EUCHNER
More than safety.

EKS *Light* Selection of Operating Mode with Pushbuttons

Contents

Subject to technical modifications; no responsibility is accepted for the accuracy of this information.

Components/modules used

EUCHNER

Description	Order no./item designation
EKS *Light* compact or EKS *Light* modular with EKS FHM	109820 / EKS-A-IPL-G01-ST05/02 or 113647 / EKS-A-APR-G08 106585 / EKS-A-SFH-G30-2000 116118 / EKS-A-SFH-G30-ST150
EKS Electronic-Key	077859 / EKS-A-K1RDWT32-EU 084735 / EKS-A-K1BKWT32-EU 091045 / EKS-A-K1BLWT32-EU 094839 / EKS-A-K1GNWT32-EU 094840 / EKS-A-K1YEWT32-EU 123097 / EKS-A-K1WHWT32-EU 123098 / EKS-A-K1OGWT32-EU
EKM *Light*	111410 / ANWPG ELECTRONIC KEY MANAGER LIGHT
MSC base unit	121289 / MSC-CB-AC-FI8FO2-121289
Six-piece terminal set for MSC	121321 / AC-SC-04-V06-121321

Tip: More information and downloads about the aforementioned EUCHNER products can be found at www.euchner.com. Simply enter the order number in the search box.

Others

Description	Item
S7-300, CPU 315F-2 PN/DP	6ES7315-2FJ14-0AB0*)
SIMATIC DP, Power Module PM-E	6ES7138-4CA01-0AA0
Digital electronics module DI8/DO 8 DC24V	6ES7323-1BH01-0AA0
Totally Integrated Automation Portal Version V13 SP1	6ES7822-1AA04-0XC5
Pushbuttons	Any manufacturer; breaking capacity at least 100 mA/24 V DC

*) Another safe PLC in addition to the EUCHNER MSC is **not** required. The application was verified exclusively via the standard PLC of this S7 CPU.

Abbreviations

Abbreviation	Designation
EKS *Light*	The EKS used in operating state 6 or 7 in this application (refer to the EUCHNER components used and the EKS *Light* operating instructions 110845)
PLC	The conventional control system that is used and that offers PLC functionality
F-PLC	The fail-safe PLC used in this application
PL	Performance Level according to EN ISO 13849-1
PL_r	Performance Level required according to EN ISO 13849-1
SRASW	Safety-related application software according to EN

	ISO 13849-1
MSO Mode of Safe Operation	Selection of operating mode on a machine as required in various C standards (e.g. EN ISO 16090, EN ISO 23125, EN ISO 16089)

Functional description

General

Selection of operating mode is to be realized on a machine using the EKS *Light* as an access system. The operating mode is selected using pushbuttons. A key switch is not necessary. Evaluation and switchover of the operating mode are realized via a fail-safe programmable logic controller (F-PLC). Up to five access rights to the selection of operating mode can be defined using the EKS *Light*. Which operating modes the owner of the related Electronic-Key can select depends on the access rights.

Electronic-Key structure and operating state

The data on the Electronic-Key are structured as follows:

Byte no.	**Description**	**Type**	**Length**	**Explanation**
109	Operating state	Byte	1 byte	State of the EKS *Light*
110 – 111	Access rights	Word	2 byte	Authorization level for access to the machine's operating mode
112 – 113	Access code	Word	2 byte	Restriction of the machine or installation group (10 bits)
114 – 115	KEYCRC	CRC	2 byte	Checksum over a certain part of the Electronic-Key as copy protection
116 – 123	KeyID	KeyID	8 byte	The KeyID is a number that is permanently pre-programmed on the Electronic-Key by EUCHNER. This number is different for each Electronic-Key

For this application, the value 6 or 7 must be set on the EKS *Light* as the operating state. With this value, the EKS *Light* will operate in the operating state that is necessary for selection of operating mode. The same value must also be saved on the Electronic-Key. Use the EKM *Light* software for this purpose.

In operating state 6, a comparison is made with the access code as to whether the Electronic-Key has the same value as is set on the DIP switches in the device. The Electronic-Key is accepted only if the values match fully.

In operating state 7, a comparison is made with the access code as to whether the bit on the Electronic-Key has the value 1 in the same position as the bit that is set on the DIP switches. Only if both the Electronic-Key and the DIP switch have a 1 in this bit is the Electronic-Key accepted.

One of the five values MSO 1 to MSO SE must be saved in the "Access rights" field; this value permits one of several operating modes to be selected. The outputs A to D, as well as STR, are set to suit this field. Each of the five outputs represents allowed access rights. Only one output is ever set. The assignment of the data words to the outputs is described in Table 1.

A checksum is entered automatically in the KEYCRC field by the EKM *Light* administration program. This checksum is recalculated in the EKS *Light*. Only if the checksum calculation produces the same value as that saved on the Electronic-Key are the outputs of the EKS *Light* switched on.

