Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern,
Germany
Deutschland/Germany
www.pilz.com

Holistic safety concepts focus on access in order to ensure safety and industrial security at the machine

Holistic safety through personalised permission management

Ostfildern, February 2023 – **We use gates, locks and keys to limit access wherever we want to protect something important. This is also true for the ultimate asset: our safety in all its forms. In the industrial environment, the goal on the one hand is to protect people (safety) and on the other to protect machinery and sensitive data (industrial security). A lack of safety and security can have various consequences: from incorrect operation to an accident to a serious cyber attack. Comprehensive Identification and Access Management that clearly defines access and entry permissions contributes to a holistic safety and industrial security concept and efficient procedures.**

In the production environment they are a familiar sight: guards that give humans a clear signal that there is a hazardous area behind the safety gate and that care must be taken. People gain access to the process behind the safety fence via a human machine interface (HMI) or a key. But what if the person is not at all qualified or authorised for this and places themselves or other people in danger? A person with malicious intent can also tamper with the process – whether directly at the machine or via remote access. The topic of access permission shows that safety and industrial security are closely linked. Or taking it a step further: industrial security ensures the integrity of safety at the machine. For example, it offers protection of plant or machinery in production against unauthorised access from outside, and protects sensitive process and machine

data from falsification, loss and unauthorised access internally. This includes explicit attacks as well as unintentional security incidents.

Safety and industrial security belong together

Operators of plant and machinery must be able to clearly issue and assign tasks and permissions, in effect establishing Identification and Access Management. This means not only organisational measures such as work instructions or regular checks of procedures, but also the integration of appropriate security solutions in the production environment. If these measures are neglected, the responsible parties in a company can be held personally liable in the event of accidents or production downtimes. These type of security solutions were previously on a voluntary basis; in many places no need for action was identified. This link between safety and security has since been recognised by lawmakers, however. The new Machinery Regulation therefore stipulates compulsory security measures.

Operating modes increase safety

Various C standards also already stipulate that different operating modes must also contain corresponding safety functions. Operating modes can be automatic mode, manual intervention under restricted conditions or service mode, for example. EN ISO 16090-1 stipulates at least two of these operating modes as mandatory for machining centres and special purpose machinery in order to guarantee functional safety. It is vital that only one operating mode at a time is selected and active and that this is clearly displayed.

Prevent anonymous access

But how do you decide which people have access during which operating mode or can even change the operating mode? For this

purpose, different groups of people who come into contact with the machine are defined, for example operating, cleaning or maintenance staff. The employees are then assigned to the groups according to their tasks or qualification. Depending on the size of the company, enables or access rights can also be issued for different user groups or, for example, for a machine type that is used across the company. During a risk assessment, safety experts evaluate the risk of anonymous access for every hazard and rate it. Measures to reduce the risk are finally defined according to the state of the art and taking into consideration the harmonised standards.

User-friendliness prevents manipulation

When implementing the measures, it is important to ensure ease of handling and usability for users at the company to preclude manipulation. This applies already in the development process for machine builders. Intuitive operating systems that are easy for users to handle prevent workers from bypassing safety precautions or operating machinery incorrectly. A well-considered safety system also contributes to efficient procedures without unnecessary downtimes. This issue of “Defeating safeguards” is a key aspect of EN ISO 14119. The standard defines guiding principles for the design and selection of safety gate systems and therefore offers practical guidance on how to prevent manipulation.

Individual safety concept

To ensure that no hazards arise if access doors are opened, whether deliberately or by accident, these are protected using a safety gate system. In terms of safety, the focus here is on the protection of the worker against hazardous machine movements. Depending on whether it is a stand-alone machine or complex

interlinked plants, a suitably tailored safety concept is required. If machinery has a hazardous overrun, guard locking will be important. If gates are accessible, an escape release is a must.

