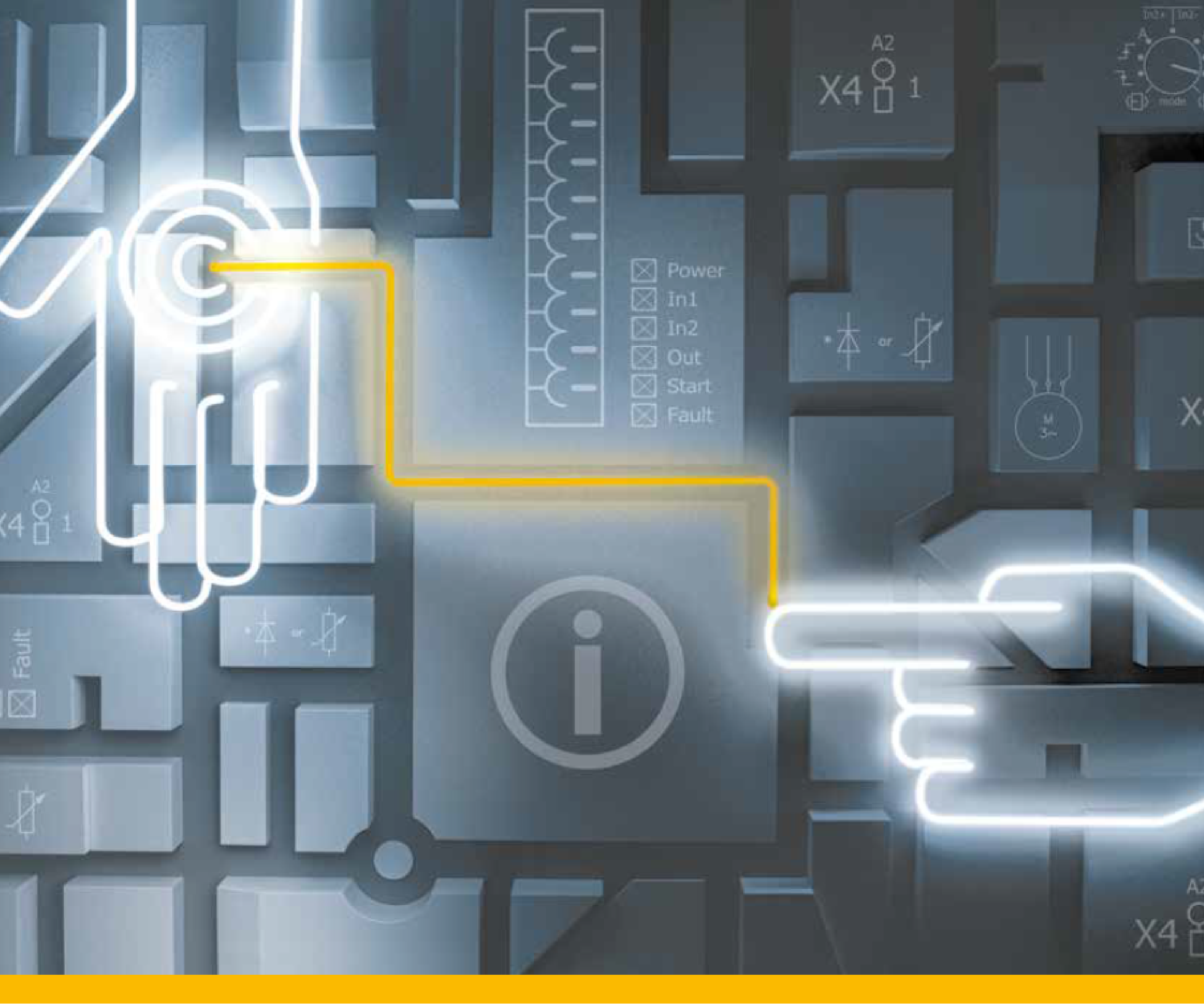


Maintenance safeguarding system Key-in-Pocket

THE SPIRIT OF SAFETY

System Description-1006613-EN-02

- Control and signal devices

This document is the original document.

Where unavoidable, for reasons of readability, the masculine form has been selected when formulating this document. We do assure you that all persons are regarded without discrimination and on an equal basis.

SD means Secure Digital

1 Introduction

1.1 Definition of symbols

Information that is particularly important is identified as follows:

DANGER!

This warning must be heeded! It warns of a hazardous situation that poses an immediate threat of serious injury and death and indicates preventive measures that can be taken.

WARNING!

This warning must be heeded! It warns of a hazardous situation that could lead to serious injury and death and indicates preventive measures that can be taken.

CAUTION!

This refers to a hazard that can lead to a less serious or minor injury plus material damage, and also provides information on preventive measures that can be taken.

NOTICE

This describes a situation in which the product or devices could be damaged and also provides information on preventive measures that can be taken. It also highlights areas within the text that are of particular importance.

INFORMATION

This gives advice on applications and provides information on special features.

2 Overview of the maintenance safeguarding system Key-in-Pocket

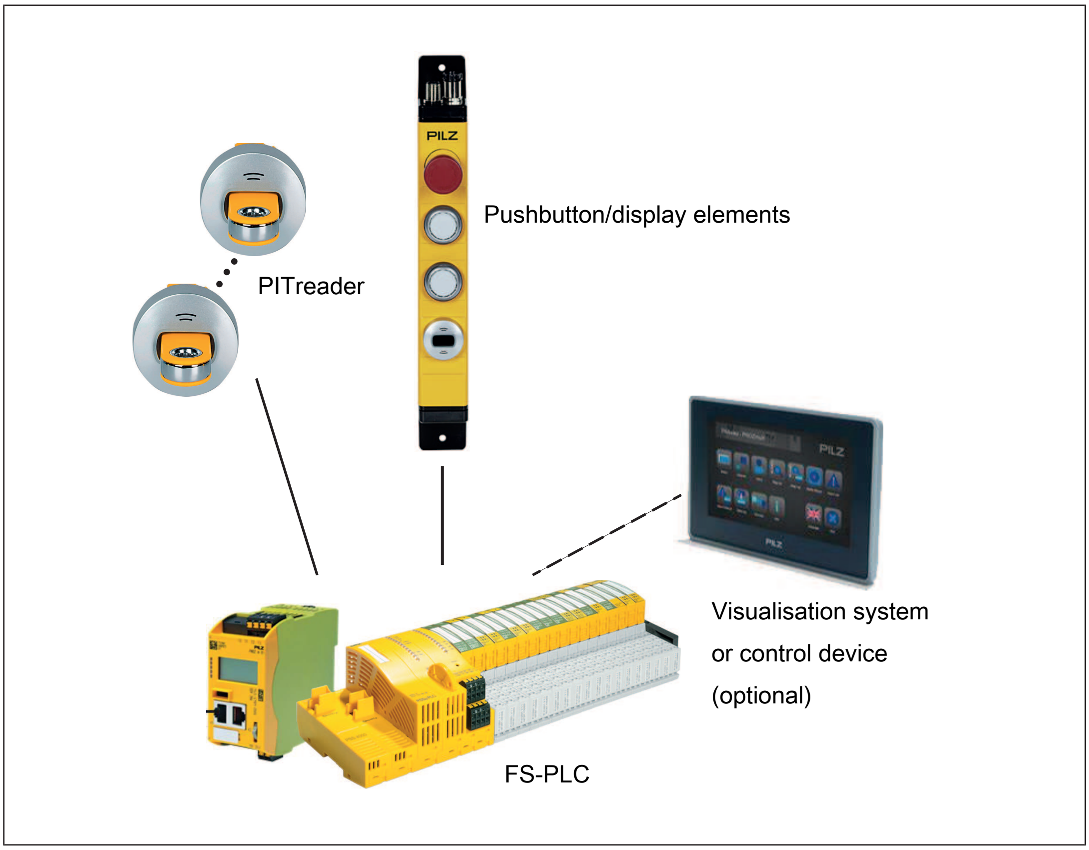


Fig.: Overview of the components in the maintenance safeguarding system "Key-in-Pocket"

On a plant in which the danger zone is accessible via safety gates, "Key-in-Pocket" is a system that guarantees that the plant cannot (re-)start until the last person has left the danger zone. For example, the Key-in-Pocket system can be used for access control when making modifications and carrying out repair and maintenance work. Each person who accesses the danger zone has to sign in to the Key-in-Pocket system’s internal sign in list. When leaving the danger zone, each person must sign out of the internal sign in list. People sign in and out via transponders belonging to the authentication system PITreader from Pilz (see PITreader operating manual).

If necessary, blind spots can be checked inside a plant (blind spot check). A blind spot is a point inside a plant that cannot be seen from the outside from any access point and control station. During a blind spot check, confirmation must be provided inside the plant that there is nobody left in the danger zone

The elements/blocks of the Key-in-Pocket system are suitable for plants that are accessible via safety gates and on which the voltage supply to the control system is not shut down in normal mode or production mode.

A Key-in-Pocket system can manage the safety gates of several access points. An access point consists of a safety gate on which a PITreader is attached externally, including a pushbutton for signing in and out.

Hardware and software components of the Key-in-Pocket system:

- Components via which the plant can be accessed from the outside, per access point:
  - Authentication system PITreader from Pilz
  - Pushbutton for signing in and out on the Key-in-Pocket system
  - Display element for showing the sign in status
- Optional: Components that are in the danger zone or can be used from there (gate with guard locking device)
  - Authentication system PITreader from Pilz
  - Display element for showing the sign in status
- Optional: Components to confirm that nobody is left within the plant, if there are blind spots (blind spot check).

  Components per blind spot check:
  - Authentication system PITreader from Pilz
  - Pushbutton for confirming that the blind spot check has been carried out
  - Display element, which indicates that the system is ready to carry out the blind spot check
- Safety controller to evaluate access control and activate/deactivate the (re)start interlock, e.g. PNOZmulti or safe controller from the automation system PSS 4000
- Elements/components from Pilz
- Additional components for guard locking and monitoring of safety gates, including control and display elements

3 Safety

3.1 Intended use

The Key-in-Pocket system may be used on plants that are accessible via gates. With the Key-in-Pocket system it is possible to guarantee that the plant cannot (re)start until the last person has left the plant. People must sign in and out via transponders belonging to the authentication system PITreader from Pilz.

The Key-in-Pocket system is **not** suitable for applications in which power is removed to the safety controller or parts of the safety or identification systems.

When gate guard locking devices are used on accessible access points, the guard locking device must have an escape release function (e.g. Pilz PSENmlock with escape release).

When a Key-in-Pocket system is used with a safety controller PNOZmulti, up to 4 access points can be managed.

When a Key-in-Pocket system is used with a safety controller from the automation system PSS 4000, up to 10 access points can be managed.

The following PITreader devices may be used:

- PITreader Key
- PITreader Card
- PIT gb with PITreader

The system can be used for applications in accordance with

- EN ISO 13849-1: up to Cat 3, PL d
- IEC EN 61508-3: up to SIL 2
- IEC EN 62061: up to SIL 2

3.2 Safety regulations

3.2.1 Additional documents that apply

Read and refer to the following documents for the Key-in-Pocket system with PNOZmulti:

- Operating manual PITreader, operating manual PIT gb RLLE y ETH
- Operating manuals for the PNOZmulti devices you are using
- PNOZmulti Configurator Online Help

Read and refer to the following documents for the Key-in-Pocket system with PSS 4000:

- Operating manual PITreader, operating manual PIT gb RLLE y ETH
- Operating manuals for the modules you are using
- PAS4000 Online Help

3.2.2 Use of qualified personnel

The products may only be assembled, installed, programmed, commissioned, operated, maintained and decommissioned by persons who are competent to do so.

A competent person is a qualified and knowledgeable person who, because of their training, experience and current professional activity, has the specialist knowledge required. To be able to inspect, assess and operate devices, systems and machines, the person has to be informed of the state of the art and the applicable national, European and international laws, directives and standards.

It is the company's responsibility only to employ personnel who

- Are familiar with the basic regulations concerning health and safety / accident prevention,
- Have read and understood the information provided in the section entitled Safety
- Have a good knowledge of the generic and specialist standards applicable to the specific application.

3.2.3 Warranty and liability

All claims to warranty and liability will be rendered invalid if

- The product was used contrary to the purpose for which it is intended,
- Damage can be attributed to not having followed the guidelines in the manual,
- Operating personnel are not suitably qualified,
- Any type of modification has been made (e.g. exchanging components on the PCB boards, soldering work etc.).

3.2.4 Disposal

- When decommissioning, please comply with local regulations regarding the disposal of electronic devices (e.g. Electrical and Electronic Equipment Act).

3.3 Application conditions

Requirements for the safe use of the Key-in-Pocket system

The system architect, system integrator and/or operator must ensure that the following requirements for the safe use of the Key-in-Pocket system are met.

WARNING!

Potential loss of safety function due to improper use!

The Key-in-Pocket system is not suitable for applications in which power is removed to the safety controller or parts of the safety or identification systems. Depending on the application, serious injury or death may result.

At the planning stage, ensure that the Key-in-Pocket system is suitable for use in your application.

⚠ **WARNING!**

Potential loss of safety function due to uncontrolled access to the danger zone!

Opening a movable guard that prevents access to the danger zone must only be possible once a person has successfully signed in to the Key-in-Pocket system, otherwise serious injury or death may result, depending on the application.

At the planning stage, ensure that an appropriate interlocking device is available.

⚠ **WARNING!**

Potential loss of safety function due to inadequate staff training!

Anyone who comes into contact with the machine must be trained to understand that the danger zone may not be accessed until they have successfully signed in to the Key-in-Pocket system, otherwise serious injury or death may result, depending on the application.

Ensure that staff receive regular and adequate training. Planning and implementation of appropriate measures is solely the responsibility of the operator.

NOTICE

Hardware outputs to signal the sign in status

Use safe hardware outputs (off test) to activate display elements that signal the sign in status.

NOTICE

Display dynamics when displaying the sign in status

Each person on the plant must have some expectation regarding the dynamics of the display elements that display the sign in status. This can be provided through training.

Planning and implementation of appropriate measures is solely the responsibility of the operator.

NOTICE

Manual deletion of entries in the sign in list

Take appropriate measures to ensure that the ability to delete entries manually from the internal sign in list is restricted to those with relevant training. Manual deletion must not be a routine action.

For example, restrict a transponder to certain permissions or use a PITreader that is specifically intended for this activity.

WARNING!

Potential loss of safety function due to manual access to the sign in list!

Following manual access to the internal sign in list, appropriate organisational measures and inspection procedures must be employed to ensure that nobody is in the danger zone, otherwise serious injury or death may result, depending on the application.

Appropriate measures and inspection procedures should be considered at the planning stage. Planning and implementation of appropriate measures and inspection procedures is solely the responsibility of the system architect, system integrator and/or operator.

WARNING!

Potential loss of safety function due to improper planning of the inside of a plant!

In the Key-in-Pocket system, PITreader units can be used to review people’s sign in status inside a plant (danger zone). This procedure may also be required if additional processes inside a plant are to be interlocked or if it is possible for people to be in a blind spot.

There must not be any device inside the plant that a person could used to sign out of the sign in list; i.e. a PITreader inside the plant must not contain a pushbutton to sign in/out, otherwise serious injury or death may result, depending on the application.

Ensure that a PITreader to check the log in status inside a plant is only used if the area is only accessible after logging in to the Key-in-Pocket system.

NOTICE

When PITreader units are used inside a plant (danger zone) to interlock additional functions depending on a person's sign in status, then these operations must be confirmed through an additional control element and may not be initiated purely as a result of checking the sign in status.

4 Security

4.1 Required security measures

- Modbus/TCP has no security mechanisms. Use a firewall to protect the product from unauthorised access.
- The products’ communication interfaces should be protected against physical manipulation.
- Protect the 24 V inputs and outputs on the safety controller against physical manipulation through protected wiring, e.g. by installing the safety controller in a lockable control cabinet.

5 Description

5.1 Operating principle

The danger zone of plant and machinery is often safeguarded using safety fences. Depending on the application, access to the danger zone may be made accessible from the outside via one or more access points. An access point consists of a safety gate on which a PITreader is attached externally, including a pushbutton for signing in and out. An access point may be a safety gate with/without guard locking, for example.