Operating mode	Hex	Meaning	Symbol	Output
MSO_0	0F0FH	Mode of Safe Operation 0: Manual mode	✋	Output A set.
MSO_1	0FF0H	Mode of Safe Operation 1: Automatic mode	◉	Output B set.
MSO_2	3333H	Mode of Safe Operation 2: Setup mode	●	Output C set.
MSO_3	33CCH	Mode of Safe Operation 3: Automatic mode with manual intervention	Ⓣ	Output D set.
MSO_SE	3C3CH	Mode of Safe Operation Service: Operating mode for servicing and setup	🔧	Output STR set.

Table 1

A screen for the EKM *Light* input software (order no. 111410) is available for Electronic-Key management.

Block diagram and description

Operating modes MSO_1 to MSO_SE can be set on the machine in this example. Operating mode MSO_0, "Manual," is not available on fully automatic machines.

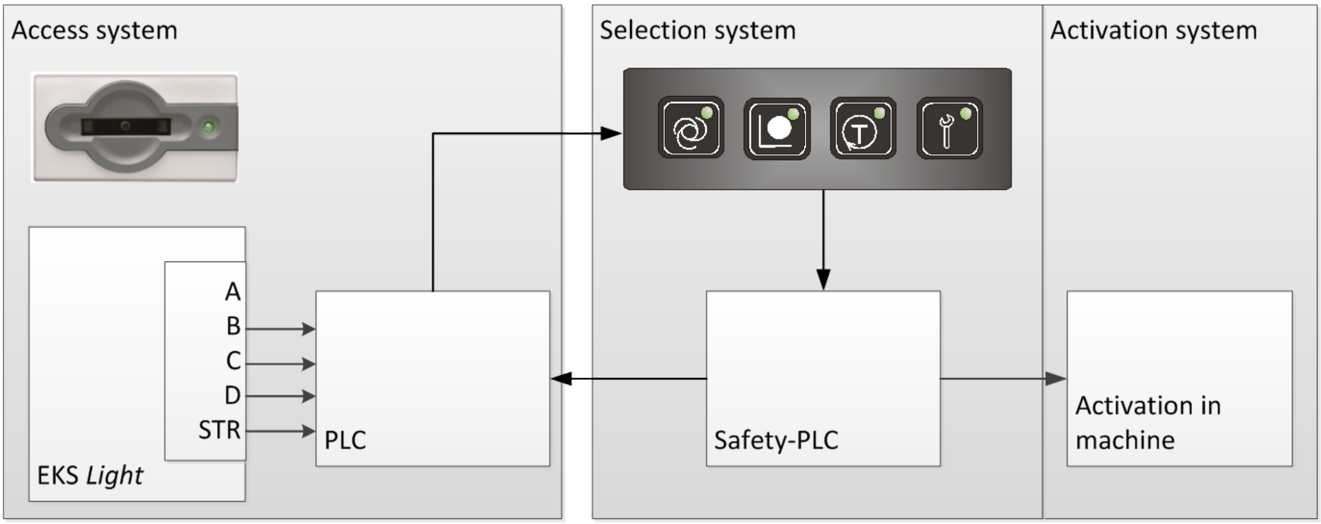

Figure 1

The highest permissible operating mode (access rights) is entered on each of the Electronic-Keys. For example, a person authorized to work in setup mode can always work in automatic mode as well. The EKS *Light* reads the access rights from the Electronic-Key and sets the corresponding output A to D or STR accordingly (only one output is ever set). Switching outputs B to D, as well as STR, of the EKS *Light* are connected to inputs on the PLC. Output A is not connected, because operating mode MSO_0, "Manual operation," is not available on automatic machines. To prevent the PLC inputs from being bypassed by simply short circuiting them to gain access to a higher operating mode, the EKS *Light* first sends a 200 ms pulse on all five outputs when an Electronic-Key is inserted. This pulse is checked in the PLC. The PLC then checks whether all EKS *Light* inputs are at 0 again. Only one output may be set afterward. This procedure can detect any faulty output or a short circuit on the cable, but also tampering.

The PLC now releases the access rights by enabling all permissible pushbuttons. The PLC then uses signal lamps in the pushbuttons to indicate which operating mode may be selected. In the event of an error, the pushbuttons for selection of operating mode will not be enabled.

The F-PLC reads the selected operating mode when a pushbutton is pressed. Here too, only one pushbutton may be pressed at a time (1-of-N selection). Pressing more than one pushbutton must cause the system to branch to an error mode that is left only when only one or no pushbutton is still pressed. Defective pushbuttons can be detected this way. Furthermore, the operating mode is switched only when the pushbutton is released (falling edge). This ensures that there is no short circuit in the cable and that no pushbutton is defective.

The F-PLC will activate the new operating mode when the machine is in a suitable state. A message is simultaneously sent to the PLC to indicate the selected operating mode. With the safety control system used, this feedback is provided via a serial channel. Parallel feedback via inputs and outputs is also possible as an alternative. The PLC indicates the selected operating mode.

No other operating mode can be selected after the EKS Electronic-Key is removed.

