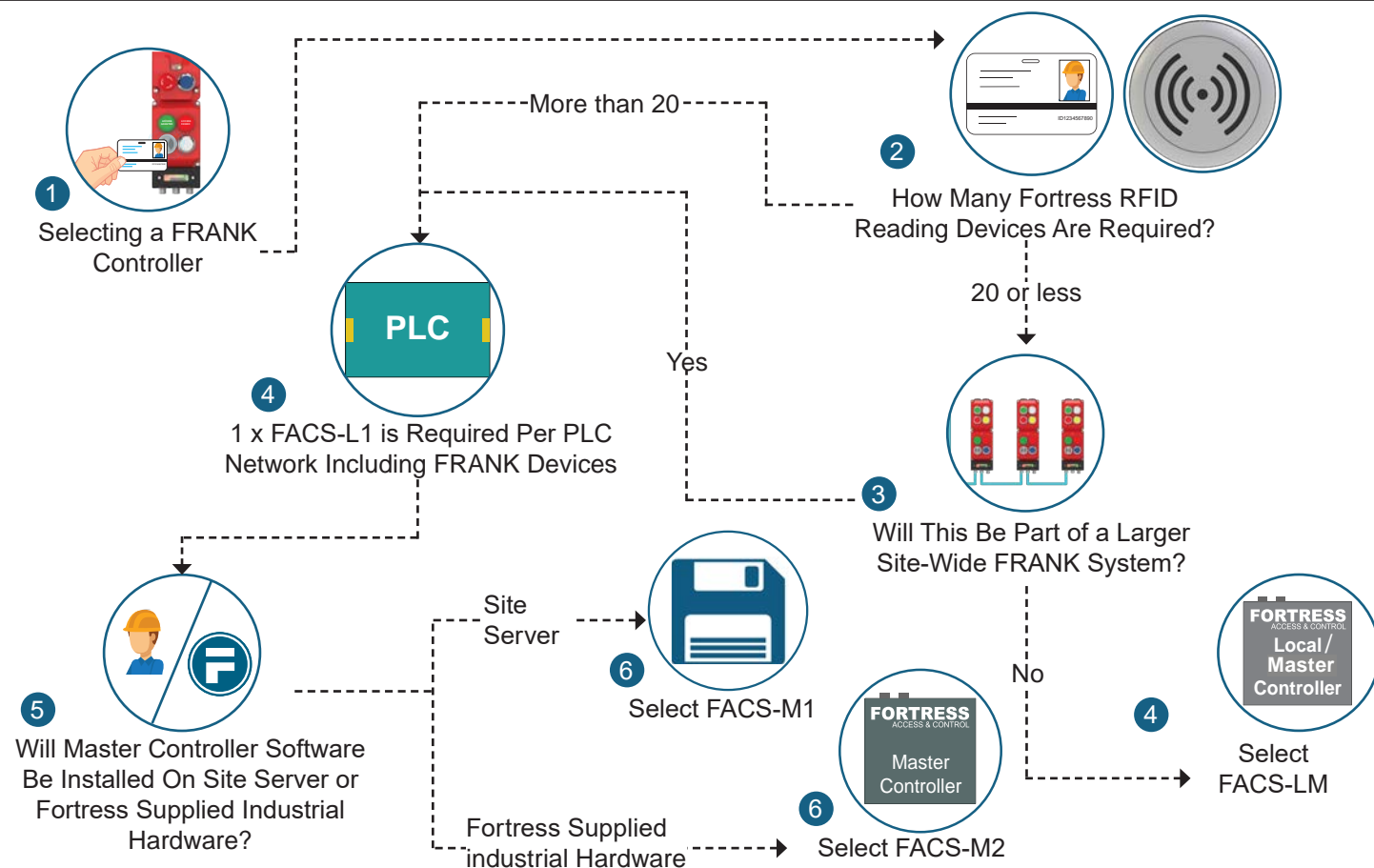
FRANK Interlock with Extracted Key

Interlock with RFID reader integration configuration including forced extracted key mechanism.

Operators are required to remove the personnel key from the lock before the guard will open. Guard is prevented from being closed while operator retains the key.



Selecting a FRANK Controller



Programming A FRANK System

Control System Inputs

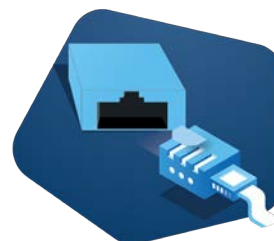
The Fortress Access Control System is designed to be programmed as simple inputs to Fortress amGardpro proNet devices. These additional inputs are shown below. For safe, unsafe, and other extended IO inputs possible in the proNet range please see alternative Fortress documentation.

Description		Bits							
		0	1	2	3	4	5	6	7
RFID									
7-14 Bytes	RFID LSB First (Reserved)								
Access Control Inputs									
Byte 0		Error	Access Granted	Access Denied	Cell Empty	-	-	-	-
Byte 1	Additional Permissions*	Additional Permission Bit 0	Additional Permission Bit 1	Additional Permission Bit 2	Additional Permission Bit 3	Additional Permission Bit 4	Additional Permission Bit 5	Additional Permission Bit 6	Additional Permission Bit 7
Access Control Outputs									
Byte 0		Reset							
<p>Access control bits will pulse high for 100ms as determined by the access control system. If a user is permitted to unlock the interlock, Access Granted will pulse high. If a user is not permitted to unlock the interlock, Access Denied will pulse high. When the interlock is relocked, Cell Empty will pulse high.</p> <p>Error Bit 0 will go high if unit is disconnected from a Local Controller.</p> <p>*Additional permissions are set in the system software as a whole byte, giving 256 possible additional permissions. Alternatively, individual bits could be used.</p>									

FRANK Software Setup

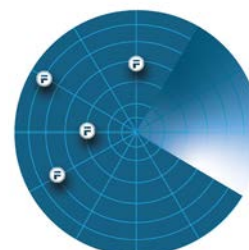
Step 1. Install

Install Fortress devices and establish communication with the PLC



Step 2. Auto Discover

Auto-discover Fortress devices on the FRANK Local Access Controller



Step 3. Import

Configure of Master Access Controller Software. Import Users and Card Details



Industrial Access Control

A **Halma** company