When the Key-in-Pocket system is used, a person may only enter a plant/machine’s danger zone if they have used their transponder outside at an access point to sign in to the internal sign in list on the Key-in-Pocket system. The transponder must have a valid permission. When signing in, a transponder's security ID and serial number are entered into an internal sign in list.

When a safety controller PNOZmulti is used, the internal sign in list can manage a maximum of 20 entries.

When a safety controller from the automation system PSS 4000 is used, the internal sign in list can manage a maximum of 21 entries.

When leaving the plant, the person must use their transponder at the access point to sign out of the sign in list. As long as there is a transponder signed in to the sign in list, the Key-in-Pocket system prevents the plant from (re)starting.

A blind spot check can be provided for any area in a plant/machine’s danger zone that cannot be seen (blind spot) from an access point and control station (e.g. control console with/without display unit). Further information is available under Blind spot check [📖 16].

5.2 Access points

The opening of a safety gate must lead to a safe state of the plant/machine in order to protect the person who is entering. The state of the safety gate must be monitored so that a (re)start is prevented while any person is in the danger zone.

Via an interlocking device on which a person's sign in status is evaluated, it is possible to ensure that the person has signed in to the sign in list before the safety gate is opened. The interlocking device also means that the person must still be signed in to the sign in list when the safety gate is closed.

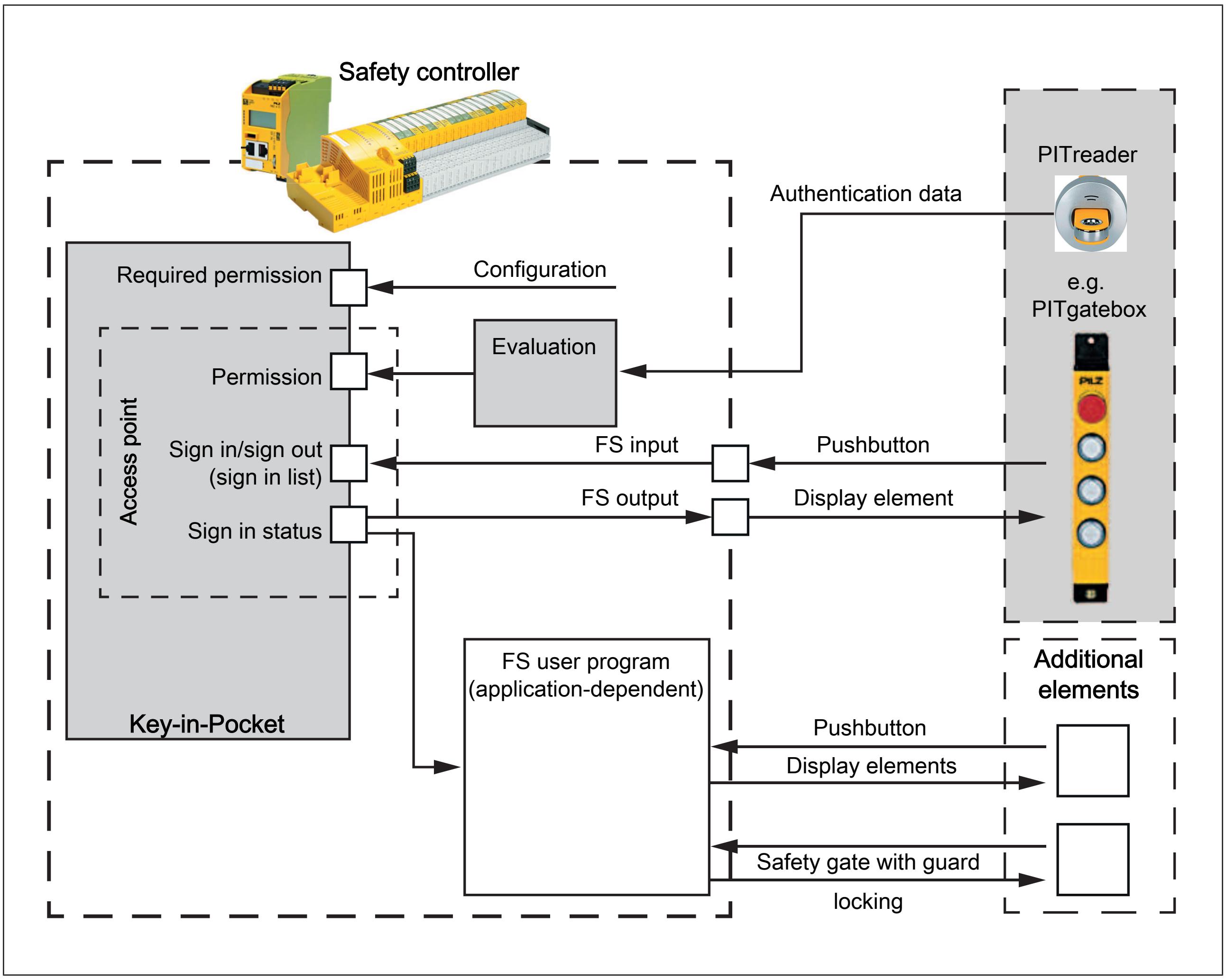


Fig.: Software and hardware components on an access point working together on the Key-in-Pocket system (principle)

Requirements

The following software and hardware components are required for each access point:

- PITreader outside the access point
- One or more transponders with the relevant configured permission
- Ability to configure the required minimum permission for using an access point
- Program section on the safety controller to evaluate a transponder's authentication data

  This includes:

  – Transponder's security ID

  - Transponder's serial number
  - Transponder's permission
- Pushbutton outside the access point

  The pushbutton is used to sign a transponder in to the sign in list and sign a transponder out of the internal sign in list.

  The pushbutton must be connected to an FS input on the safety controller.
- Display element outside the access point

  The display element is used to display whether the transponder with its security ID and serial number is included in the internal sign in list; i.e. the display element lights up if the transponder has been signed in to the internal sign in list.

5.3 Blind spot check

If the inside of a plant (danger zone) contains an area that cannot be seen (blind spot) from an access point and control station (e.g. control console with/without display unit), then the area can be inspected by carrying out a blind spot check.

For the blind spot check, a pushbutton to confirm the check must be installed at a suitable location, and an additional PITreader may be installed as an option.

The last person to be inside the plant must inspect the blind spot visually, if necessary identify themselves with their transponder for the blind spot check and confirm the check via the pushbutton.

As long as the blind spot check has not been carried out or the inspection has not been confirmed and a transponder is signed in to the sign in list, the Key-in-Pocket system prevents the plant from (re)starting.

Blind spot checks can be used in parallel or in serial. The selection of the procedure must result from the risk analysis, depending on the application. The selection of the procedure and its correct implementation is the user's responsibility.

- Blind spot check with parallel evaluation

  Parallel evaluation can be used when the order in which the blind spot checks are carried out does not impact negatively on safety.
  The blind spot checks can be carried out in the user program in any order.
- Blind spot checks with serial evaluation

  Serial evaluation must be used when you can only guarantee that nobody remains undetected in the plant by carrying out the blind spot checks in a certain order.

  With serial evaluation, one blind spot check must be confirmed first before the next blind spot check is activated.

5.4 Plant architectures

The Key-in-Pocket system can be used for a variety of plant architectures.

Examples of plant architectures:

- Plant architecture with a single access point to the danger zone

  Features:

  - Entry to the danger zone is only permitted if a person has signed in to the internal sign in list via their transponder with a valid permission.

  - When leaving the danger zone, the person must sign out of the internal sign in list via their transponder.
  - The Key-in-Pocket system interlocks the (re)start as long as one or more people are signed in.
- Plant architecture with multiple access points to the danger zone

  Features:

  - Entry to the danger zone via one of the access points is only possible if a person has signed in to the shared internal sign in list via their transponder with a valid permission.
  - When leaving the danger zone via one of the access points, the person must sign out of the shared internal sign in list via their transponder.
  - A restart is prevented as long as there are one or more people signed in to the sign in list or one of the safety gates is not closed and locked.
- Plant architecture with one access point for entering the danger zone and one access point for leaving the plant

  Features:

  - Entry to the danger zone is only possible if a person has signed in to the internal sign in list via their transponder with a valid permission.
    The safety gate for access must be closed after entering, to enable the danger zone to be left via a different safety gate.
  - When leaving the danger zone, the person must use their transponder to sign out of the shared internal sign in list.
  - The Key-in-Pocket system interlocks the (re)start as long as one or more people are signed in or one of the safety gates is not interlocked.
- Plant architecture with one access point or multiple access points to the danger zone and an area inside the plant that cannot be seen from any access point and control station (e.g. control console with/without display unit).

  Features:

  - Entry to the danger zone via an access point is only possible if a person has signed in to the shared internal sign in list via their transponder with a valid permission.
  - When leaving the danger zone, the person must use their transponder to sign out of the shared internal sign in list.
  - To confirm that the last person to leave the danger zone has inspected the danger zone that cannot be seen (blind spot), this area must contain a separate PITreader, which the person uses to identify themselves on the Key-in-Pocket system for the blind spot check. The person must confirm the blind spot check via an additional pushbutton.
  - A restart is prevented as long as there are one or more people signed in to the sign in list or one of the safety gates is not closed and locked.

5.5 Sign in list

An internal sign in list is at the heart of the Key-in-Pocket system. The Key-in-Pocket system manages all the sign ins and sign outs for all of a plant's access points in a shared internal sign in list; i.e. everyone who is currently logged into the system is signed in to the internal sign in list. These people are represented in the internal sign in list via the transponder they are using.

An entry in the internal sign in list consists of the following data:

- Transponder's security ID
- Transponder's serial number

When a safety controller PNOZmulti is used, the internal sign in list can manage a maximum of 20 entries.

When a safety controller from the automation system PSS 4000 is used, the internal sign in list can manage a maximum of 21 entries.

If an attempt is made to add an additional entry to a full sign in list, the failed operation is displayed using the relevant diagnostic information.

To enable a transponder to be signed in to the internal sign in list or signed out of the internal sign in list, various requirements must be met:

- Sign transponder in to the internal sign in list

  A transponder is only signed in to the sign in list if the transponder has been removed from a PITreader since the last sign out and has been positioned again.
- Sign transponder out of the internal sign in list

  A transponder is only signed out of the sign in list if the transponder has been removed from a PITreader since the last sign in and has been positioned again.

6 Operation

6.1 Status of the Key-in-Pocket system after power up.

When the safety controller is started up or restarted (voltage supply switched off - on), the status of the Key-in-Pocket system is unknown. In these cases, a deliberate operator action is required in order to carry out a function test and confirm the state of the Key-in-Pocket system. To do this, a person must run a sign in and out process, and if necessary include a blind spot check.

6.2 Procedure for a valid sign in/sign out, including blind spot check

The procedure is identical for each access point on a plant. An access point is a safety gate, on the outside of which is at least one PITreader and a pushbutton to sign in and out.

In order to enter the plant, a person must use their transponder to sign in to the shared internal sign in list. When leaving the plant, a person must use their transponder to sign out of the shared internal sign in list. As long as there is any transponder in the sign in list, the machine cannot be started.

If the plant contains a danger zone that cannot be seen from the outside (= blind spot), the person with the transponder that is signed in as the last remaining transponder in the internal sign in list must carry out and confirm a blind spot check. If not, after leaving the danger zone, the person will not be able to sign out of the internal sign in list and the (re)start interlock will remain activated.

The following example describes the principle procedure for signing in and out at an access point of the Key-in-Pocket system. In the example there are two access points and one blind spot in the danger zone.

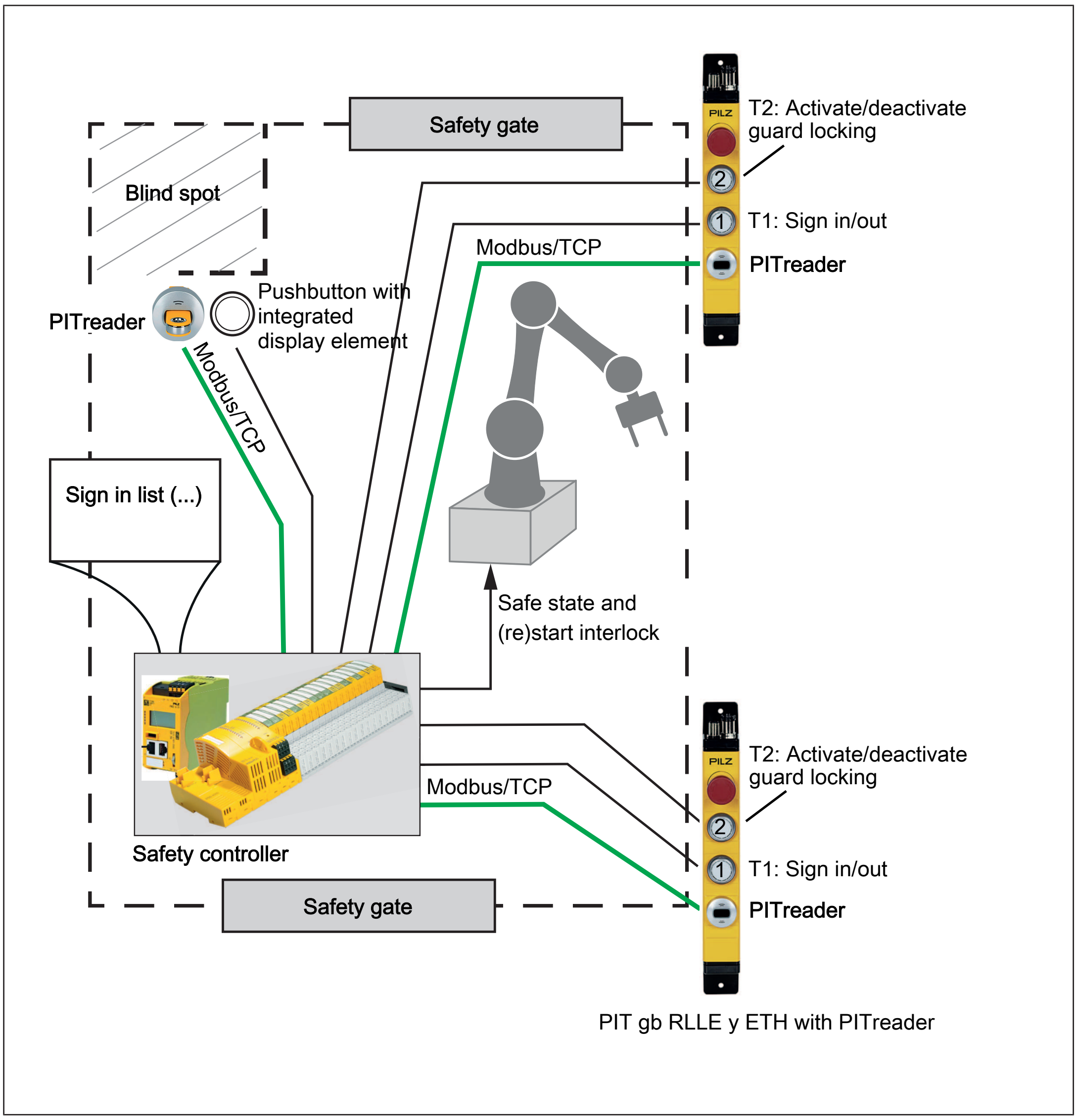

Safety gate
T2: Activate/deactivate guard locking
Blind spot
T1: Sign in/out
Modbus/TCP
PITreader
PITreader
Pushbutton with integrated display element
Modbus/TCP
Sign in list (...)
Safe state and (re)start interlock
T2: Activate/deactivate guard locking
Modbus/TCP
Safety controller
T1: Sign in/out
PITreader
Safety gate
PIT gb RLLE y ETH with PITreader

Fig.: Signing in and out at access points of the Key-in-Pocket system from Pilz (principle)

Prerequisites

- Control elements outside on the safety gates for the access points
  - Pushbutton unit PIT gb RLLE y ETH with PITreader from Pilz

  Configuration:
  - Pushbutton T1 (lower) Pushbutton for signing a transponder in/out
  - Pushbutton T2 (upper): pushbutton for activating/deactivating the guard locking device on a safety gate (optional)
- Control elements in the danger zone at the blind spot
  - Pushbutton with integrated display element for confirming the blind spot check
  - PITreader

Example of a signing in procedure

Sequence	**PITreader display element (safety gate)**	**Pushbutton display elements**	
		T1 (sign in/out)	**T2 (De)activate guard locking**
Start position Outside on the safety gate for the access point, no transponder is positioned on the PITreader.	Blue PITreader is ready for operation	Off	Off
A person positions their transponder with valid permission on the PITreader.	▲	Off	Off
Within 60 s, the person operates pushbutton T1 (for a period of 500 – 5000 ms) in order to sign the transponder in to the sign in list. ▸ The transponder, including security ID and serial number, is signed in to the shared internal sign in list.	Green Transponder has been recognised as valid	-> Lights up	Lights up Guard locking is activated on the safety gate
The person operates pushbutton T2 in order to deactivate guard locking on the safety gate. ▸ Depending on the application, the plant is switched to a safe state by the user program and guard locking on the safety device is deactivated.	Green	Lights up Transponder is signed in	-> Off
The person can open the safety gate.	Green	Lights up	Off Guard locking is deactivated on the safety gate
Remove transponder The person removes their transponder from the PITreader.	▼	Off	Off

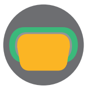
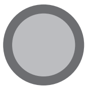
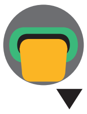
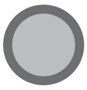
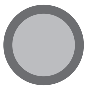
Sequence	PITreader display element (safety gate)	Pushbutton display elements	
		T1 (sign in/out)	T2 (De)activate guard locking
The persons enters the plant with their transponder and carries out their work.	Blue	Off	Off

If necessary other people may enter the plant. The procedure for signing in and out is always the same, irrespective of the access point by which a person enters and leaves the plant.