Programming in the safe control system

The inputs are connected to a single-channel SWITCH input in the F-PLC. A logic function comprising an AND gate and an OR NOT is used to check whether exactly one input is set in each case. The output of the AND gate is connected to an edge-triggered USER RESTART MONITORED memory module that assumes the logical 1 state (LL1) in its output with the falling edge (release of the pushbutton for selection of operating mode). This operating mode remains selected until another operating mode is selected or an error is detected. The USER RESTART MONITORED memory module is cleared by selecting a different operating mode OR by an error.
An error output is set if several pushbuttons are pressed simultaneously. This error output resets all memory outputs.
Synchronous serial data transmission is used for messages to the PLC. The four operating modes and the fault display are sent. With serial data transmission from the MSC, a pause is observed between the characters. The output is set to 1 during this time. The time is adjustable. The PLC synchronizes itself with this pause. A valid bit is then transmitted with every falling edge on the CLK output. The part of programming that involves sending a message to the PLC is not relevant to safety.

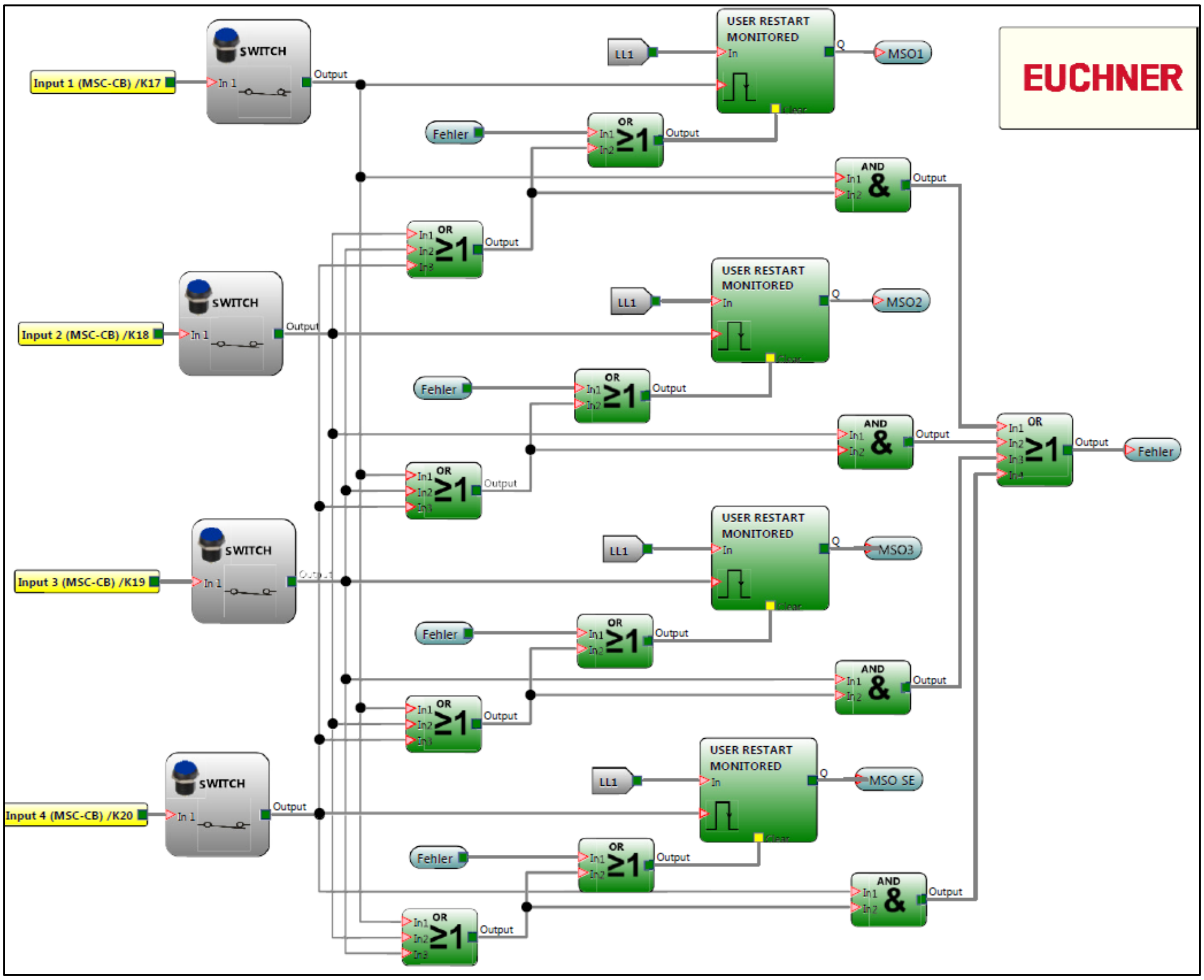

Figure 2

The data can be messaged to the PLC either via five monitoring outputs in parallel or, with the MSC, also via serial data transmission. The message includes both the currently selected operating mode and any pending error message.