Tailored safeguarding of safety gates

A modular safety gate system such as PSENmlock from Pilz combines safety gate monitoring with safe guard locking inside one system and also provides safety functions such as emergency stop, escape release and a mechanical restart interlock. It offers flexibility and decentralised intelligence to safeguard a wide range of applications. An individual solution is comprised of a combination of sensors, escape release, door handles and a control and pushbutton unit. Depending on the application, users design their own customised safety gate solution. To meet the demands for industrial security, the focus is now on access and permissions.

One system for safety and industrial security

Protection against unauthorised access can be implemented in practice with an operating mode selection and access permission system. It combines safety and industrial security: the selection of the operating mode and permission control for machine access. This type of solution is provided by the devices from Pilz's PITmode product group. These allow switching between defined operating modes and control of access permission. Operation is intuitive, as each user receives an individual transponder that enables clear user authentication and prevents manipulation.

Individual management of access and operating modes

PITmode is available in various versions to allow for an individual design of the safety concept. As a compact all-in-one device, PITmode includes the pushbuttons for operating mode selection as

well as an evaluation unit, thus saving space on the installation. The modular system PITmode fusion, on the other hand, consists of the reading unit PITreader with RFID technology and integrated web server as well as a safe evaluation unit (SEU). Another version is the PITmode flex: PITreader is used here together with a Pilz controller and a software block for safe evaluation. The modular setup allows the access permission and operating mode selection to be integrated into the design of existing control consoles. Existing buttons can be used for the selection of the operating mode, which enables easy operation for the user. Identification with the transponder is performed by the reading unit PITreader. PITmode and PITmode fusion provide functionally safe operating mode selection and access permission up to PL d.

Simple authentication – even remotely

To select the operating mode, the user connects their transponder directly to the PITmode and presses a button defined for the operating mode or the corresponding button on an HMI. If the user has the permission, they receive access to the process. The same also applies if a service employee wants to access a machine via remote maintenance: remote maintenance can only be started if a person on site gives the corresponding enable in the system. After the maintenance work, this access is closed again before the machine starts back up. Manipulation by unauthorised parties or a port that inadvertently remains open following the maintenance work can thus be ruled out. Operating companies increase industrial security because they control who has what permission and therefore who is granted access to the process.

Complete solution for access management

If only access control is to be performed, PITreader can also be used as an access permission system as a stand-alone device or in combination with a controller from Pilz. In combination with the configurable small controller PNOZmulti 2, the administrator easily configures the access permissions for plant and machinery using “drag and drop” with the associated configuration tool PNOZmulti Configurator. These are then transferred to the RFID transponder key via the reading unit PITreader. The version PITreader S can also be used with devices from other manufacturers through the integration of the OPC UA standard, independent of a Pilz controller. As already mentioned, PITmode devices can be easily integrated in existing control panels.

The choice between key, card or sticker

The version PITreader card unit offers additional flexibility for operators and users: RFID-capable cards and stickers can be used together with or instead of an RFID transponder key. If the company already uses RFID-capable cards, these can also be used in conjunction with PITreader card unit: in this case, users need only one card for multiple functions. In general, the advantage of the RFID transponders – whether key, card or sticker – lies in the fact that several functions can be bundled on one transponder, thereby consolidating an entire mechanical key ring. This is convenient for the user because they only need to carry one identification medium. Administrators also save time and effort when managing and maintaining the keys.

A plus for security

Security aspects are also considered with a view to user authentication, qualification and access protection. If, despite all safety and security measures, an accident or a security incident

does occur at the machine, the RFID transponder can be read out to determine who made which change. If this optional function is desired, the control system uses the authentication to also record the access time in the internal, non-modifiable audit trail (event log).

Careful administration is the key

To ensure that safety and industrial security are guaranteed across the entire lifecycle of the application, administrators put a lot of effort into maintaining the permissions. To ensure simple administration, the appropriate software tools from Pilz support the organisation of users and transponders. This means that complex permissions matrices or group-wide specifications can be concealed in a small RFID key. With the integrated PITreader web server, administrators program the RFID transponders that belong to PITmode or PITreader and store the user data and permissions on them. All important settings are made directly on the reading unit, which speeds up commissioning, including the configuration of interfaces.