The section below describes the procedure for signing out with a prior blind spot check:

Example of the procedure for a blind spot check

Sequence	PITreader display element (blind spot)	Pushbutton display element (confirm check)
Start position There is just one last person in the plant's danger zone. This person has the transponder that is signed in as the last remaining transponder in the shared internal sign in list and has permission to carry out the blind spot check. All other people have used their respective transponder to sign out on the PITreader at an access point, after leaving the danger zone.	Blue PITreader is ready for operation	Lights up Blind spot check must be confirmed
The person with the last remaining transponder in the sign in list goes to the blind spot and carries out a visual inspection.	Blue	Lights up
If there is nobody in the blind spot, the person positions their transponder on the PITreader.	▲	Lights up
If the transponder is recognised as valid, the person operates the pushbutton to confirm that the blind spot check has been carried out.	Green Transponder has been recognised as valid	-> Off

Sequence	PITreader display element (blind spot)	Pushbutton display element (confirm check)
The display element on the pushbutton goes out as a sign that the blind spot check has been confirmed correctly.	 Green	 Off Blind spot check was confirmed
The person removes their transponder from the PITreader.		 Off
The person leaves the plant within the configured timeframe and closes the safety gate behind them.	 Blue	 Off

Example of a signing out procedure

Sequence	PITreader display element (safety gate)	Pushbutton display elements	
		T1 **(sign in/out)**	**T2** **((de)activate guard locking)**
Start position ▸ There is nobody in the plant's danger zone. ▸ The safety gates for the access points were closed from the outside.	▭ Blue PITreader is ready for operation	○ Off	○ Off
The person with the last remaining transponder in the sign in list positions the transponder on the PITreader on the safety gate.	▭ ▲	● Lights up There is still 1 transponder signed in.	○ Off
The person operates pushbutton T2 in order to activate guard locking on the safety gate. Guard locking is activated on the safety gate	▭ Green Transponder has been recognised as valid	● Lights up	○ ☝ -> ● Lights up
The person operates pushbutton T1 (for a period of 500 – 5000 ms) in order to sign their transponder out of the sign in list. The (re)start interlock is reset.	▭ Green	● ☝ -> ○ Off	● -> ○ Off Guard locking can no longer be deactivated

Sequence	**PITreader display element (safety gate)**	**Pushbutton display elements**	
		T1 (sign in/out)	**T2 ((de)activate guard locking)**
The person removes their transponder from the PITreader.	🟩 ▼	○ Off No other transponder is signed in.	○ Off
From this point the machine can be started, using a control panel for example. Note: A machine start is only possible under the following conditions: ▸ The sign in list is empty ▸ The safety gates on all access points are closed. ▸ The guard locking devices on all safety gates are activated.	🟦 Blue	○ Off	○ Off

6.3 Establish a transponder’s sign in status

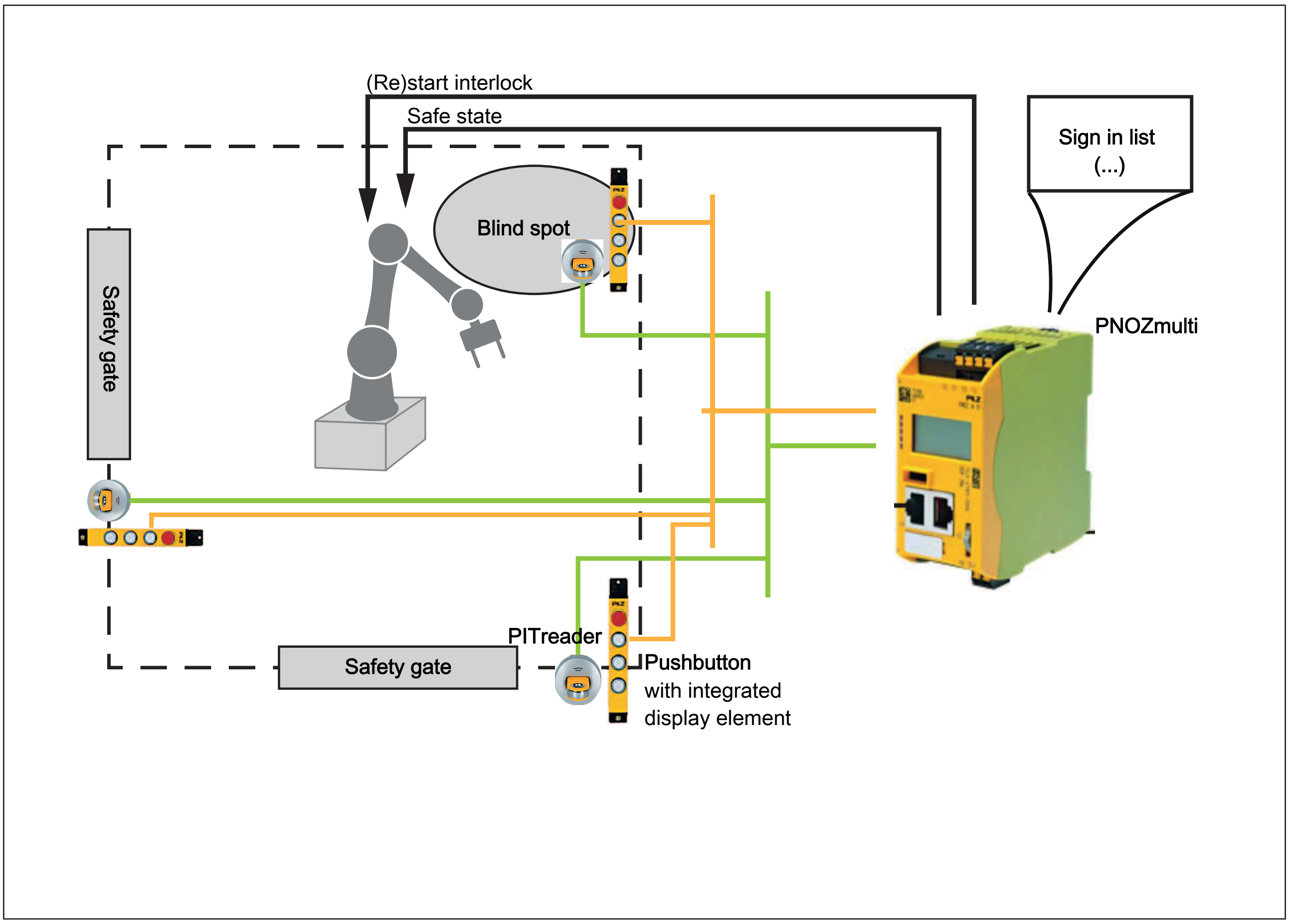
It is possible to establish whether a transponder is signed in to the internal sign in list.

Transponder is signed in	PITreader display element	Pushbutton with display element
Start position No transponder is positioned on the PITreader.	Blue PITreader is ready for operation	Off
A person positions their transponder with valid permission on the PITreader.	▲	Off
Status of the transponder in the internal sign in list:	Green Transponder has been recognised as valid	Lights up Transponder is signed in

Transponder is not signed in	PITreader display element	Pushbutton with display element
Start position No transponder is positioned on the PITreader.	Blue PITreader is ready for operation	Off
A person positions their transponder with valid permission on the PITreader.	▲	Off
Status of the transponder in the internal sign in list:	Green Transponder has been recognised as valid	Off Transponder is not signed in

7 Key-in-Pocket system with PNOZmulti

7.1 System overview



The Key-in-Pocket system with PNOZmulti is implemented using the elements in the PNOZmulti Configurator, the base unit PNOZ m B1 (Burner) and the PITreader.

The Key-in-Pocket system is supported from PNOZmulti Configurator V11.2.0.

Elements of the Key-in-Pocket system with PNOZmulti

- **Key-in-Pocket element**

  Communication with the PITreader and monitoring of the pushbutton for signing in and out at the access point

- **Blind spot check element**

  For the blind spot check, a pushbutton to confirm the check must be installed at a suitable location, and an additional PITreader can be installed as an option.

  The blind spot check is activated when there is only one transponder left in the sign in list. It is activated via the activate blind spot check output on the ***Key-in-Pocket*** element.

  The last person to be inside the plant must inspect the blind spot visually, identify themselves on the PITreader if necessary and confirm the check via the pushbutton.

  Only then can the transponder be signed out of the sign in list.

- **Delete sign in list element**

In certain cases, a plant cannot be put back into operation because there are entries in the sign in list, even though there is nobody left in the plant:

- People have not signed out correctly before leaving the plant
- People have lost their transponder

In these cases, an authorised person can delete the sign in list. The ***Delete sign in list*** element is available for this purpose.

The person authorised to delete the sign in list must use their transponder to authenticate themselves and be signed in to the sign in list. The pushbutton to delete the sign in list must then be operated.

The enable through the Key-in-Pocket system occurs once the person who has deleted the sign in list signs out.

NOTICE

Permission to delete the sign in list

Take appropriate measures to ensure that the ability to delete the sign in list is restricted to those with relevant training. Manual deletion must not be a routine action.

For example, restrict a transponder to certain permissions or use a PITreader that is specifically intended for this activity.

7.2 System expansion

Maximum system expansion for the configurable safe small controllers PNOZmulti 2:

- A maximum of 20 people at a time can be signed into a sign in list with their transponder.
- The Key-in-Pocket system can monitor a max. of 4 independent plant sections. A sign in list is assigned to each plant section.
- Each plant section can have one or more access points. A ***Key-in-Pocket*** element must be configured for each access point.
  As a max. of 4 PITreader units can be connected, the max. number of access points is also limited to 4.

7.3 Installation

7.3.1 Connect PITreader

The PITreader is connected to the PNOZmulti via an Ethernet cable. Please refer to the information and requirements in the operating manual for the PITreader.

7.3.2 Connect external pushbuttons and display elements

A Key-in-Pocket system requires pushbuttons and display elements for various activities. You can use components as external pushbuttons and display elements in the following formats:

- Pushbuttons and display elements as separate components (one display element per pushbutton)

- Pushbutton with integrated display elements

The pushbuttons must have single-channel N/O contacts.

Note: A pushbutton with integrated display element should be preferred as the pushbutton and display element (e.g. pushbutton unit PITgatebox from Pilz).

Required pushbuttons and display elements

Depending on the application, pushbuttons and display elements may be required for the following activities:

- Pushbutton and corresponding display element to sign a transponder in to the internal sign in list and sign a transponder out of the internal sign in list.

  One pushbutton with corresponding display element is required per access point.
- Pushbutton and corresponding display element to delete the sign in list
- Pushbutton and display elements to confirm a blind spot check.

  One pushbutton with corresponding display element is required per blind spot check.

Connect pushbutton

Use digital, safe inputs to connect the pushbuttons to the PNOZmulti. Please refer to the information and technical details stated in the operating manual of the PNOZmulti device you are using.

Connect display elements

Use digital, safe outputs to connect the display elements to the safety controller. Please refer to the information and technical details stated in the operating manual of the PNOZmulti device you are using.

7.4 Connect PITreader

The PITreader is connected to the PNOZmulti via an Ethernet cable. Please refer to the information and requirements in the operating manual for the PITreader.

7.5 Configure user program

In the PNOZmulti Configurator, add the following devices to the hardware configuration:

- Base unit PNOZ m B1 or PNOZ m B1 Burner from firmware version 01.09
- Input and output modules

  You must use modules with safe inputs and/or safe outputs.
- PITreader

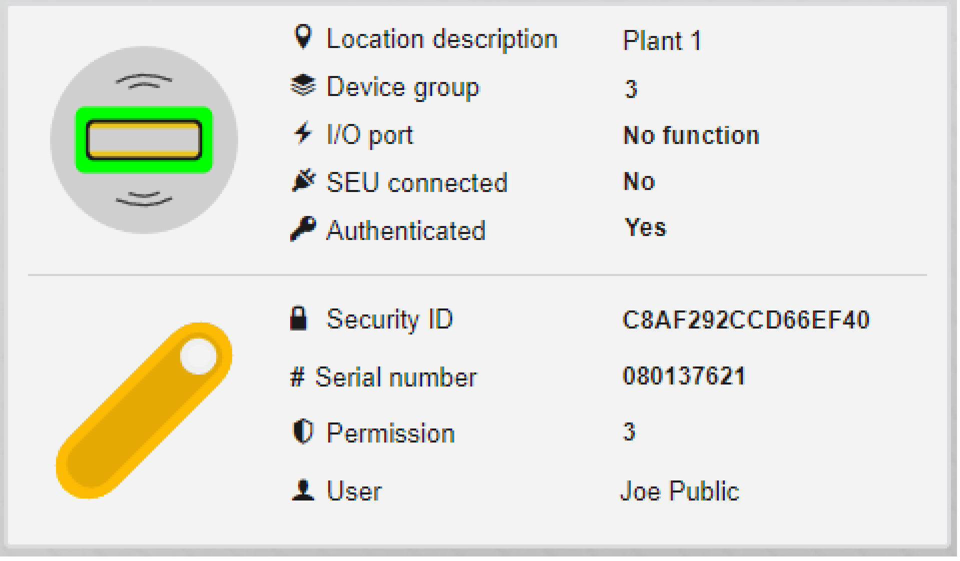
Configure the Key-in-Pocket elements as described in the PNOZmulti Configurator Online Help.

7.6 Visualisation

Various information about the Key-in-Pocket system can be displayed in the PASvisu visualisation.

7.6.1 Show PITreader status

Status information for the PITreader and the transponder can be displayed for each PITreader configured as the data source in the PASvisu project.



Location description	Plant 1
Device group	3
I/O port	No function
SEU connected	No
Authenticated	Yes
Security ID	C8AF292CCD66EF40
# Serial number	080137621
Permission	3
User	Joe Public

Fig.: PITreader status tile

The "PITreader status" tile is used for the display.

It is possible to configure:

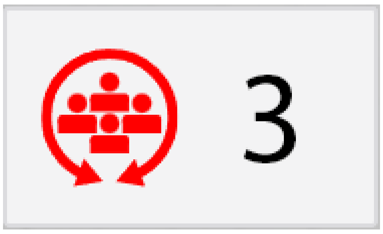
- Whether the status of the PITreader and the transponder is to be displayed, or just one of the two
- Whether only the icons for the PITreader/transponder are displayed or also the texts on the right-hand side

Details of the tile can be found in the PASvisu Builder Online Help.