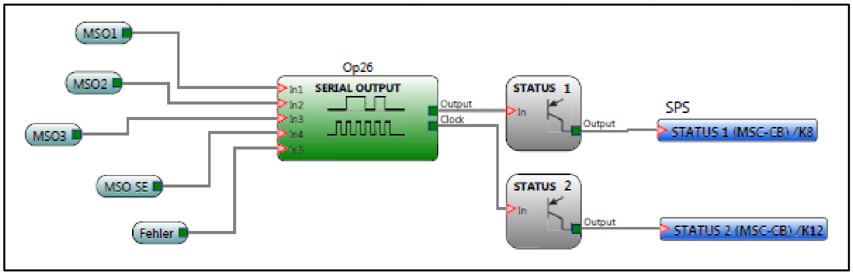

Figure 3

A bit duration of 40 ms and an inter-character time of 100 ms are set as values for serial transmission.

Programming in the PLC – evaluation of the EKS Electronic-Key

The PLC evaluates the access rights assigned to the Electronic-Key of the EKS *Light* connected to the PLC inputs (designated as inputs in Figure 4). In EKS operating state 6 or 7, the EKS outputs can be protected against tampering and short circuits to 24 V. When an EKS Electronic-Key is inserted, all EKS outputs are always connected to 1 for approx. 200 ms first and then to 0 for approx. 200 ms. Only then are the access rights available at a single EKS output. The EKS output indicates the highest permissible operating mode. This procedure can be checked using a simple status machine as shown in Figure 4. The PLC releases the outputs that are connected to the pushbuttons (= outputs in Figure 4). A timeout of 500 ms can be assumed for the entire procedure.

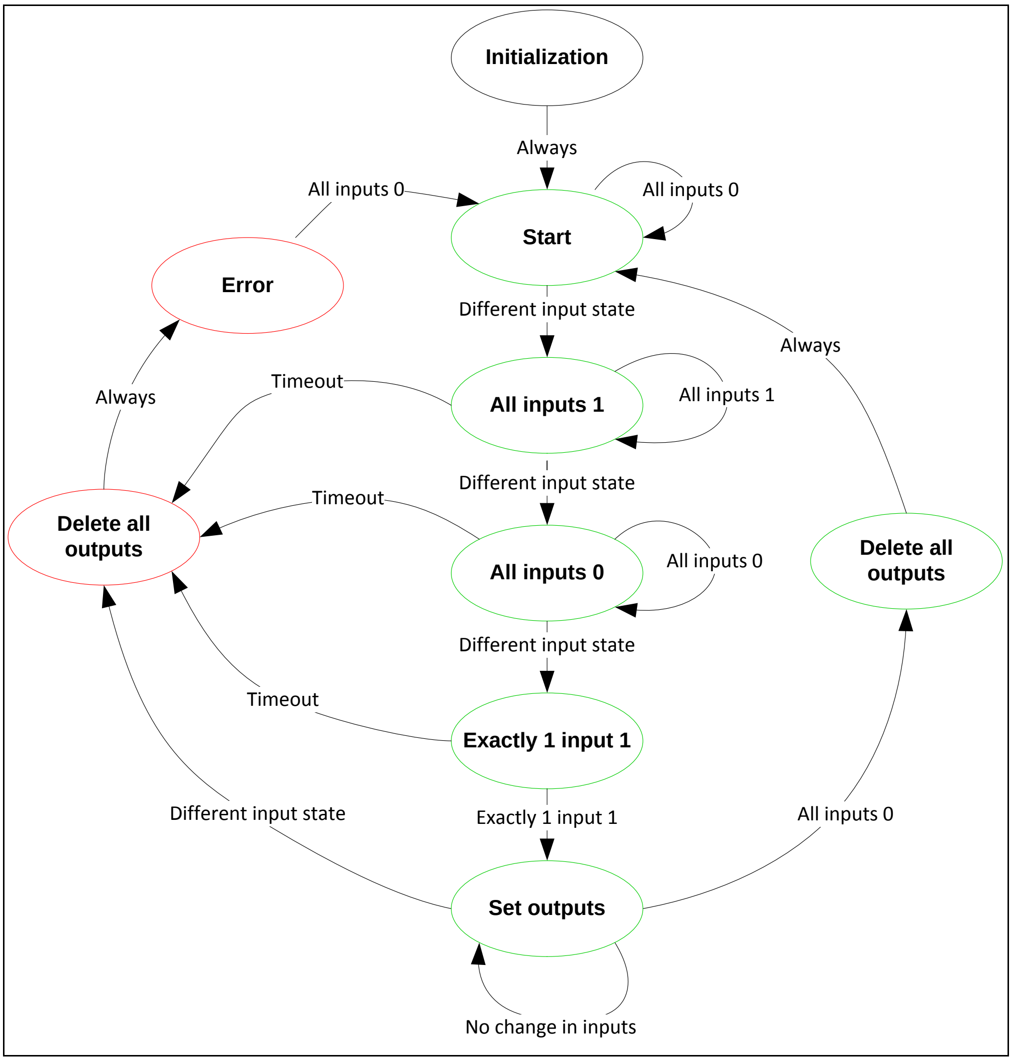

Figure 4

Programming in the PLC – evaluation of the serial feedback from the F-PLC

Data are read from the safe PLC via synchronous serial data transmission. Data are sent on one input, and a CLK signal is sent for synchronization on the second one. The respective bit is always read on the falling edge of the CLK signal. Figure 5 shows the procedure in principle. Whenever an error occurs, it is attempted to perform synchronization again. The five bits sent in the safe control system must be assigned to the respective state.
The timer must be adapted to the inter-character time in the MSC. A timeout must always be reached before the first bit arrives. With an 80 ms timer, the cycle time in the PLC must be less than 20 ms for this purpose.