Limit access to interfaces

The possibilities of Identification and Access Management extend to enabling special industrial USB ports, one of the main gateways in security incidents. The access permission system PITreader is combined with an operation element such as PIT oe USB that has an activatable USB 2.0 host interface. This solution enables the manipulation-proof import of programs, export of data and connection of a keyboard or mouse. Because the activation of the interface is performed exclusively with corresponding permission, thereby protecting the data flow of a production facility. Together with an industrial firewall such as SecurityBridge from Pilz, which controls the data communication within an industrial automation

network, machines can be protected against unauthorised access and manipulation.

Existing machinery – safe and secure

If existing machinery is updated to the state of the art or if a need for action is identified as part of a risk assessment, the access permission system PITreader can be easily retrofitted: the device can be mounted directly using the standardised cut-outs for key switches with 22.5 mm diameter. Together with a Pilz controller, the desired security function can be set up directly. If a third-party controller is in use, PITmode fusion is used to integrate the evaluation of the access permission and operating mode. Depending on which transponder medium is being considered, existing RFID key cards in the company can be used for authentication.

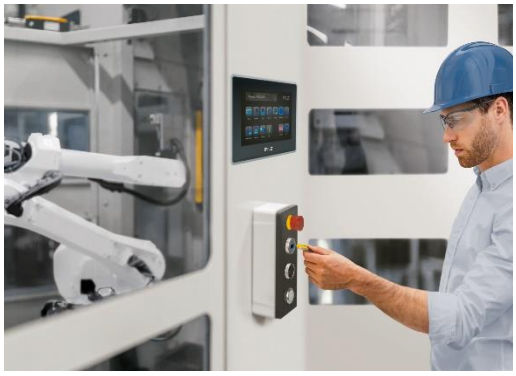
Conclusion

In order to protect the ultimate asset, namely our safety, it is necessary to design holistic safety concepts and to regularly examine whether they are up to date. An important element is Identification and Access Management, which clearly regulates permissions and access in a company. The solution is a concept that includes measures and specifications and also contains appropriate safety and security functions. An access permission system such as PITreader is the appropriate hardware block for this when rounded out with the supplemental software components for organising users and transponders. Additional components such as safety gate systems, controller and software as well as functions such as operating mode selection enhance the solution to form a holistic safety and industrial security concept. The system is easy for the user to handle, namely with the individual key in their hand.

Characters: 14,675

Figures

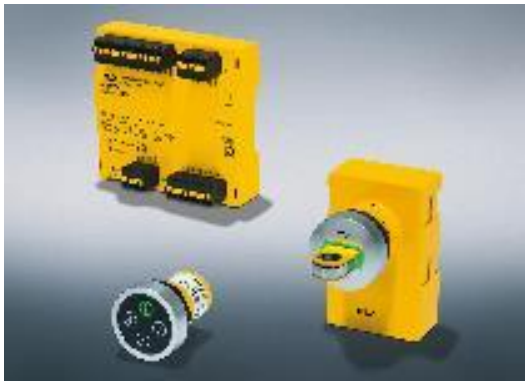
Fig. 1:
F_Press_IAM_Man_using_PITreader_Key_cold1.jpg (© Pilz GmbH & Co. KG)



CAPTION: A comprehensive Identification and Access Management controls access to the application, thereby ensuring the integrity of the safety functions and measures – including safety and industrial security.

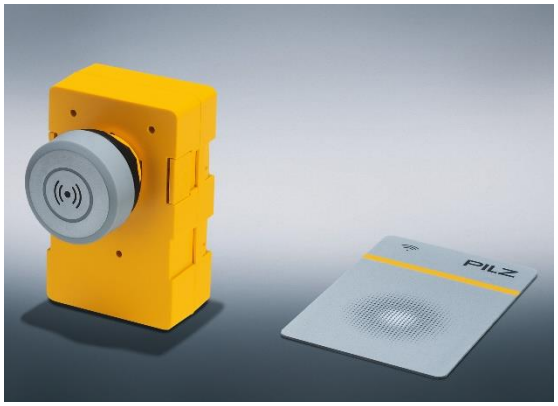
Fig. 2:

F_Press_PITmode_fusion_402251_PIT_oe_4023311_P1_B_8_2_cold_2020_01.jpg (Pilz GmbH & Co. KG)



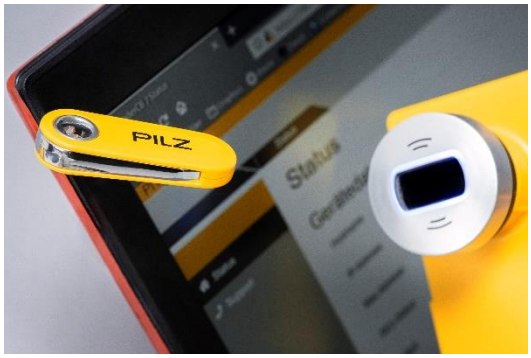
CAPTION: PITmode fusion from Pilz is a modular operating mode selection and access permission system that combines safety and industrial security in one system.

Fig. 3:
F_Press_PITreader_S_card_unit_402321_and_PITreader_card_ye_g_402330_P1_B8_2_cold.jpg (Pilz GmbH & Co. KG)



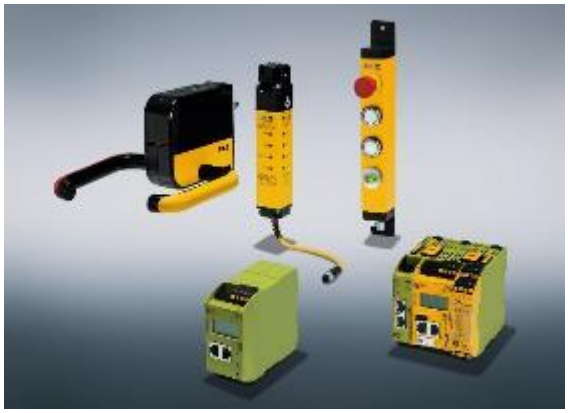
CAPTION: The access permission system PITreader card unit from Pilz together with the RFID-capable cards PITreader card and stickers PITreader sticker offers additional formats for implementing an efficient access permission system.

Fig. 4:
F_Press_PITreader_Webserver.jpg (© Pilz GmbH & Co. KG)



CAPTION: The RFID transponder keys are read and taught in the PITreader. The assignment of access permissions and operating modes is performed easily using the associated web server.

Fig. 5:
F_Press_Group_7_Modular_safety_gate_system_with_diagnostic_and_evaluation_P1_B8_2_cold.jpg (© Pilz GmbH & Co. KG)



CAPTION: The flexible combination of the safety gate system PSENmlock with the appropriate handle module (top left), the pushbutton unit PITgatebox with integrated access permission

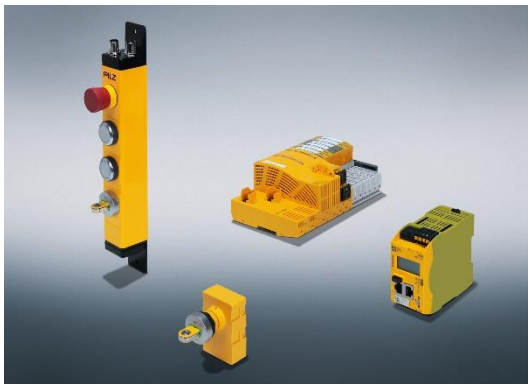
system PITreader (top right) and the configurable safe small controller PNOZmulti 2 (bottom right) plus the diagnostic solution Safety Device Diagnostics (bottom left) offers a complete safety gate solution with access permission.