7.6.2 Show sign in list

The sign in lists can be displayed for each PNOZmulti project that is configured as the data source in the PASvisu project and contains one or more ***Key-in-Pocket*** elements.

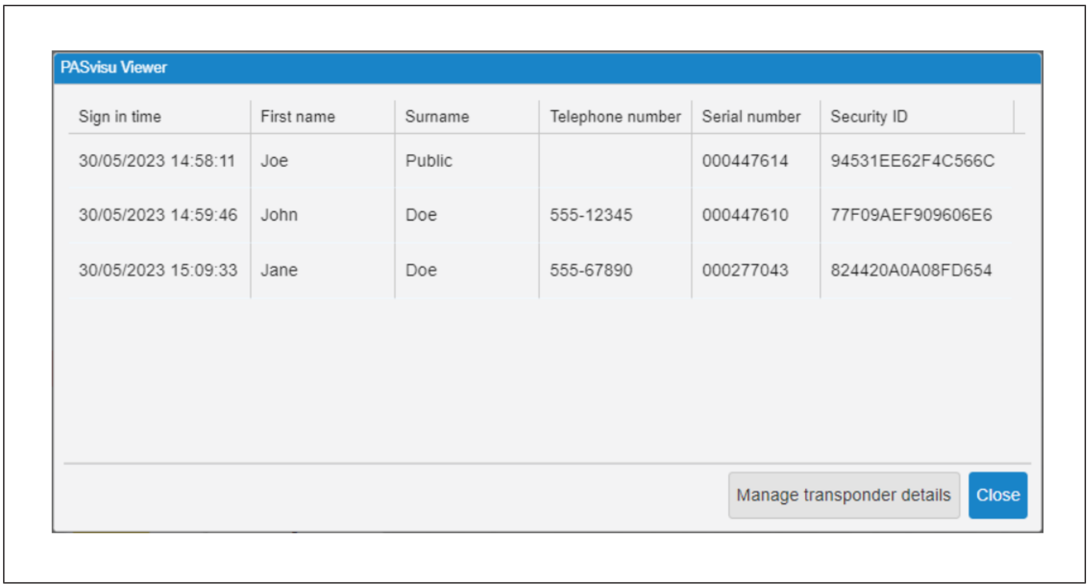
The number of users who are currently signed in to the sign in list is displayed:



3

Fig.: Key-in-Pocket sign in list tile

The content of the sign in list is displayed by clicking on the tile:



PASvisu Viewer

Sign in time	First name	Surname	Telephone number	Serial number	Security ID
30/05/2023 14:58:11	Joe	Public		000447614	94531EE62F4C566C
30/05/2023 14:59:46	John	Doe	555-12345	000447610	77F09AEF909606E6
30/05/2023 15:09:33	Jane	Doe	555-67890	000277043	824420A0A08FD654

Fig.: Content of the sign in list

The "Key-in-Pocket sign in list" tile is used for the display. A separate tile is required for each sign in list.

Details of the tile can be found in the PASvisu Builder Online Help.

INFORMATION

The "Key-in-Pocket sign in list" tile is available in the PASvisu Builder from Version 1.14.0.

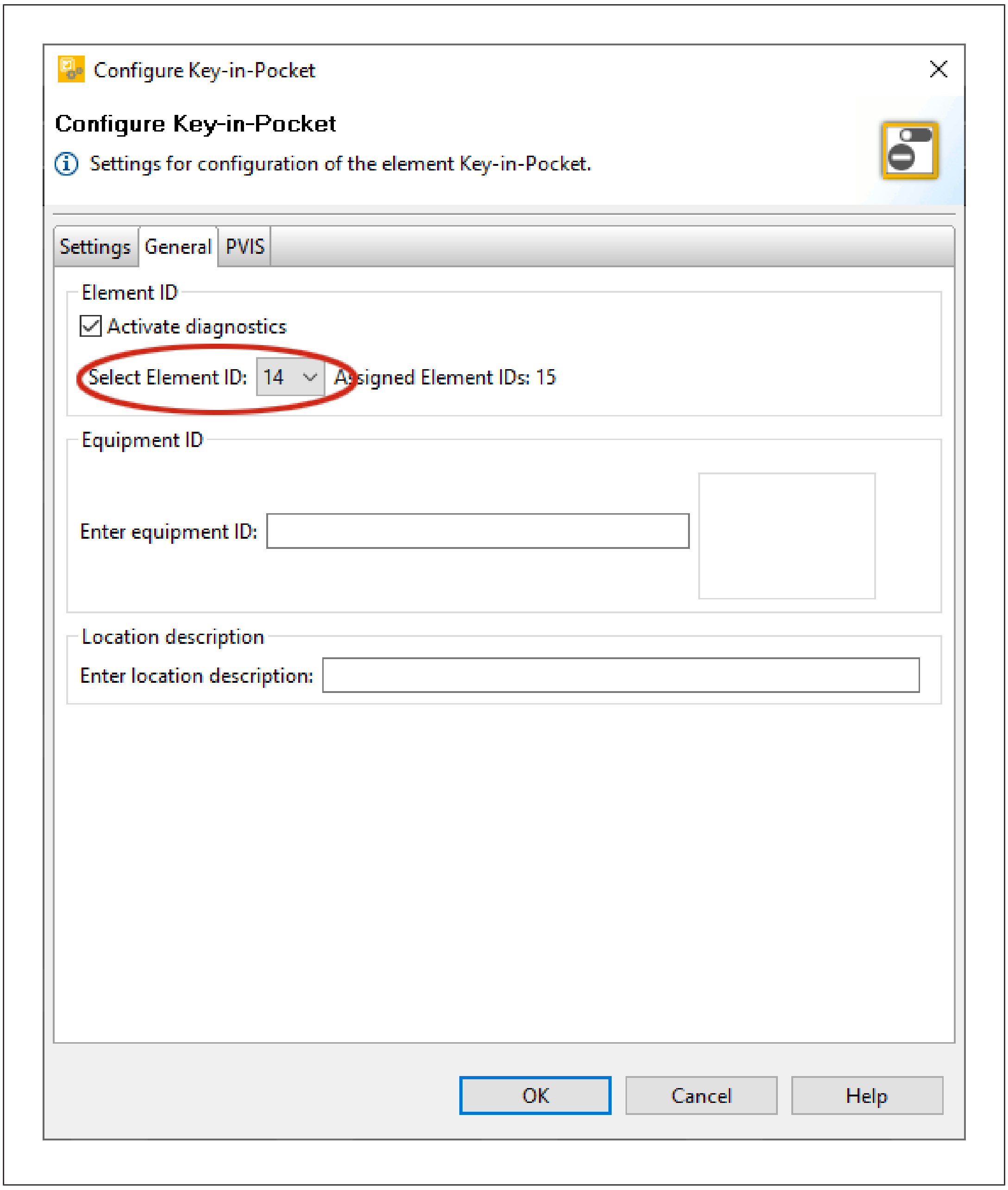
7.6.3 Show status information for the Key-in-Pocket system

Various information about the Key-in-Pocket system can be displayed in a PASvisu project. This information can be found in the PNOZmulti project in diagnostic word 1 and 2 of the "Key-in-Pocket" element.

Example: Show length of the sign in list

In the PASvisu project, it is possible to show how many users are currently signed into the sign in list on the "Non-decimal value" tile.

To do this, the "Key-in-Pocket" element must be inserted in the PNOZmulti project. In this case, the element has element ID "14".



Configure Key-in-Pocket

Configure Key-in-Pocket

Settings for configuration of the element Key-in-Pocket.

Element ID

☑ Activate diagnostics

Select Element ID: 14 Assigned Element IDs: 15

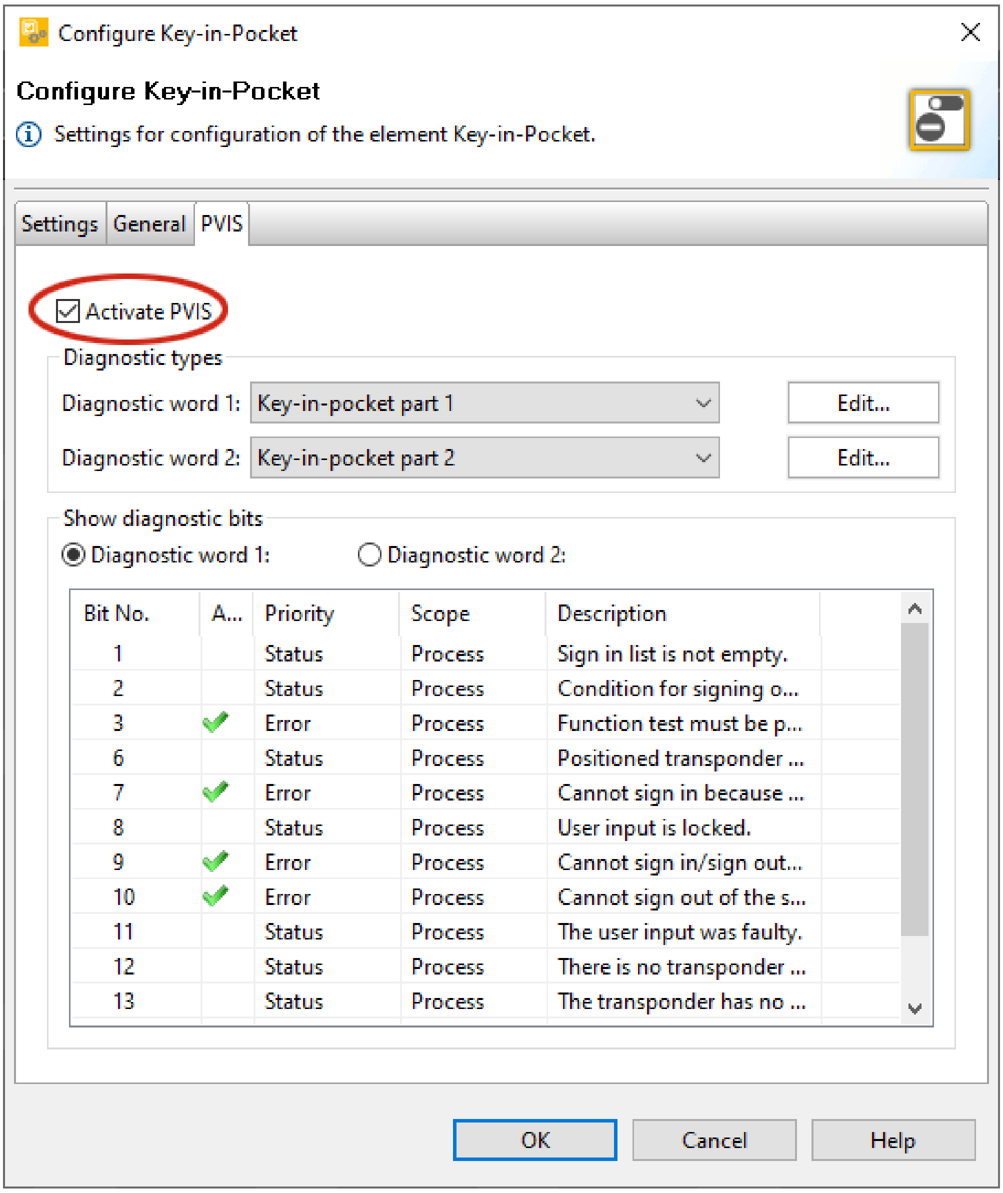
Equipment ID

Enter equipment ID:

Location description

Enter location description:

In the PNOZmulti project, PVIS diagnostics must be activated for the "Key-in-Pocket" element.



Configure Key-in-Pocket

Configure Key-in-Pocket

ⓘ Settings for configuration of the element Key-in-Pocket.

☑ Activate PVIS

Diagnostic types

Diagnostic word 1: Key-in-pocket part 1

Diagnostic word 2: Key-in-pocket part 2

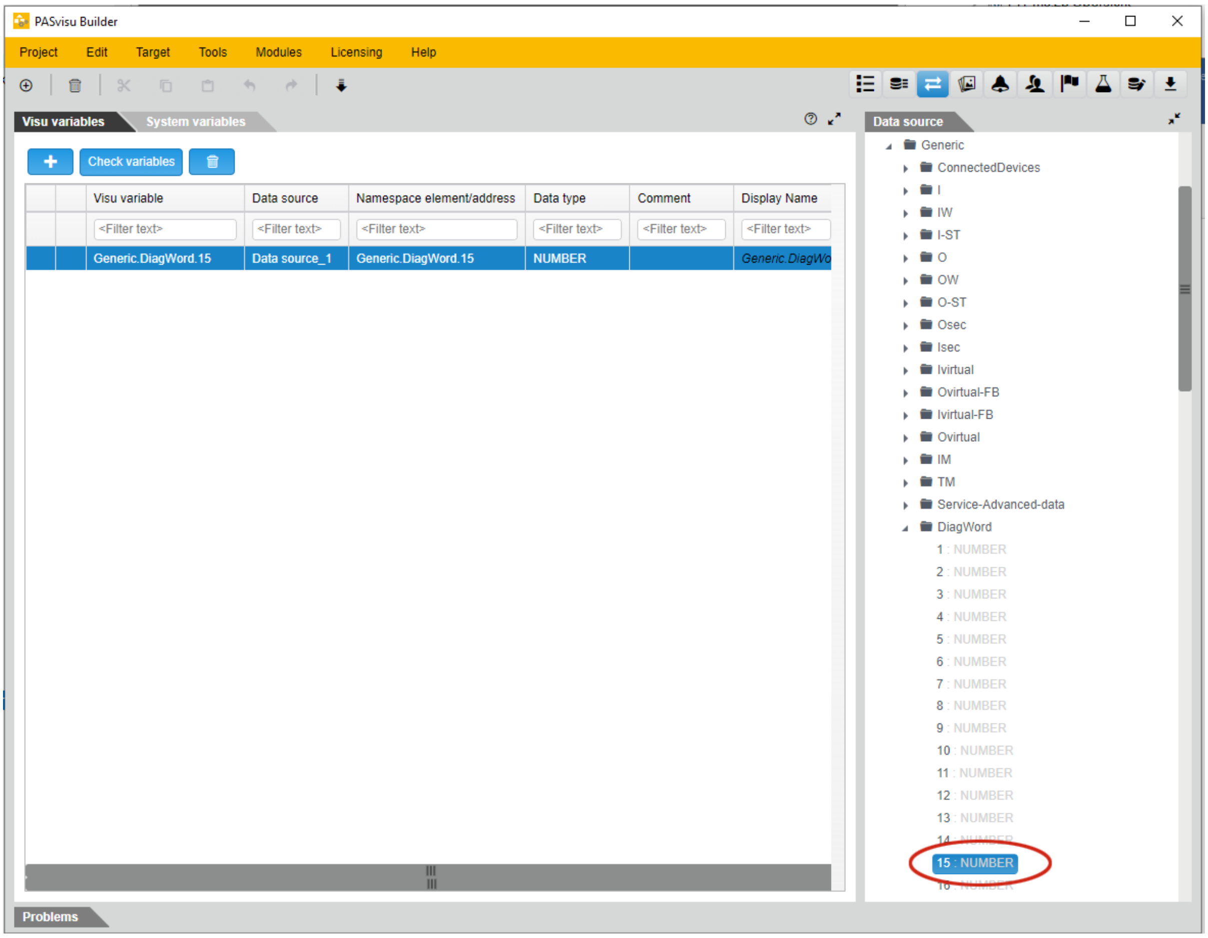
Show diagnostic bits

● Diagnostic word 1: ○ Diagnostic word 2:

Bit No.	A...	Priority	Scope	Description
1		Status	Process	Sign in list is not empty.
2		Status	Process	Condition for signing o...
3	✓	Error	Process	Function test must be p...
6		Status	Process	Positioned transponder ...
7	✓	Error	Process	Cannot sign in because ...
8		Status	Process	User input is locked.
9	✓	Error	Process	Cannot sign in/sign out...
10	✓	Error	Process	Cannot sign out of the s...
11		Status	Process	The user input was faulty.
12		Status	Process	There is no transponder ...
13		Status	Process	The transponder has no ...