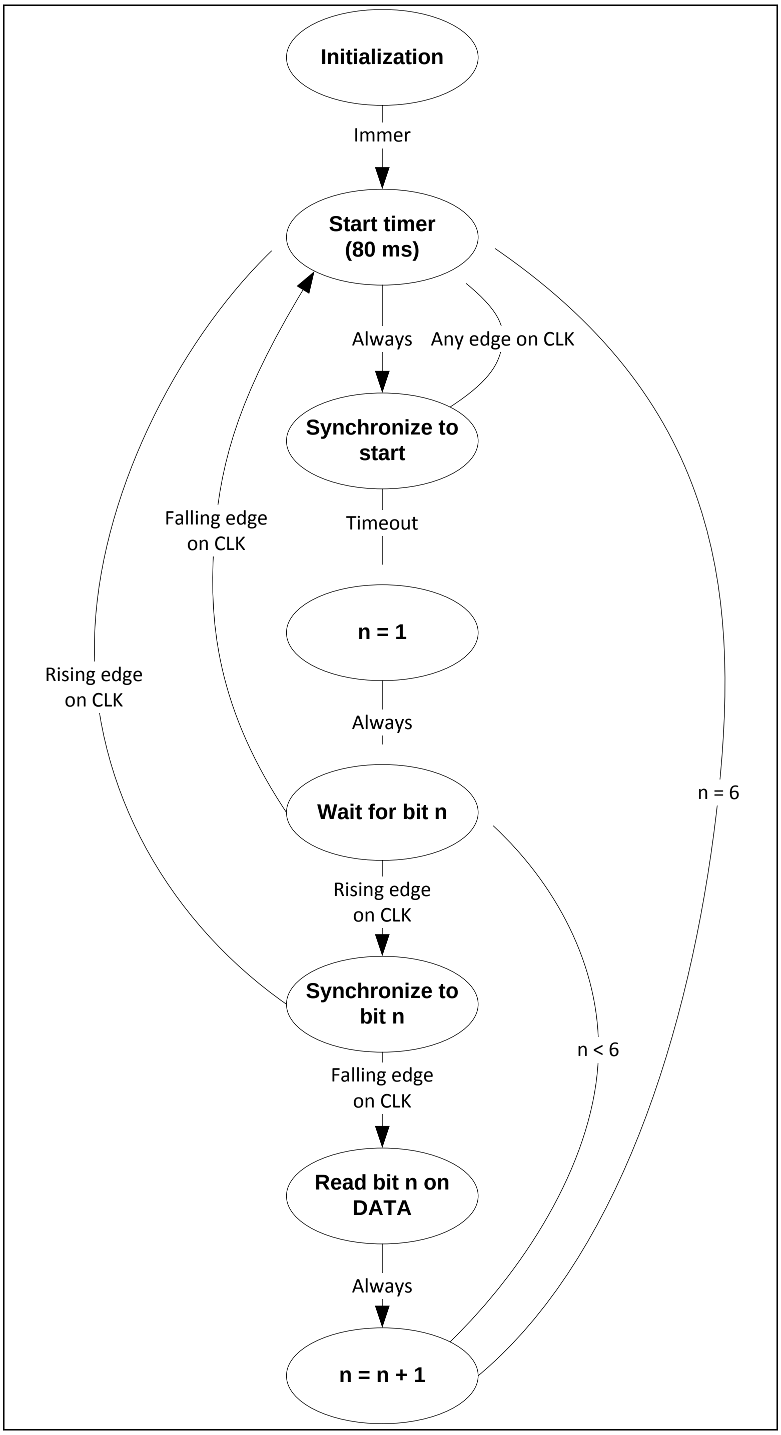

Figure 5

Programming in the PLC – lamp control

Lamps are included in the pushbuttons for selecting the operating mode. These lamps flash to indicate the selectable operating mode, and they illuminate continuously to indicate the currently selected operating mode. The currently selected operating mode is indicated by continuous illumination in the "Flash H..." states. Flashing of all selectable operating modes is achieved by repeatedly cycling through all states for indication during flashing.