Box: Digital maintenance safeguarding system Key-in-pocket

Beyond pure access permission, when combined with a Pilz controller such as the configurable safe small controller PNOZmulti 2 or the automation system PSS 4000, the PITreader can be used for efficient digital “Key-in-pocket” maintenance safeguarding. This ensures that the machine does not restart while maintenance work is being carried out and that unauthorised persons do not gain access. This is achieved as follows in practice: one or more users authorised for maintenance work authenticate themselves on the plant. After successful authentication, a personalised security ID is stored for the user in the Pilz controller, in a safe list. The machine can now be shut down, the safety gate opened and the machine accessed. During this time, the RFID keys remain with the respective users “in their pocket”. Once maintenance is complete and people have left the danger zone, everyone signs out. The security IDs are removed from the safe list on the Pilz controller and the machine can be restarted. In contrast to maintenance safeguarding with mechanical keys, it is possible to enter or exit the plant at any safety gate. In this way, “key-in-pocket” offers the personnel more flexibility and time savings during maintenance. Digital maintenance safeguarding is specifically designed for machines with danger zones that are protected via safety fences. At all times, the operator knows who has access for which task; temporary permissions can also be assigned.

1,578 characters

Fig. for key-in-pocket box:
F_Press_Group_PIT_Key_in_pocket_solutions_P1_B8_2_cold.jpg (© Pilz GmbH & Co. KG)



CAPTION: The maintenance safeguarding system “key-in-pocket” consists of the access permission system PITreader, pushbutton unit PITgatebox and a Pilz controller such as the configurable small controller PNOZmulti 2 or automation system PSS 4000.

Box: Assign and maintain permissions

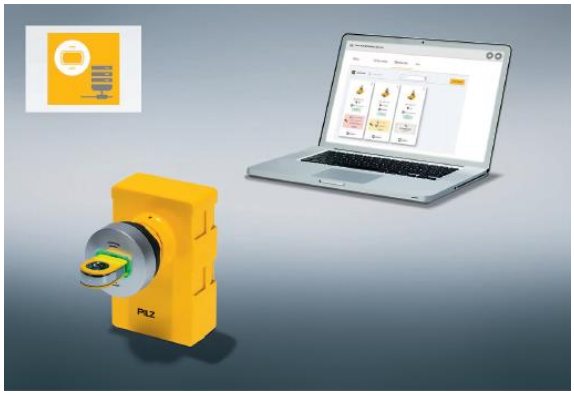
If an access permission system is used in the company, regular maintenance and management of the permissions and user data is vital to ensure a high degree of safety and security. Pilz provides the software tool PIT Transponder Manager (PTM) for this purpose: on a graphical interface, the administrator manages their user settings, block lists and user data. With pre-configured templates and in import function, individual user permissions are written to the transponder key in just a few steps.

If several PITmode or PITreader devices are in use at a company, these are organised using the software PIT User Authentication

Service (UAS) from Pilz. It enables the connection of management systems such as the PTM or a different user management software with PITreader. PIT UAS has a central authorisation database for users, thereby enabling the import and assignment of data from the PTM to all PITreader devices. Administrators can view the current status of all PITreaders and display a diagnostic list. In this way, a quick overview is also possible with the use of several devices.

1,218 characters

Fig. for user management box:
((Image to follow)).jpg (© Pilz GmbH & Co. KG)



CAPTION: If a company uses several reading units PITreader, these are organised using the User Authentication Service (UAS) software tool.

Pilz Group

The Pilz Group is a global supplier of products, systems and services for automation technology. The family business is based in Ostfildern and employs around 2,500 staff. With 42 subsidiaries and branches around the world, Pilz supplies safe solutions for human, machine and the environment.
The technology leader offers complete automation solutions comprising sensor, control and drive technology – including systems for industrial communication, diagnostics and visualisation. An international range of services with consultancy, engineering and training completes the portfolio. Pilz solutions are used in many industries beyond mechanical engineering, such as intralogistics, railway technology or the robotics sector for example.

www.pilz.com

Contact for the press:

Martin Kurth

Corporate and Technical Press
Tel: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

Technical and Corporate Press
Tel: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

Technical Press

Tel: +49 711 3409-1067
j.skarman@pilz.de

Sabrina Schilling

Technical Press

Tel: +49 711 3409-7147
s.schilling@pilz.de

Hansjörg Sperling-Wohlgemuth

Conference and Presentation Management
Tel: +49 711 3409-239
h.sperling@pilz.de