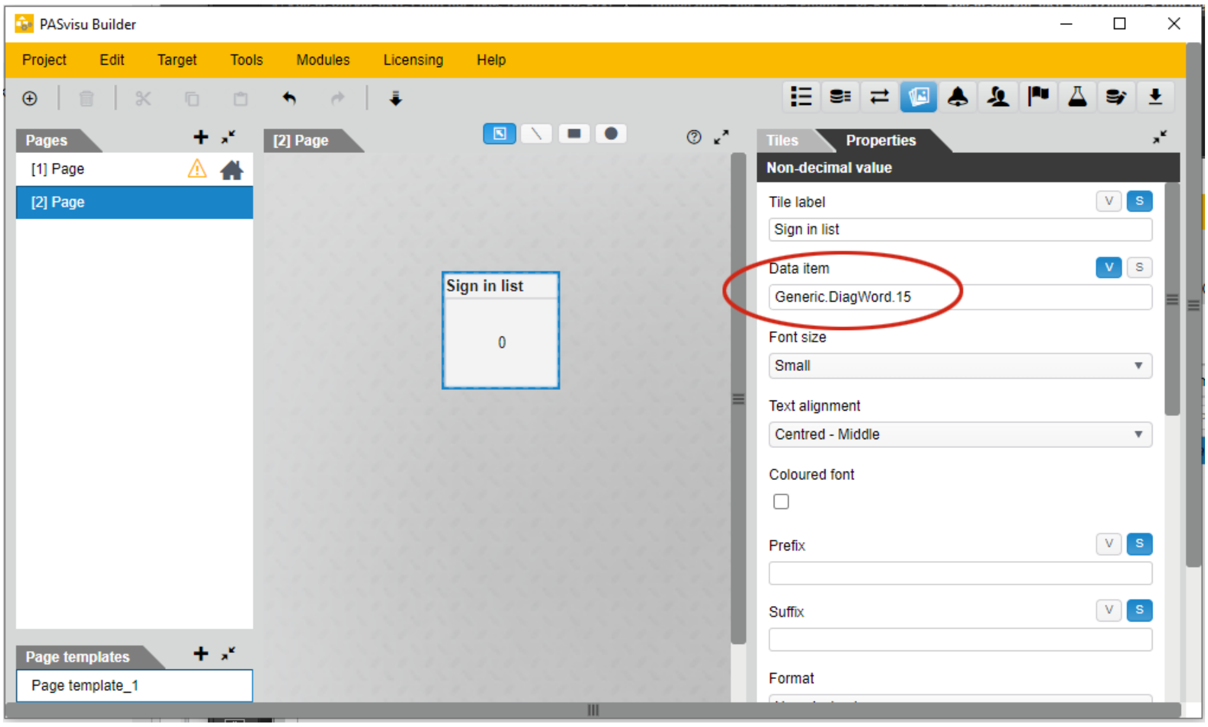
To do this, the diagnostic configuration must be linked in the PNOZmulti Configurator (***Diagnostics -> Link diagnostic configuration***). Then, the PNOZmulti project can be configured as the data source in the PASvisu project.

The information regarding the "Number of users signed in to the sign in list" can be found in diagnostic word 2 of the "Key-in-Pocket" element with element ID 14. In order to access this information you need a Visu variable that is assigned to the namespace element "Generic.DiagWord.15".



		Visu variable	Data source	Namespace element/address	Data type	Comment	Display Name
		<Filter text>	<Filter text>	<Filter text>	<Filter text>	<Filter text>	<Filter text>
		Generic.DiagWord.15	Data source_1	Generic.DiagWord.15	NUMBER		Generic.DiagWo

This Visu variable will then be used as the data item for the "Non-decimal value" tile.



Non-decimal value

Tile label: Sign in list

Data item: Generic.DiagWord.15

Font size: Small

Text alignment: Centred - Middle

Coloured font □

Prefix

Suffix

Format

7.7 Diagnostics

The current status of the key-in-pocket system can be retrieved via the PNOZmulti diagnostics.

- The number of transponders that are signed into the sign in list.
- Identification data for the transponders that are signed into the sign in list.

You should also read the document entitled "Communication interfaces PNOZmulti 2".

7.8 Examples

7.8.1 1 access point and 2 blind spots

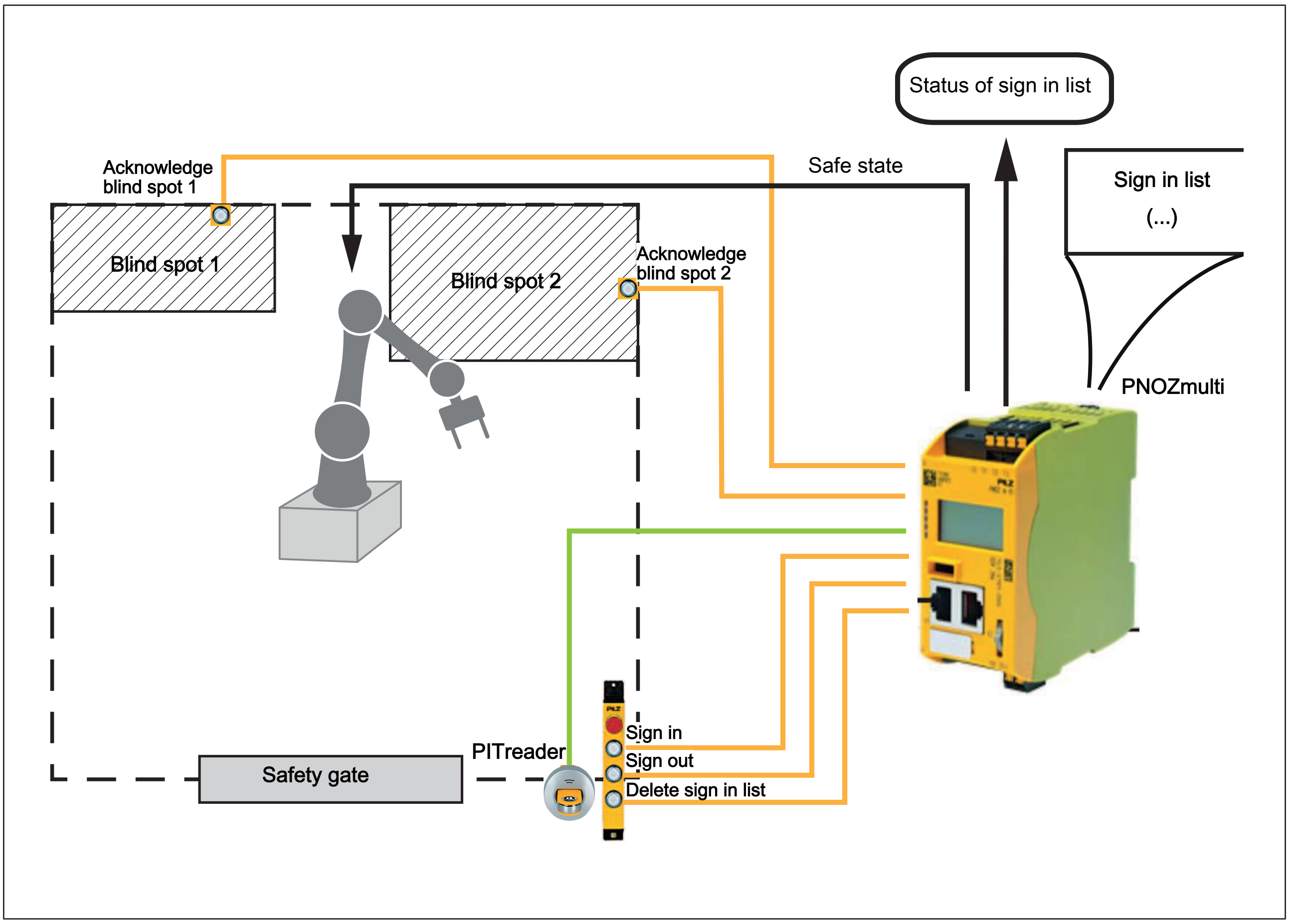
System overview

The Key-in-Pocket system consists of the following components:

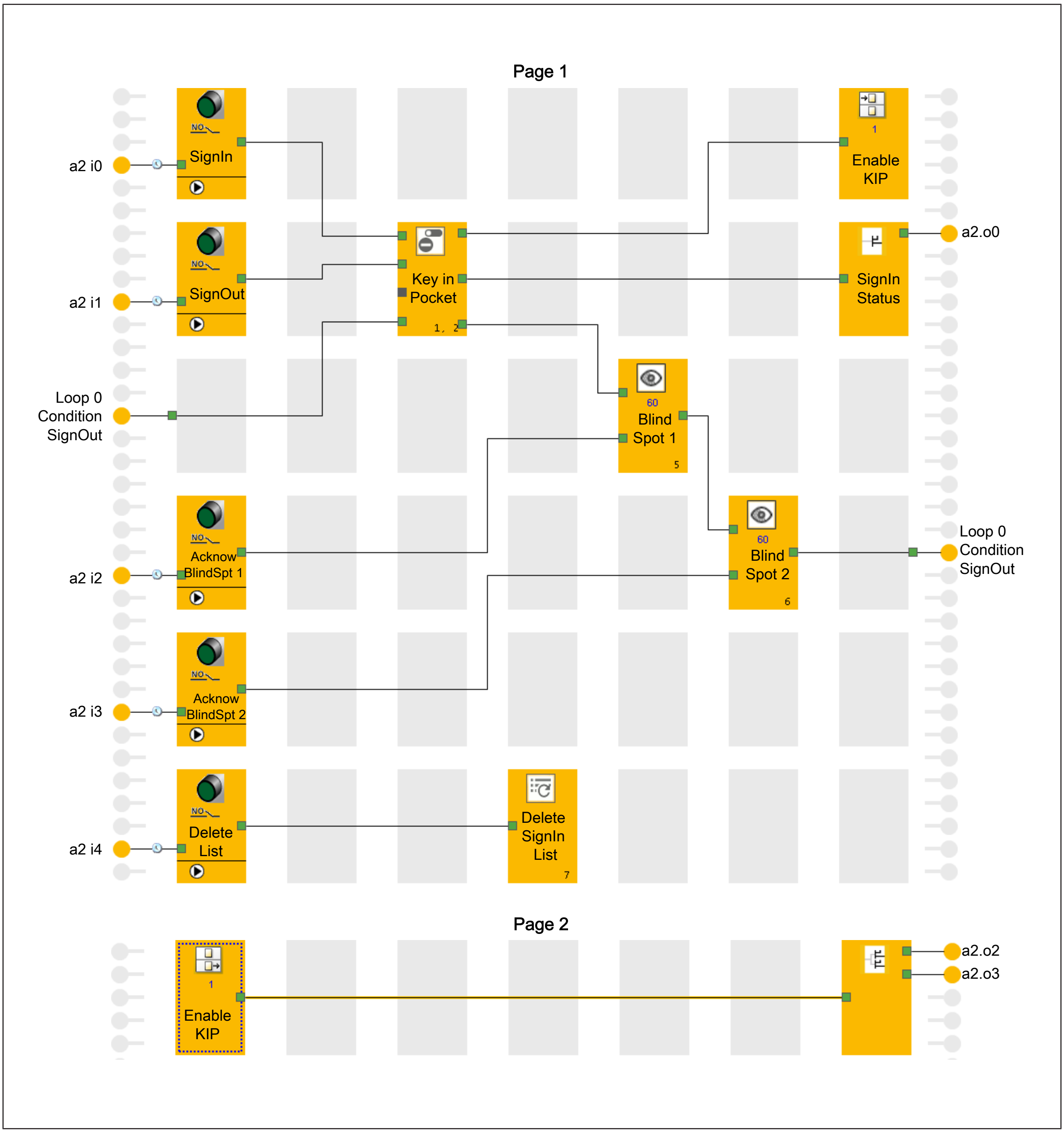
- One safety gate as access point
- One PITreader on the safety gate
- One pushbutton on the safety gate to sign in to the sign in list (Sign in)
- One pushbutton on the safety gate to sign out of the sign in list (Sign out)
- One pushbutton on the safety gate to delete the sign in list (Delete list)
- One pushbutton in the area of blind spot 1 to confirm the blind spot check (Acknowledge blind spot 1)
- One pushbutton in the area of blind spot 2 to confirm the blind spot check (Acknowledge blind spot 2).

The pushbuttons for the blind spot check are connected in series and must therefore be operated in the correct order. The pushbutton for blind spot 1 must be operated first, followed by the pushbutton for blind spot 2.

In this example, there is no monitoring as to whether the safety gates are closed or will be locked. If necessary, these conditions can be added in an AND element "Condition for Sign Out".



Configuration in PNOZmulti Configurator



7.8.2 2 access point and 2 blind spots

System overview

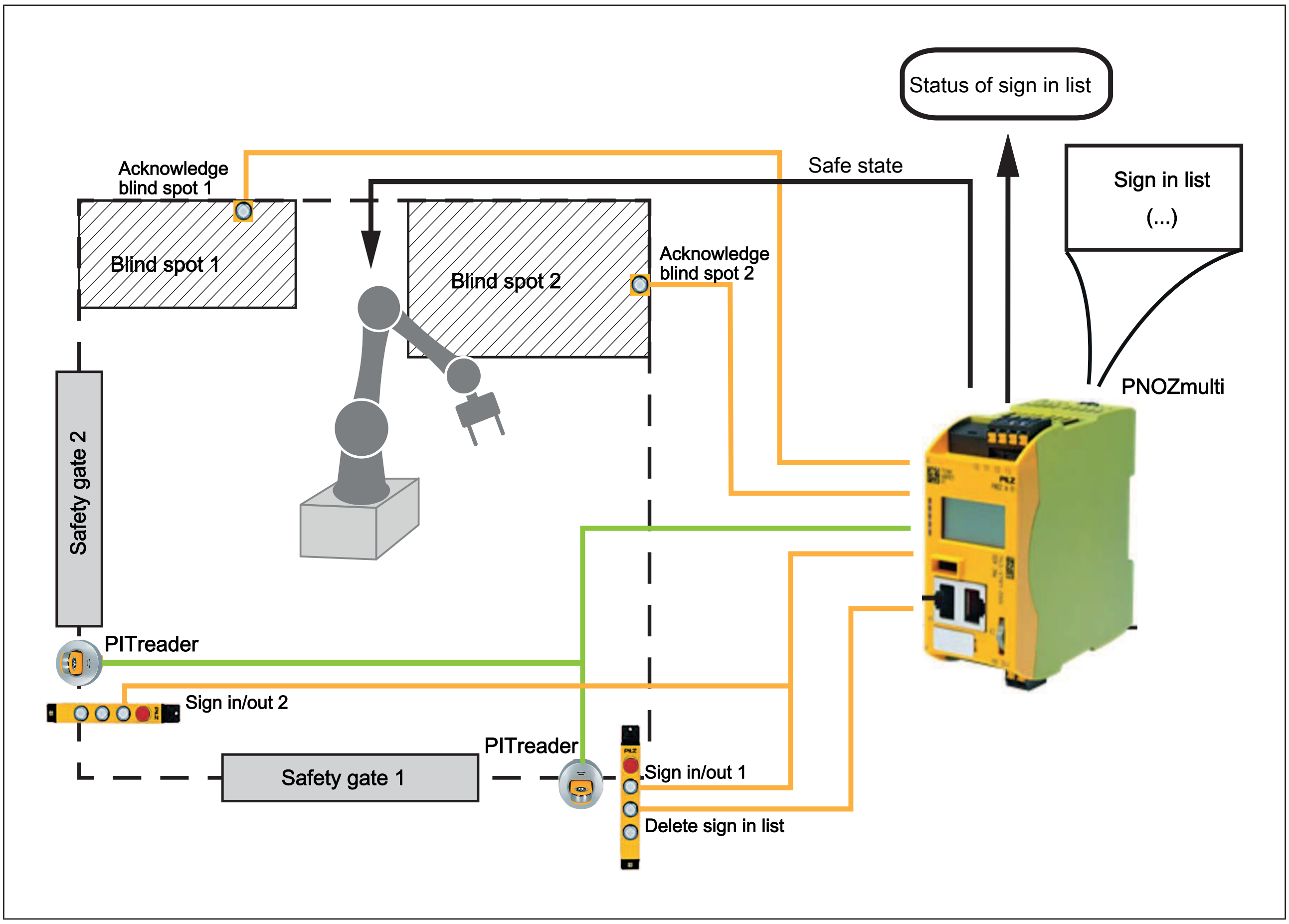
The Key-in-Pocket system consists of the following components:

- Two safety gates as access points
- One PITreader on each safety gate
- **One** sign in/out pushbutton on each safety gate to sign in to the sign in list and sign out of the sign in list (Sign In/Out 1, Sign In/Out 2)
- One pushbutton on safety gate 1 to delete the sign in list (Delete list)
- One pushbutton in the area of blind spot 1 to confirm the blind spot check (Acknowledge blind spot 1)
- One pushbutton in the area of blind spot 2 to confirm the blind spot check (Acknowledge blind spot 2).

