# TN2155004

# Two-Factor Authentication for Industrial Control Systems

Author: Emanuel Oliveira

## 1 INTRODUCTION

Two-factor authentication (2FA), or more generically, multi-factor authentication (MFA), has proven to be an effective method to prevent unauthorised access to a given system.

However, in Industrial Control Systems, 2FA is not a usual approach, leaving the systems exposed to only the traditional user and password authentication method.

This document specifies the required hardware and describes the implementation methodology to implement a 2FA system in any industrial equipment or system. However, it is assumed that one authentication method is the usual username and password entered via some form of user interface (e.g. graphical console or SCADA).

## 2 HARDWARE SETUP

The additional authentication is achieved using a coded key fob.

There is a multitude of hardware solutions in the market for coded key fobs and respective readers. The suitability of each solution should be assessed against the project requirements.

The selected device is the **Operating Mode Selector** PIT m3.2p from Pilz, shown in Figure 1. This device provides two types of signals: safety outputs connected to a **Safety Controller** and a set of inputs and outputs intended to be connected to a controller (a **PLC** in this case) to exchange data regarding the key fob and user selection.


*Figure 1: Pilz PIT m3.2p Operating Mode Selector*

The user interface is provided by a graphical console (**H**uman **M**achine **I**nterface) or a **S**upervisory **C**ontrol **a**nd **D**ata **A**cquisition. HMI or SCADA should have embedded user authentication functionalities. From this point on, the user interface will be referred to as HMI.

## 3 IMPLEMENTATION

The activation of the actuator[1] will require the safety contactors to be energised (closed). For that, two events must happen:

- a key fob must be inserted, which will activate the (hardwired) safety signal to the Safety Controller, and
- a Reset signal is issued to the Safety Controller.

The activation of the Reset signal is performed by the PLC[2] using a hardwired signal to the Safety Controller or using the Fieldbus connection if the latter supports it.

[1] Depicted as a motor in Figure 2.
[2] Having a Reset signal being triggered by a physical pushbutton connected directly to the Safety Controller is not suitable for the 2FA functionality.

For the PLC to activate the Reset signal, logic must be in place to ensure that the user has logged in and the key fob that was associated with that user is inserted. The association between the user (and his credentials) and the key fob ID constitutes the 2FA functionality.

Figure 2 depicts an overview of the interconnections between the devices identified in the previous section and the functionality described above.