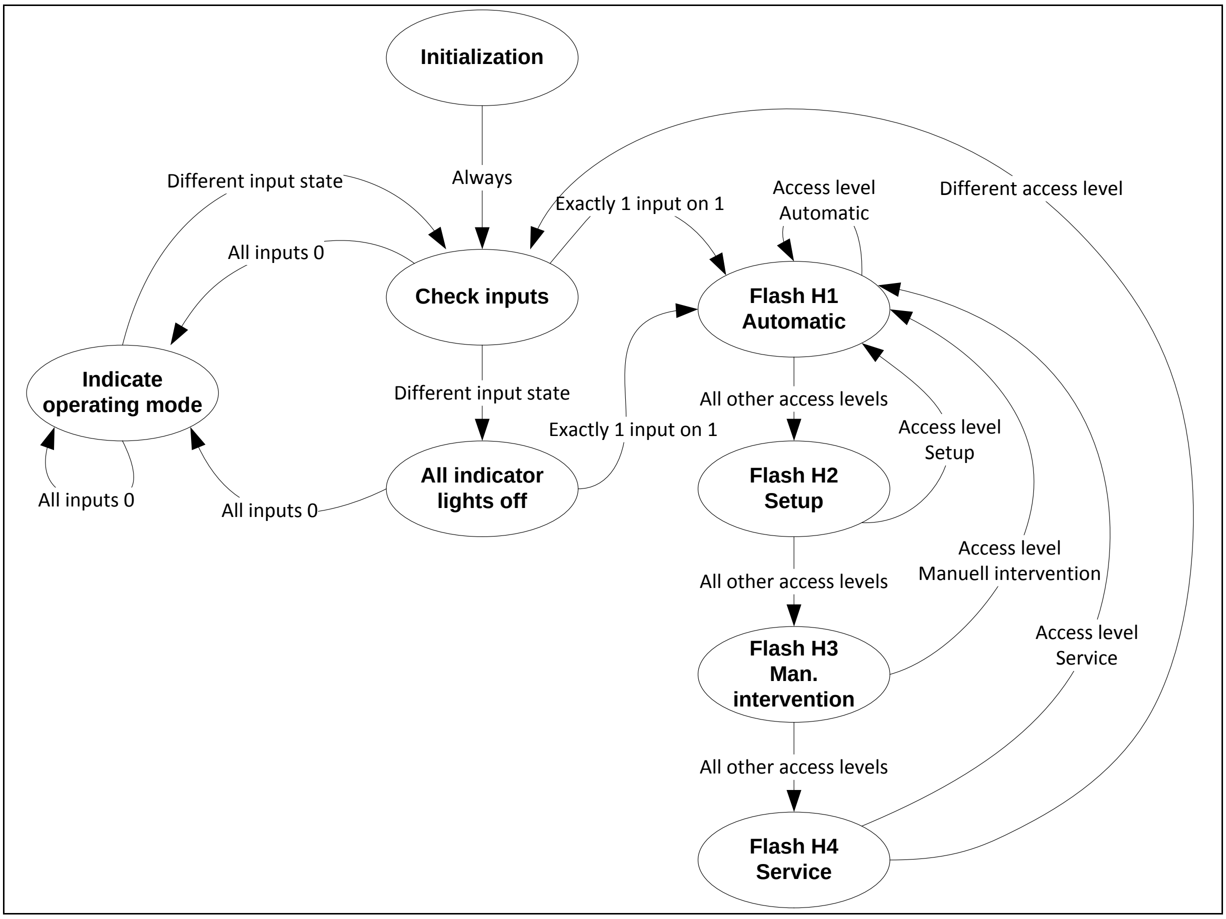

Figure 6

Principle circuit diagram

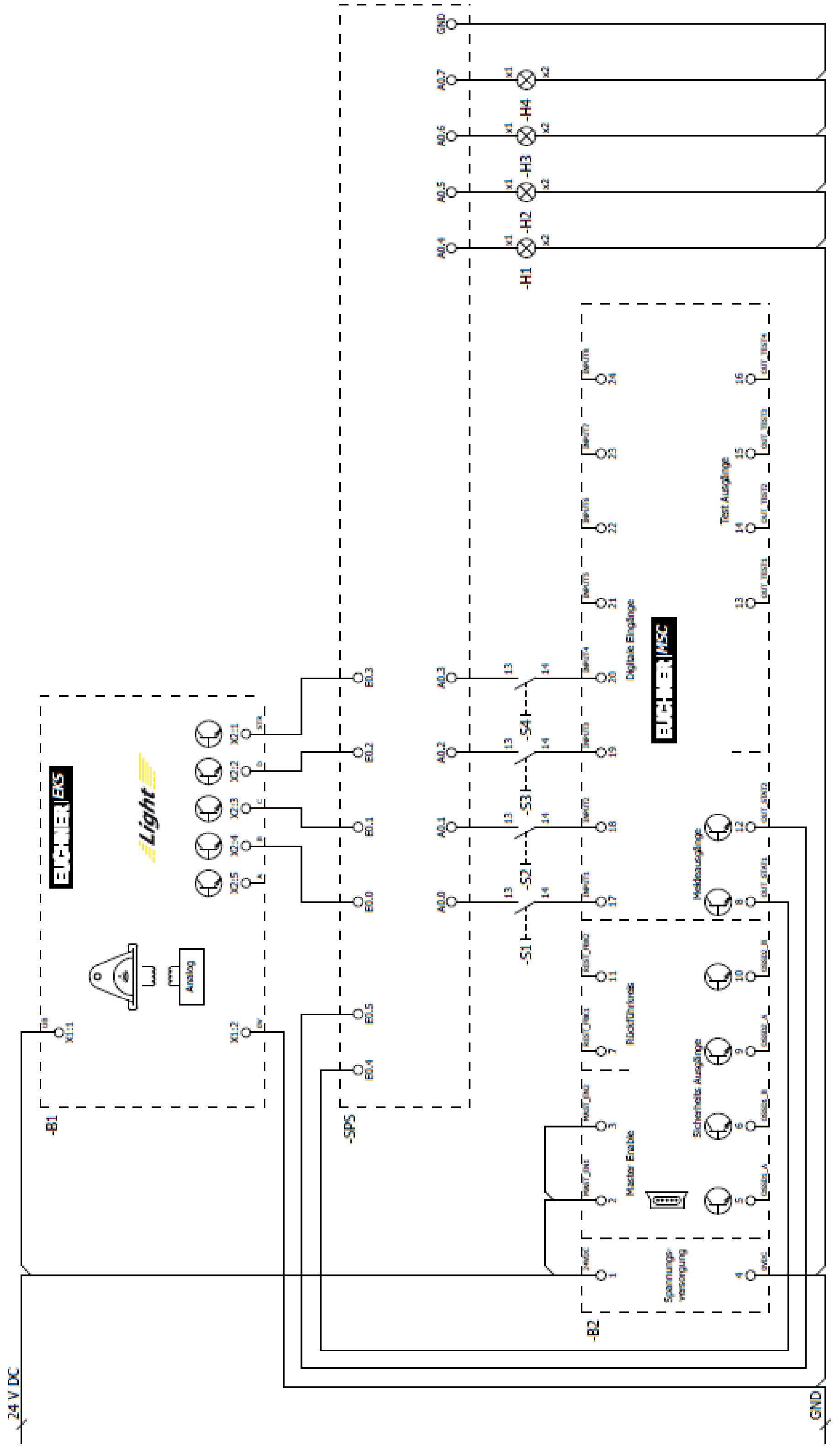

Figure 7

Safety assessment

Selection of operating mode is subdivided into three blocks – access system, selection system and activation system. DGUV Information “Sicherheitsbezogene Betriebsarten” (“safety-related operating modes”) from the German Social Accident Insurance (DGUV) (Fachbereich Holz und Metall/wood and metal department) contains further details about this subdivision.

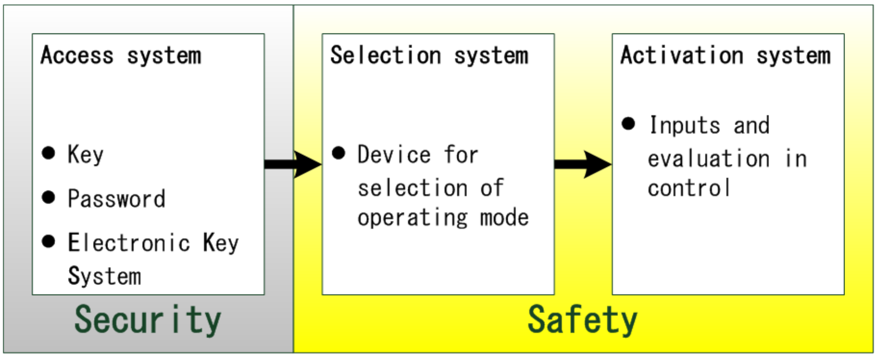

Figure 8

General notes about programming

Programming in the safe PLC is relevant for safety and must be performed in accordance with section 4.6 of EN ISO 13849-1. The software must be validated according to EN ISO 13849-2.

Access system

The access system consists of the EKS and the PLC. The access system does not have to fulfill any safety functions with regard to the safety of machinery. It does not require a PL. This part of selection of operating mode serves to restrict access. The EKS *Light*, in combination with evaluation by the PLC, is well protected against tampering and misuse. The copying of Electronic-Keys and tampering at the PLC inputs are effectively prevented.
When a valid Electronic-Key is read, the PLC outputs to which pushbuttons S1 to S4 are connected are set. Only the outputs enabled by the Electronic-Key content are released.

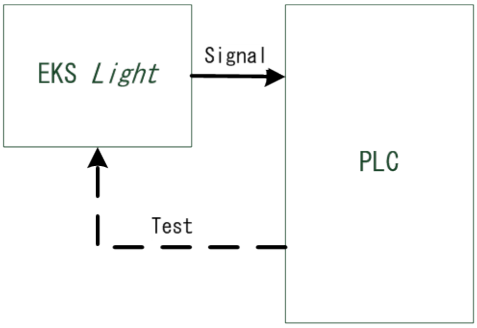

Figure 9

Selection system

Safety classification is required for the selection system and activation system. These two system parts must fulfill the PL_r resulting from the risk assessment for the respective machine.