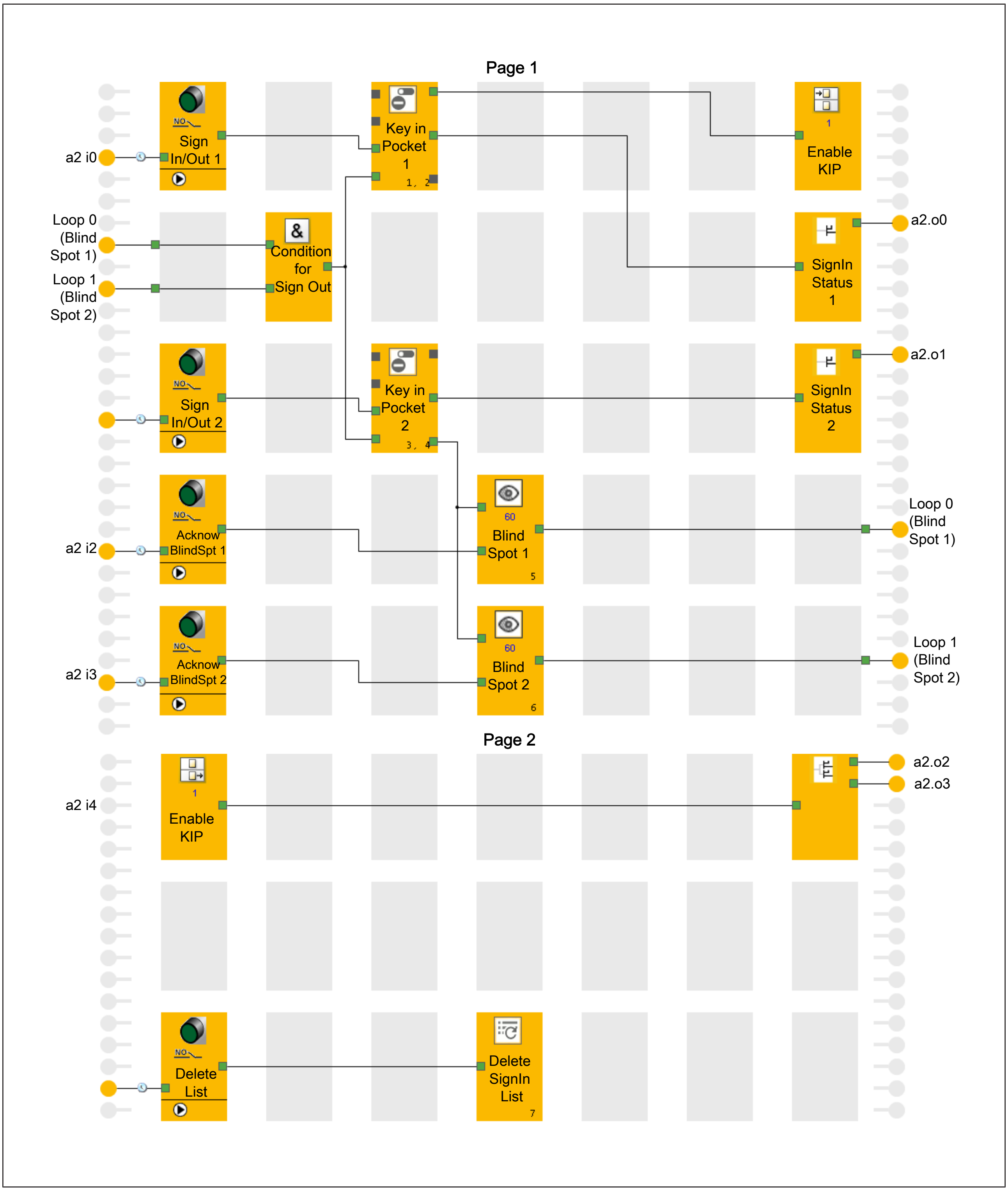
The pushbuttons for the blind spot check are connected in parallel and therefore can be operated in any order.

A person can sign in and out via one of the two PITreader devices.

In this example, there is no monitoring as to whether the safety gates are closed or will be locked. If necessary, these conditions can be added in the AND element "Condition for Sign Out".

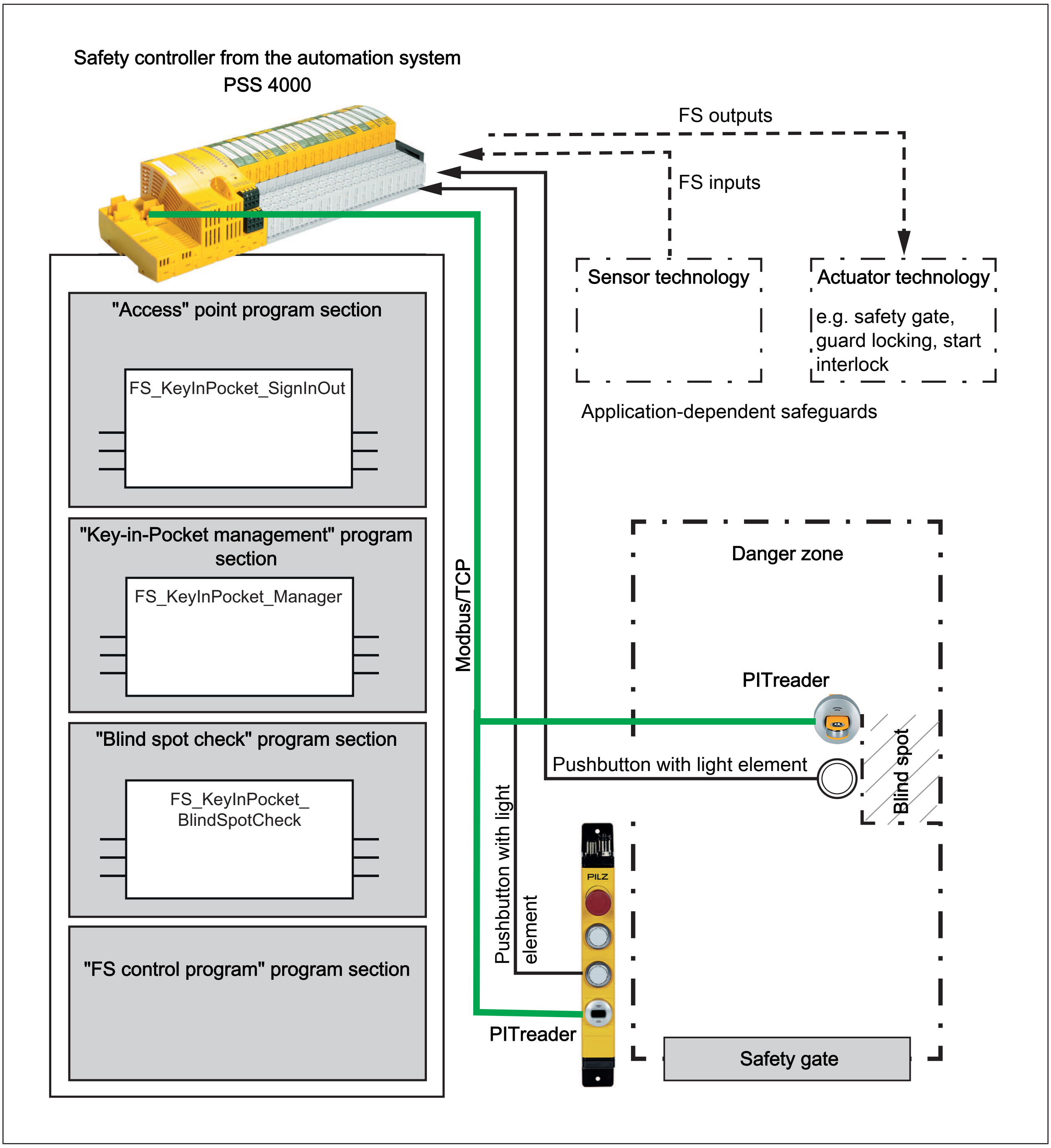


Configuration in PNOZmulti Configurator



8 Key-in-Pocket system with PSS 4000

8.1 System overview


Safety controller from the automation system
PSS 4000
FS outputs
FS inputs
Sensor technology
Actuator technology
e.g. safety gate, guard locking, start interlock
Application-dependent safeguards
"Access" point program section
FS_KeyInPocket_SignInOut
"Key-in-Pocket management" program section
FS_KeyInPocket_Manager
"Blind spot check" program section
FS_KeyInPocket_BlindSpotCheck
"FS control program" program section
Modbus/TCP
Danger zone
PITreader
Pushbutton with light element
Blind spot
Pushbutton with light element
PILZ
PITreader
Safety gate

Blocks in the Key-in-Pocket system

- Function block FS_KeyInPocket_SignInOut

  Communication with the PITreader and monitoring of the pushbutton for signing in and out at the access point

- Function block FS_KeyInPocket_Manager

Management of the internal list with the signed in transponders

- Optional: FS_KeyInPocket_BlindSpotCheck for the blind spot check

  The blocks in the Key-in-Pocket system are suitable for plants that are accessible via (safety) gates and on which the voltage supply to the control system is not normally shut down.

8.2 System expansion

Maximum system expansion for a safety controller from the automation system PSS 4000:

- PSS 4000 device with IP connections system section
- A Key-in-Pocket system is designed for a maximum of 10 access points and multiple blind spot checks. A PITreader is required for each access point and each blind spot check.

  The maximum number of PITreader devices that can be connected to a safety controller depends on the maximum number of IP connections that a safety controller can manage. Please also refer to the information on IP connections in the PAS4000 Online Help.

8.3 Installation

8.3.1 Connect PITreader

The PITreader is connected to the safety controller from the automation system PSS 4000 via an Ethernet cable. Please refer to the information and requirements in the operating manual for the PITreader.

8.3.2 Connect external pushbuttons and display elements

A Key-in-Pocket system requires pushbuttons and display elements for various activities. You can use components as external pushbuttons and display elements in the following formats:

- Pushbuttons and display elements as separate components (one display element per pushbutton)
- Pushbutton with integrated display elements

The pushbuttons must have single-channel N/O contacts.

Note: A pushbutton with integrated display element should be preferred as the pushbutton and display element (e.g. pushbutton unit PITgatebox from Pilz).

Required pushbuttons and display elements

Depending on the application, pushbuttons and display elements may be required for the following activities:

- Pushbutton and corresponding display element to sign a transponder in to the internal sign in list and sign a transponder out of the internal sign in list.

  One pushbutton with corresponding display element is required per access point.
- Pushbutton and corresponding display element to delete the sign in list
- Pushbutton and display elements to confirm a blind spot check.

  One pushbutton with corresponding display element is required per blind spot check.

Connect pushbutton

Use digital FS input modules (e.g. PSSu E F 4DI) to connect the pushbuttons to the safety controller. Please refer to the information and technical details stated in the operating manual of the FS input module you are using.

- Connect external pushbuttons to FS inputs on the safety controller.

Connect display elements

Use digital FS output modules (e.g. E F 4DO 0.5) to connect the display elements to the safety controller. Please refer to the information and technical details stated in the operating manual of the FS output module you are using.

- Connect external display elements to FS outputs on the safety controller.

8.4 Configuration and programming

8.4.1 Configure PITreader

The PITreader is configured using a web application, see PITreader operating manual.

8.4.2 Configure and program safety controller

All the configurations and the user program creation are made in PAS4000.

8.4.2.1 Configure hardware

In PAS4000, in the Project Manager, add the following devices under ***Hardware configuration***:

- PSS 4000 device of the PSS 4000 PLC performance class (e.g. PSSu system).
- Input and output modules

  You must use modules with FS inputs and/or FS outputs. The off tests on the FS outputs must be activated.

8.4.2.2 Configure connection to the PITreader

The connection to the PITreader is established via Modbus/TCP.

In PAS4000, in the PSS 4000 project, a Modbus/TCP Client connection (IP connection) must be created and configured between the safety controller and PITreader for each PITreader in a Key-in-Pocket system.

Prerequisite

- PITreader and safety controller are connected via an Ethernet cable.

Procedure

- Open the IP Connections Editor in PAS4000.
- Create a new Modbus/TCP Client connection.
- Configure the following network settings for the connection:
  - ***Remote IP address***: Enter the PITreader's IP address. The factory default setting is 192.168.0.12.
  - ***Local port number***: 0
  - ***Remote port number***: 502
  - ***Unit ID***: 255
  - ***Keep alive settings***: Deactivate checkbox
  - ***Connection timeout***: Activate checkbox
  - ***Connection cycles***: 10
  - ***Connection cycle time***: Activate "Calculate automatically" checkbox
- Configure the following data settings for the connection:
  - ***Function code***: Read Input Register 3x
  - Start address and data length for receive:
    - ***Start address***: 24

- ***Data length***: 14

I/O mapping

Besides a Modbus/TCP Client connection, a block instance of FS_Key-InPocket_SignInOut must be created and configured for each PITreader in a Key-in Pocket system.

▶ In the PAS4000 I/O Mapping Editor, map the I-PI variable *PITreaderAccessData* of each block instance to a Modbus/TCP Client connection.

8.4.2.3 Create user program for an access point

When creating the user program, please refer to the information on assigning the input and output interfaces, as well as the application guidelines in the PAS4000 Online Help.

Requirements of the user program

- Resource assignment of the user program

  Assign the user program to a task on the FS resource.

- Reaction times

  The general statements on the reaction times in the PSS 4000 System Description or in the PAS4000 Online Help apply.

- Required block instances

  Instances of the blocks in the Key-in-Pocket system must be created in the user program.

  – For the access point, one instance of the block FS_KeyInPocket_SignInOut

  – Per key-in-pocket system, one instance of the block FS_KeyInPocket_Manager

  – If necessary:
  per blind spot check, one instance of the block FS_KeyInPocket_BlindSpotCheck

  We recommend that the block instances are called in the documented order.

Recommended order in the user program

- Create and call up the "Access point" program section

  In the "Access point" program section, the access device (PITreader with assigned pushbutton) must be evaluated using the block FS_KeyInPocket_SignInOut.

- Create and call up the "Key-in-Pocket Manager" program section

  In the "Key-in-Pocket Manager" program section, the sign in list must be evaluated and monitored using the block FS_KeyInPocket_Manager, depending on the application.

- If applicable: Create and call up the "Blind spot check" program section

  In the "Blind spot check" program section, the blind spot check must be evaluated using the block FS_KeyInPocket_BlindSpotCheck, depending on the application.