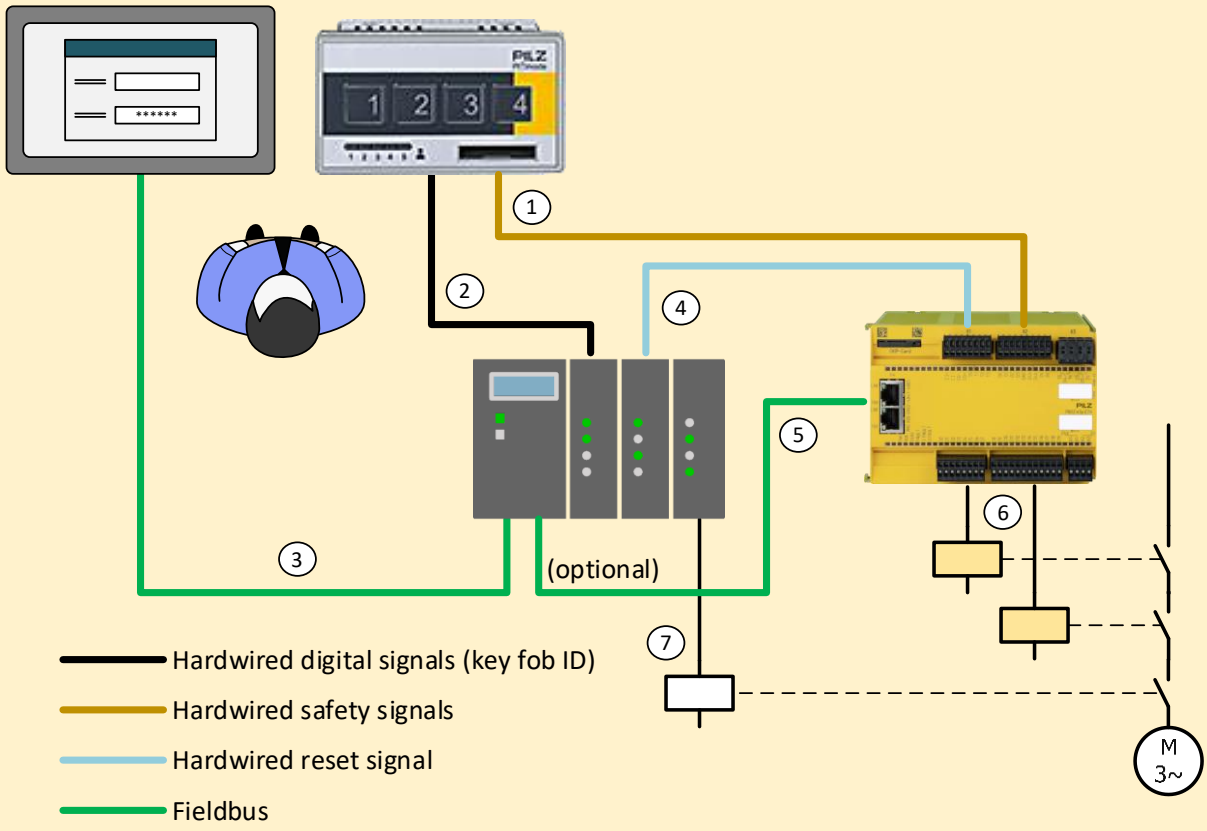


*Figure 2: Overview diagram*

The table below details the functionalities associated with each connection.

*Table 1: Connections*

| Connection | Description |
|---|---|
| 1 | The safety signal will only be active if a key fob is inserted in the Operating Mode Selector. |
| 2 | The Operating Mode Selector transmits the key fob ID to the PLC, which will then relay that information to the HMI (see connection 3). |
| 3 | The HMI retrieves the key fob ID is collected by, or the SCADA sends the user ID to the PLC, depending on the selected approach for the user – key fob association (see Section 3.2). |
| 4 | The Reset signal is activated by the PLC only when a logged-in user with the assigned key fob inserted issues a reset command. |
| 5 | Same as connection 4, but using a Fieldbus connection between the PLC and the Safety Controller. |
| 6 | The Safety contactors will be energised if a key fob is inserted and after the reset command is received. |
| 7 | The control signal to the actuator is activated by the user using the HMI or any trigger signal connected to the PLC; for additional security, this control signal can be subjected to the same constraints as the Reset signal (see connection 4). |

### 3.1 User Credentials

User credentials management must be an embedded functionality in the PLC/SCADA. Implementing credentials management using any scripting functionality should be avoided unless there are means to store credentials securely.

### 3.2 Key fob Assignment

The association between the key fob and a user is the key aspect in implementing the 2FA.

The association between users and key fobs is no more than a two-dimensional array with users' IDs and key fobs' IDs, referred from now on as IDs Lookup Table.

The current used ID and key fob ID reported by the Operating Mode Selector will then be compared against the IDs Lookup Table's information to assess if the current user has the assigned key fob in the system. This functionality can be implemented in the PLC or HMI.

The PLC implementation requires information about the logged-in user to be sent from the HMI to the PLC. The PLC, which contains the IDs lookup Table, will then assess if the assigned key fob ID reported by the Operating Mode Selector matches the key fob ID in the two-dimensional array.

The HMI implementation requires the key fob ID reported by the Operating Mode Selector to be made available by the PLC to the HMI. The HMI, which holds the IDs lookup table, verifies if the logged-in user has the right key fob inserted in the system.

The HMI should contain functionality to edit the IDs Lookup Table restricted to a user with higher privileges.

**NOTES**:

www.hardpath.co.uk