Protecting People, Protecting Productivity

Industrial Access Control
Access Control at the Interlock with FRANK

The FRANK Industrial Access Control Solution:

• Prevents unauthorised access and unauthorised line shut down.
• Simple installation and integration to a network, using your existing ID cards.
• Easy management of access permissions.

How it Works:

System Network

- Switch
- PLC
- Local Controller

FRANK Enabled Unit

Event Logging and Insights

- Unit Network Connection
- Master/Local Link

Fortress www.fortressinterlocks.com
Prevents Unauthorised Shut Down & Maintenance

Unauthorised access to manufacturing areas can cause unnecessary machine downtime. Enforcing training plans reduces risk to valuable equipment.

Cell access is often uncontrolled allowing anyone to request to enter. Mechanical access keys require management.

**FRANK** ensures locations are only accessed by authorised personnel, protecting uptime in manufacturing. Existing ID cards can be utilised.

Productivity Insights

Without recording event information, identifying root cause and corrective actions is problematic.

It can be difficult to understand who accessed a controlled area and how long was spent resolving issues.

The **FRANK** software logs all access events. This allows reviews of time spent and enables productivity analysis. This can contribute to wider predictive maintenance.

**FRANK** can also be used to monitor other environments such as inspection areas when an audit trail is desired.

Simple Integration

Access control systems can be difficult to integrate into industrial environments and interlock safety systems.

External readers are often less robust for industrial environments, requiring additional wiring, and interfaces between the IT network or extensive reprogramming of the PLC.

With the reader integrated into the interlock, **FRANK** manages permissions through an industrial controller and then delivers simple inputs to the PLC, just like a pushbutton. Negating IT interfaces or complex system integration.
System Overview

Configurable Form Factors
The FRANK RFID module can be located in any available slot, delivering all the configurability of a regular pushbutton. User can specify card type (e.g. 125 Hz), to use existing ID cards and design outputs to visualise that access has been granted.

Monitor a Range of Environments
As well as monitoring the entrance and exit at a cell, FRANK modules can monitor for identification at any point of your process. Simple inputs to the PLC mean that access to a HMI can be granted or inspections can be tracked by associating users with button presses.

Without Compromising Safety
FRANK is separate from the safety inputs of the interlock. Using non-safety inputs to the PLC, just like a pushbutton. FRANK based procedures can be paired with Fortress’ extracted key or other lock out tag out solutions when specified.

Control Access

Manage Productivity

PLC processes inputs, door locked. Local Controller reports activity to Master Controller

Machine restarts

Master Controller logs all activity and manages permissions

Viewable events list and insights

User finishes task, closes the interlock and badges out using personal employee card

User requests access using personal employee card

User approved, PLC processes inputs and door unlocks

Local Controller reports activity to Master Controller

Machine stops
Implementation

Topology

Local controller provides robustness and line-side communication
Master controller syncs local controllers for central management

Bit Input Mapping

<table>
<thead>
<tr>
<th>Description</th>
<th>Bits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Non-Safe Inputs</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Byte 0</th>
<th>Bit is set when switch is pressed</th>
<th>[Button / Switch]</th>
<th>[Button / Switch]</th>
<th>[Button / Switch]</th>
<th>-</th>
<th>-</th>
<th>-</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte 1 to 4</td>
<td>Reserved</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Byte 5</td>
<td>Bit is set when tongue is removed from head</td>
<td>Head Monitor</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Byte 6</td>
<td>Bit is set when gate is unlocked</td>
<td>Solenoid Monitor</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Byte 7 to 14</td>
<td>Reserved</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Byte 15</td>
<td>Access Control</td>
<td>-</td>
<td>Access Granted</td>
<td>Access Denied</td>
<td>Cell Empty</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Byte 16</td>
<td>Additional Permissions</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Access control bits will pulse high for 100ms. If a user is authorised, Access Granted will pulse high. If a user is unauthorised, Access Denied will pulse high. When all users have badged out, Cell Empty will pulse high. Additional permissions can be set for custom inputs such as ‘teach mode’.

For more information please email us at FRANK@fortressinterlocks.com

Or visit www.fortressinterlocks.com