Example of the order in the user program

```
//Access point
    FS_KeyInPocket_SignInOut_01(
    ActivateSignInOut := TRUE,
    SignInOutPermission := USINT#5,
    SignInOut := SignInOut_01,
    SignInOut_Valid := SignInOut01_Valid
    );

// Key-in-Pocket Manager
```

```
     FS_KeyInPocket_Manager(
     NumberOfChannels := USINT#1,
     SignInOutData := FS_KeyInPocket_SignInOut_01.SignInOutData,
     DeactivateBlindSpotCheck := FALSE,
     BlindSpotCheckOK := FS_KeyInPocket_BlindSpotCheck_01.Blind-
     SpotCheckOK,
     Enable => Enable,
     SignInStatus1 => SignInStatus1
     );

//Blind spot check
     FS_KeyInPocket_SignInOut_11(
     ActivateSignInOut := FALSE,
     SignInOutPermission := USINT#5
     );

     FS_KeyInPocket_BlindSpotCheck_01(
     ActivateBlindSpotCheck := FS_KeyInPocket_Manager.Activ-
     ateBlindSpotCheck,
     RequiredSecurityID := FS_KeyInPocket_Manager.SecurityID_Blind-
     SpotCheck,
     RequiredSerialNumber := FS_KeyInPocket_Manager.SerialNum-
     berBlindSpotCheck,
     SignInOutData := FS_KeyInPocket_SignInOut_11.SignInOutData,
     ConfirmCheck := ConfirmCheck,
     ConfirmCheck_Valid := ConfirmCheck_Valid,
     ReadyForCheck => ReadyForCheck
     );
```

I/O mapping

The I/O mapping must be performed in the PAS4000 I/O Mapping Editor.

- Map the I/O variables to the inputs and outputs to which the external pushbuttons and display elements are connected.
- Map the I-PI variable *PITreaderAccessData* to a Modbus/TCP Client connection.

8.4.2.4 Create user program for multiple access points

Prerequisites

- Multiple access points (safety gates);

  The following assumes the maximum expansion of 10 access points;
  i.e. FS_KeyInPocket_Manager: I-variable *NumberOfChannels* = 10
- The MUX multiplexer from the elementary library is used.
- PI variables are declared for the pushbuttons and display elements.
- With the I-PI variables, one variable each is declared for the valid bit.
- A *SignInOutData* variable with the derived data type *KeyInPocketData* is declared.

Note: For reasons of clarity, not all input and output variables are listed. Please refer to the information on assigning the input and output interfaces, as well as the application guidelines in the PAS4000 Online Help.

Requirements of the user program

- Resource assignment of the user program

  Assign the user program to a task on the FS resource.
- Reaction times

  The general statements on the reaction times in the PSS 4000 System Description or in the PAS4000 Online Help apply.

  Note:

  An increasing number of access points may mean there is a noticeable delay when displaying the sign in status. In a worst case scenario (task cycle time 100 ms, 10 access points), after a valid pushbutton operation to sign in or sign out, it may take approx. 1 second before the entry in the sign in list is changed and the status of the assigned display element changes.
- Required block instances

  Instances of the blocks in the Key-in-Pocket system must be created in the user program.

  – Per access point, one instance of the block FS_KeyInPocket_SignInOut
    In this case: 10 instances of FS_KeyInPocket_SignInOut

  – Per key-in-pocket system, one instance of the block FS_KeyInPocket_Manager

  – If necessary:
    per blind spot check, one instance of the block FS_KeyInPocket_BlindSpotCheck

  We recommend that the block instances are called in the documented order.

Recommended order in the user program

- Create and call up the "Access point" program section

  In the "Access point" program section, the access devices (PITreader with assigned pushbutton for confirmation) must be evaluated using the block FS_KeyInPocket_SignInOut.

  – Create an instance of the block FS_KeyInPocket_SignInOut for each access device.

  – Connect the O-variable *SignInOut* of each instance of FS_KeyInPocket_SignInOut to the corresponding I-variable *Channel1 … Channel10* on the MUX multiplexer.
- Create and call up the "Key-in-Pocket Manager" program section

In the "Key-in-Pocket Manager" program section, the sign in list must be evaluated and monitored using the block FS_KeyInPocket_Manager, depending on the application.

- Create an instance of the block FS_KeyInPocket_Manager to manage the sign in list.
- Connect the I-variable *SignInOutData* of FS_KeyInPocket_Manager to the O-variable *Out* on the MUX multiplexer. Establish the connection using the variable *SignInOutData*.

- If applicable: Create and call up the "Blind spot check" program section

  In the "Blind spot check" program section, the sign in list must be evaluated and monitored using the block FS_KeyInPocket_BlindSpotCheck, depending on the application.

  - Create an instance of the block FS_KeyInPocket_BlindSpotCheck for each blind spot that is to be monitored.

Example of the order in the user program

```
// Access point 1 … 10
      FS_KeyInPocket_SignInOut_01(
      ActivateSignInOut := TRUE,
      SignInOutPermission := USINT#5,
      SignInOut := SignInOut_01,
      SignInOut_Valid := SignInOut01_Valid
      );

      FS_KeyInPocket_SignInOut_02(..);
      ...
      FS_KeyInPocket_SignInOut_10(..);


// Multiplexer
      SignInOutData := MUX(
      K := FS_KeyInPocket_Manager.Channel,
      IN0 := FS_KeyInPocket_SignInOut_01.SignInOutData,
      IN1 := FS_KeyInPocket_SignInOut_02.SignInOutData,
      IN2 := FS_KeyInPocket_SignInOut_03.SignInOutData,
      IN3 := FS_KeyInPocket_SignInOut_04.SignInOutData,
      IN4 := FS_KeyInPocket_SignInOut_05.SignInOutData,
      IN5 := FS_KeyInPocket_SignInOut_06.SignInOutData,
      IN6 := FS_KeyInPocket_SignInOut_07.SignInOutData,
      IN7 := FS_KeyInPocket_SignInOut_08.SignInOutData,
      IN8 := FS_KeyInPocket_SignInOut_09.SignInOutData,
      IN9 := FS_KeyInPocket_SignInOut_10.SignInOutData
      );


// Key-in-Pocket Manager
```

```
      FS_KeyInPocket_Manager(
      NumberOfChannels := USINT#10,
      SignInOutData := SignInOutData,
      DeactivateBlindSpotCheck := FALSE,
      BlindSpotCheckOK := FS_KeyInPocket_BlindSpotCheck_01.Blind-
      SpotCheckOK,
      Enable => Enable,
      SignInStatus1 => SignInStatus1,
      ...
      SignInStatus10 => SignInStatus10
      );

// Blind spot check
      FS_KeyInPocket_SignInOut_11(
      ActivateSignInOut := FALSE,
      SignInOutPermission := USINT#5
      );

      FS_KeyInPocket_BlindSpotCheck_01(
      ActivateBlindSpotCheck := FS_KeyInPocket_Manager.Activ-
      ateBlindSpotCheck,
      RequiredSecurityID := FS_KeyInPocket_Manager.Secur-
      ityID_BlindSpotCheck,
      RequiredSerialNumber := FS_KeyInPocket_Manager.SerialNum-
      berBlindSpotCheck,
      SignInOutData := FS_KeyInPocket_SignInOut_11.SignInOutData,
      ConfirmCheck := ConfirmCheck,
      ConfirmCheck_Valid := ConfirmCheck_Valid,
      ReadyForCheck => ReadyForCheck
      );
```

I/O mapping

The I/O mapping must be performed in the PAS4000 I/O Mapping Editor.

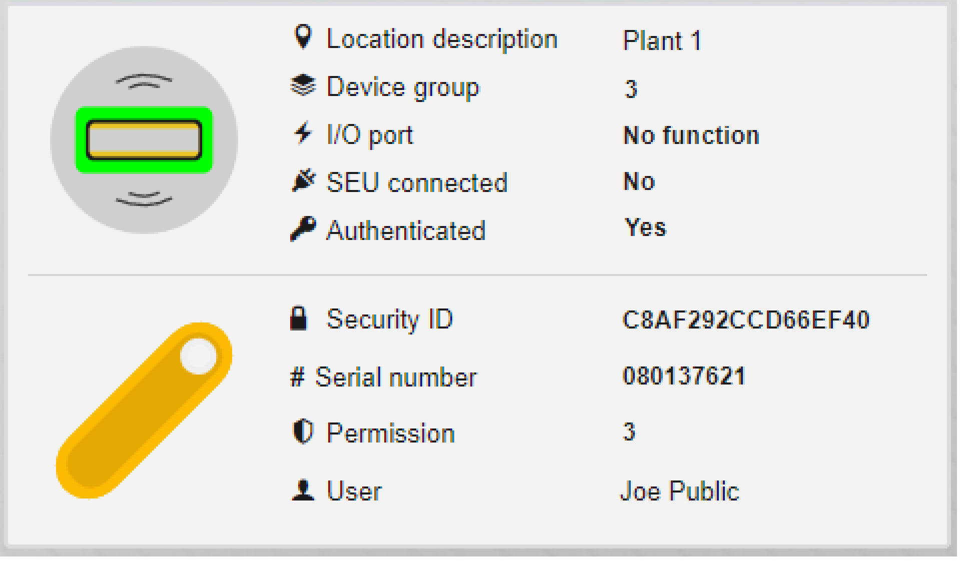
- Map the I/O variables to the inputs and outputs to which the external pushbuttons and display elements are connected.
- Map the relevant Modbus/TCP Client connections to the I-PI variables *PITreaderAccessData*.

8.5 Visualisation

Various information about the Key-in-Pocket system can be displayed in the PASvisu visualisation.

8.5.1 Show PITreader status

Status information for the PITreader and the transponder can be displayed for each PITreader configured as the data source in the PASvisu project.



Location description	Plant 1
Device group	3
I/O port	No function
SEU connected	No
Authenticated	Yes
Security ID	C8AF292CCD66EF40
# Serial number	080137621
Permission	3
User	Joe Public

Fig.: PITreader status tile

The "PITreader status" tile is used for the display.

It is possible to configure:

- Whether the status of the PITreader and the transponder is to be displayed, or just one of the two
- Whether only the icons for the PITreader/transponder are displayed or also the texts on the right-hand side

Details of the tile can be found in the PASvisu Builder Online Help.

8.5.2 Show sign in list

The sign in lists can be displayed for each PSS 4000 project that is configured as the data source in the PASvisu project and contains one or more FS_KeyInPocket_Manager blocks.

The number of users who are currently signed in to the sign in list is displayed:

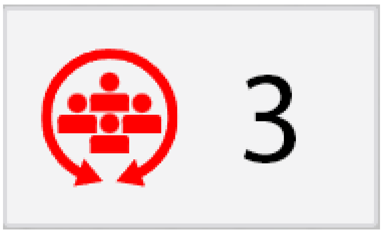
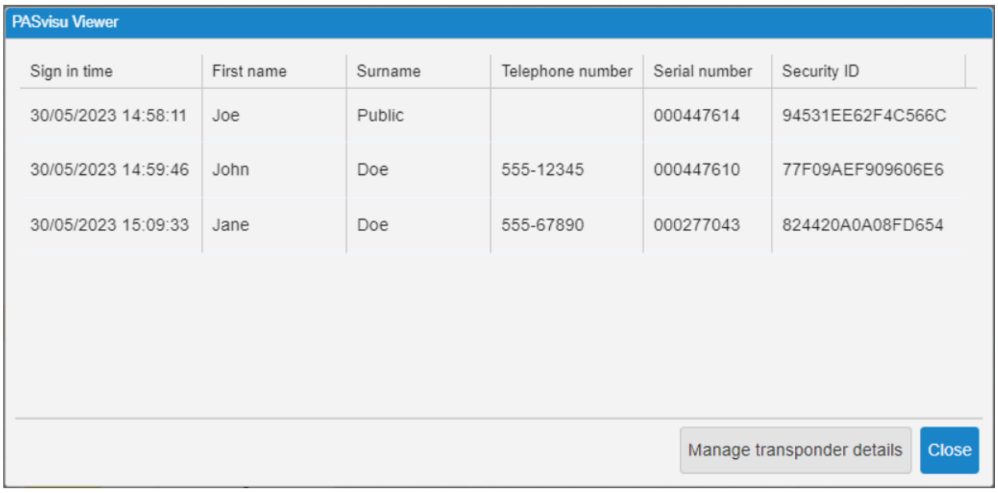


Fig.: Key-in-Pocket sign in list tile

The content of the sign in list is displayed by clicking on the tile:



Sign in time	First name	Surname	Telephone number	Serial number	Security ID
30/05/2023 14:58:11	Joe	Public		000447614	94531EE62F4C566C
30/05/2023 14:59:46	John	Doe	555-12345	000447610	77F09AEF909606E6
30/05/2023 15:09:33	Jane	Doe	555-67890	000277043	824420A0A08FD654

Fig.: Content of the sign in list

The "Key-in-Pocket sign in list" tile is used for the display. A separate tile is required for each sign in list.

Details of the tile can be found in the PASvisu Builder Online Help.

INFORMATION

The "Key-in-Pocket sign in list" tile is available in the PASvisu Builder from Version 1.14.0.

8.5.3 Show status information for the Key-in-Pocket system

All I- and O-variables of the blocks FS_KeyInPocket_Manager, FS_KeyInPocket_SignInOut and FS_KeyInPocket_BlindSpotCheck can be displayed in the PASvisu visualisation. See the PASvisu Builder Online Help, under "Notes on PSS 4000 project as data source".

8.6 Delete sign in list

The situation can arise where a plant cannot be put back into operation because there are entries in the sign in list, even though there is nobody left in the danger zone:

- People have failed to sign out correctly before leaving the danger zone.
- People have lost their transponder.

In these cases, the sign in list can be deleted manually.

NOTICE

Permission to delete the sign in list

Take appropriate measures to ensure that the ability to delete the sign in list is restricted to those with relevant training. Manual deletion must not be a routine action.

For example, restrict a transponder to certain permissions or use a PITreader that is specifically intended for this activity.

The person authorised to delete the sign in list must use their transponder to authenticate themselves and be signed in to the sign in list. The pushbutton to delete the sign in list must then be operated.

The enable through the Key-in-Pocket system occurs once the person who has deleted the sign in list signs out.

8.7 Diagnostics

Blocks belonging to the Key-in-Pocket system: FS_KeyInPocket_SignInOut, FS_KeyInPocket_Manager and FS_KeyInPocket_BlindSpotCheck, signal a variety of diagnostic information to the O-variables *Diag…*<*…*>.

These O-variables can be used to continue processing diagnostic information in the user program. A description of the diagnostic information can be found in the block descriptions (PAS4000 Online Help). Under the default setting, all diagnostic information also appears in the safety controller's diagnostic list and diagnostic log. If individual or all diagnostic messages are unwanted, then the corresponding basic diagnostic items in PAS4000's Diagnostic Editor can be deactivated (deactivate "Enable" checkbox).
Detailed information on system diagnostics and process diagnostics can be found in the PAS4000 Online Help.

8.8 Examples

8.8.1 2 access points and 1 blind spot

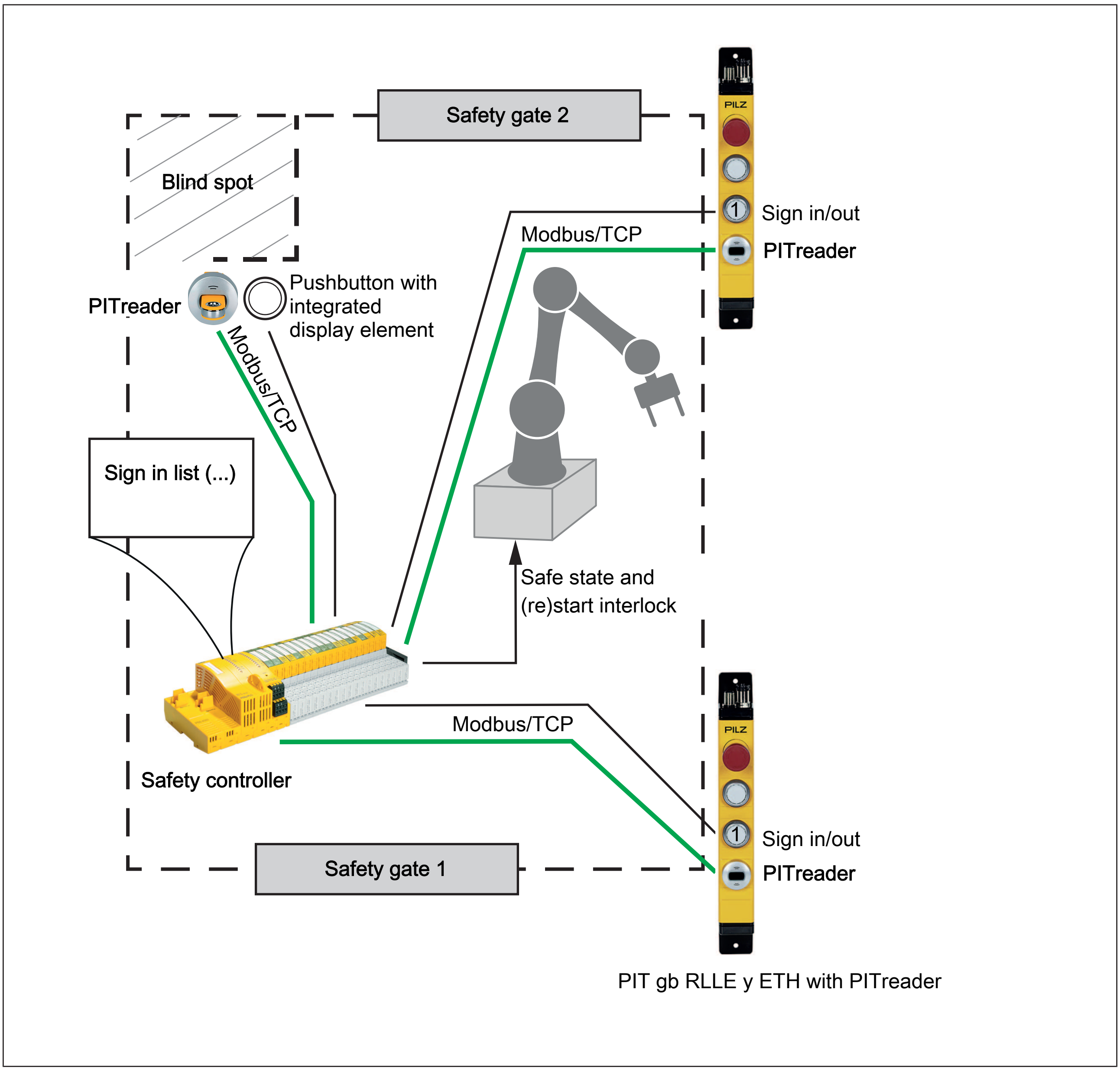
System overview

The Key-in-Pocket system consists of the following components:

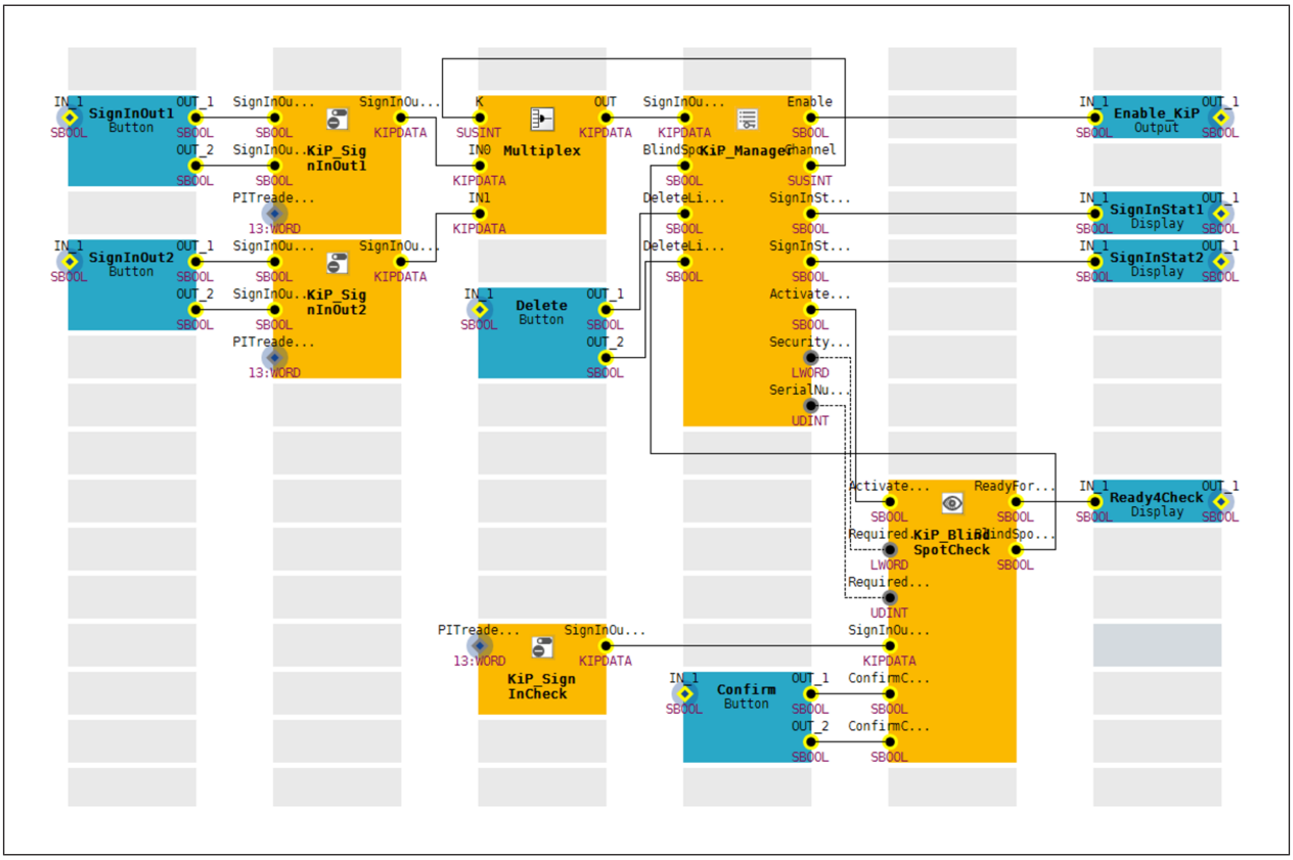
- Two safety gates as access points
- One PITreader on each safety gate
- One pushbutton on each safety gate to sign in to the sign in list and sign out of the sign in list (Sign in/out)
- One PITreader and one pushbutton in the area of the blind spot to confirm the blind spot check (Confirm).
- One pushbutton on safety gate 1 to delete the sign in list (Delete list)

A person can sign in and out via one of the two PITreader devices.

In this example, there is no monitoring as to whether the safety gates are closed or will be locked. If necessary, these conditions must be implemented separately.


Safety gate 2
Blind spot
Modbus/TCP
Sign in/out
PITreader
PITreader
Pushbutton with
integrated
display element
Modbus/TCP
Sign in list (...)
Safe state and
(re)start interlock
Modbus/TCP
Safety controller
Sign in/out
PITreader
Safety gate 1
PIT gb RLLE y ETH with PITreader

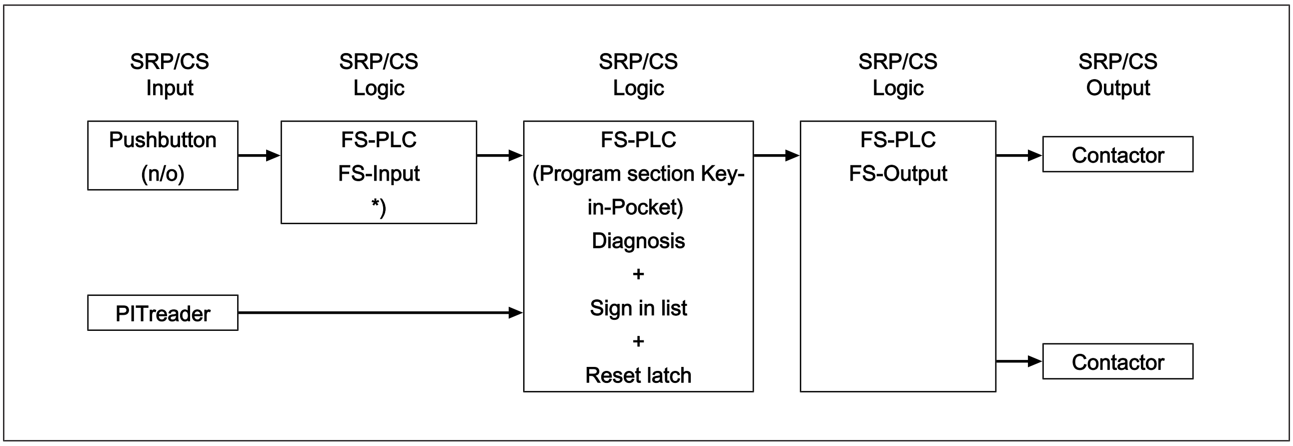
Programming in PAS4000 (Multi programming)



9 Calculating the safety characteristic data

All the units used within a safety function must be considered when calculating the safety characteristic data.

Safety-related architecture



*) The share of the safety controller’s single-channel safety input on the PL is so low that it can be ignored and does not need to be taken into account in the calculation.

The safety function depends equally on both input functions (pushbutton and PITreader). The PITreader can therefore be regarded as a channel of the "Input" subsystem.

In accordance with EN ISO 13849-1, the following parameters may be applied for the PITreader:

- DC 90 % (through dynamic principles, signature and code protection)
- $MTTF_D$ = 2 x MTBF = 72 years

In accordance with EN ISO 13849-1, the following parameters may be applied for the external pushbutton with N/O contact:

- DC 90 % (shorts between contacts in the wiring are also detected)
- Measures against CCF (min. score of 65 in accordance with Table F.1 (EN ISO 13849-1) can be considered to have been fulfilled if the user can confirm that the items marked "Customer" have been fulfilled (see table below).

No.	Measures against CCF	Score	Con-firmed by
1	Physical separation between signal paths, for example: ▸ Separation in wiring/piping ▸ Detection of short circuits and open circuits in cables by dynamic test ▸ Separate shielding for the signal path of each channel ▸ Sufficient clearances and creepage distances on printed-circuit boards	**15**	**Pilz**
3.1	Protection against over-voltage, over-pressure, over-current, over-temperature, etc.	**15**	**Customer**
6.1	For electric/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326-3-1) Fluidic systems: Filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium NOTE: For combined fluidic and electric systems, both aspects should be considered.	**25**	**Pilz**
6.2	Other influences: Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).	**10**	**Customer**
	Total	**65**	

Extract from Table F.1 (EN ISO 13849-1)

- The user must provide the following data:
  - The pushbutton must meet Cat. B
  - To calculate the $MTTF_D$ of the pushbutton:
  - $B10_D$ value
  - n_{op} (average number of operations per year) of the pushbutton

INFORMATION

A safety function's SIL/PL values are **not** identical to the SIL/PL values of the units that are used and may differ from these. We recommend that you use the PAScal software tool from Pilz to calculate the safety function's SIL/PL values.

10 Calculation example for a safety function

Safety characteristic data, input (pushbutton) channel 1	
DC	90%
CCF	Min. 65 score
Pushbutton must meet Cat. B	
B10$_D$ (2 x B10)	B10 = 1,300.000 (in accordance with the operating manual PIT gb RLLE y ETH) x 2 = 2,600,000
n$_{op,}$ number of operations is assumed	50 operations per day x 220 days = 11,000 operations per year
MTTF$_D$	B10$_D$ / 0.1 x n$_{op}$ = 2,600,000 / 0.1 x 11,000 = 2,363.63 years Restricted to 100 years

Safety characteristic data, input (PITreader) channel 2	
DC	90%
MTTF$_D$	2 x MTBF = 72 years

Safety characteristic data, input (channel symmetrisation)	
MTTF$_{D\ sym}$	$\mathrm{MTTF_D} = \frac{2}{3}\left[\mathrm{MTTF_{DC1}} + \mathrm{MTTF_{DC2}} - \frac{1}{\frac{1}{\mathrm{MTTF_{DC1}}} + \frac{1}{\mathrm{MTTF_{DC2}}}}\right]$ = 2 / 3 [100 + 72 - 1 / 1/100 + 1/72] = 86.759 years
Category	3
DC$_{avg}$	90%
PFH$_D$ input, in accordance with Table K.1 from the standard EN ISO 13849-1	5,79E-08 [1/h]

Safety characteristic data, logic	
PFH$_D$ PNOZ m B1	4,19E-10
PFH$_D$ PNOZ m EF 8DI4DO (logic)	2,84E-10
PFH$_D$ PNOZ m EF 8DI4DO (output)	1,64E-10

Safety characteristic data, output (contactor)	
$B10_D$, in accordance with Table C.1 from the standard EN ISO 13849-1, for "Contactors with nominal load"	1,300,000
n_{op}, number of operations is assumed	5 operations per day x 220 days = 1,100 operations per year
$MTTF_D$	$B10_D$ / 0.1 x n_{op} = 1,300,000 / 0.1 x 1,100 = 11,818.18 years Restricted to 2500 years
PFH_D output, in accordance with Table K.1 from the standard EN ISO 13849-1	With "$MTTF_D$ for each channel" 2500 years, "Cat.4, DC_{avg} = high" = 9,06E-10 [1/h]

Safety characteristic data, total

PFH_D PITreader/pushbutton	5,79E-8 [1/h]
PFH_D PNOZ m B1	4,19E-10 [1/h]
PFH_D PNOZ m EF 8DI4DO (logic)	2,84E-10 [1/h]
PFH_D PNOZ m EF 8DI4DO (output)	1,64E-10 [1/h]
PFH_D Contactors redundant with nominal load	9,06E-10 [1/h]

Total value PFH_D

= 5,79E-8 [1/h] + 4,19E-10 [1/h] + 2,84E-10 [1/h] + 1,64E-10 [1/h] + 9,06E-10 [1/h]

= 5,97E-08 [1/h]

Performance level (PL)

Total value, mathematical evaluation PFH_D 5,97E-08 [1/h]

= PLe in accordance with the standard EN ISO 13849-1

NOTICE

Achievable performance level (PL)

The maximum achievable performance level (PL) is restricted to PL d due to a system limitation.

Support

Technical support is available from Pilz round the clock.

Americas

Brazil	+55 11 97569-2804
Canada	+1 888 315 7459
Mexico	+52 55 5572 1300
USA (toll-free)	+1 877-PILZUSA (745-9872)

Asia

China	+86 21 60880878-216
Japan	+81 45 471-2281
South Korea	+82 31 778 3300

Australia and Oceania

Australia	+61 3 95600621
New Zealand	+64 9 6345350

Europe

Austria	+43 1 7986263-0
Belgium, Luxembourg	+32 9 3217570
France	+33 3 88104003
Germany	+49 711 3409-444
Ireland	+353 21 4804983
Italy, Malta	+39 0362 1826711
Scandinavia	+45 74436332
Spain	+34 938497433
Switzerland	+41 62 88979-32
The Netherlands	+31 347 320477
Turkey	+90 216 5775552
United Kingdom	+44 1536 462203

You can reach our international hotline on:
+49 711 3409-222
support@pilz.com

Pilz develops environmentally-friendly products using ecological materials and energy-saving technologies. Offices and production facilities are ecologically designed, environmentally-aware and energy-saving. So Pilz offers sustainability, plus the security of using energy-efficient products and environmentally-friendly solutions.

BLUECOMPETENCE Alliance Member
Partner of the Engineering Industry Sustainability Initiative

We are represented internationally. Please refer to our homepage www.pilz.com for further details or contact our headquarters.

Headquarters: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Germany
Telephone: +49 711 3409-0, Telefax: +49 711 3409-133, E-Mail: info@pilz.com, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY

CECE®, CHRE®, CMSE®, InduraNET p®, Leansafe®, Master of Safety®, Master of Security®, PAS4000®, PAScal®, PASconfig®, Pilz®, PIT®, PLID®, PMCprimo®, PMCprotego®, PMCtendo®, PMD®, PMI®, PNOZ®, PRBT®, PRCM®, Primo®, PRTM®, PSEN®, PSS®, PVIS®, SafetyBUS p®, SafetyEYE®, SafetyNET p®, THE SPIRIT OF SAFETY® are registered and protected trademarks of Pilz GmbH & Co. KG in some countries. We would point out that product features may vary from the details stated in this document, depending on the status at the time of publication and the scope of the equipment. We accept no responsibility for the validity, accuracy and entirety of the text and graphics presented in this information. Please contact our Technical Sup if you have any questions.

1006613-EN-02, 2023-07 Printed in Germany