The selection system consists of the selection pushbuttons and the safe PLC. The safe PLC in this example is the MSC from EUCHNER. Its hardware fulfills PL e. The category and the MTTFd for the pushbuttons must be determined.

The activation system is not considered in the application; it must be calculated separately. It will typically consist of contactors and/or valves.

The safety engineering structure corresponds to Figure 10 or Figure 11. The input side (pushbuttons) corresponds to category 2 and the output side to category 4.

The safe PLC monitors the single-channel pushbuttons' functions. The safe PLC fulfills PL e. The activation system consists of contactors or valves. They must also be designed to be monitored.

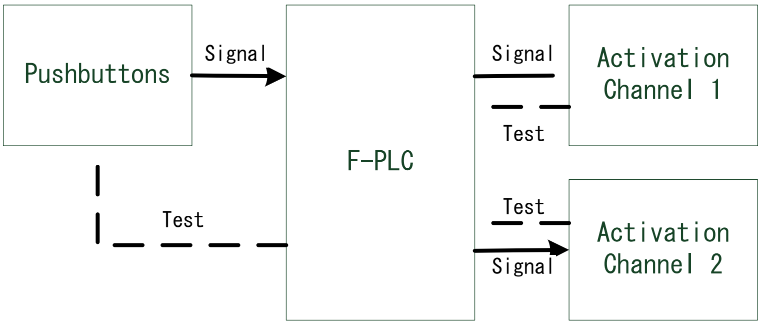

Figure 10

The overall circuit is subdivided into subsystems to calculate the safety values using the SISTEMA software.

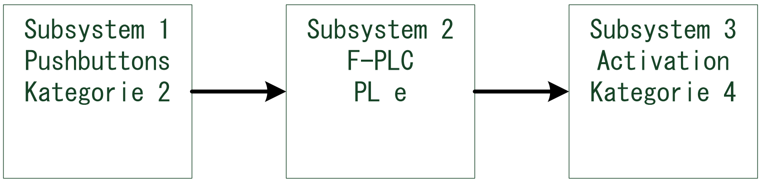

Figure 11

Each subsystem is calculated separately.

Selection system: subsystem 1 – pushbuttons

The subsystem fulfills the requirements for category 2.

Basic safety principles according to EN ISO 13849-2 are observed:

- Application of the energy separation principle – the operating mode can be changed only when voltage is applied.
- Suitable protection against ingress of fluids and dust – the required IP rating must be met.

Proven safety principles according to EN ISO 13849-2 are observed:

- Overdimensioning – the pushbuttons must be able to switch ten times the current required by the safe PLC at the inputs.
- Reducing the failure modes – the safety-related function is separated from the other functions.

The pushbuttons' B_{10d} values are required for calculation. If the values are not available from the pushbuttons' manufacturer, the value 1,000,000 can be used instead (source: BGIA Report 2/2008, Table D.2). In this case, pushbuttons must be used that are capable of switching at least ten times the current required by the safe PLC at the inputs.

Position switches and pushbuttons[b)] under resistive load and overdimensioned (⩽ 10% of the maximum bad) referred to the electrical contacts	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 1,000,000

b) *For normally open contacts and for normally closed contacts if fault exclusion for positive opening is not possible*

Figure 12

This value can be used to determine the pushbuttons' $MTTF_d$. Assuming that the operating mode is changed 100 times a day, the resulting $MTTF_d$ is 273 years.

Fault detection in the safe PLC is performed according to two principles. Switchover to another operating mode takes place only with a falling edge at an input of the safe PLC. Additionally, only one input may be set.

Part	Possible failure	Fault detection	Effect / reaction
Pushbutton	Does not open	The operating mode is accepted only with a falling edge.	Failure in the safe direction
		Pressing another pushbutton deactivates the previously selected operating mode. This completely switches off the machine.	Leads to complete shutdown of the machine
	Does not close	The fault cannot be detected, but it does not represent a dangerous failure. This operating mode can no longer be selected in this case.	Failure in the safe direction
	Short circuit to 0 V on pin 13 of a pushbutton	The fault cannot be detected, but it does not represent a dangerous failure. This operating mode can no longer be selected in this case.	Failure in the safe direction
	Short circuit to 24 V on pin 13 of the pushbutton	The fault cannot be detected. The associated operating mode can always be selected. The fault can be assigned to the access system and does not have to be considered from a safety engineering perspective.	Fault is not detected
	Short circuit to 0 V on pin 14 of a pushbutton	The fault cannot be detected, but it does not represent a dangerous failure. This operating mode can no longer be selected in this case.	Failure in the safe direction
	Short circuit to 24 V on pin 14 of a pushbutton	This fault produces a rising edge. A falling edge can no longer be produced.	Failure in the safe direction
		Pressing another pushbutton deactivates the previously selected operating mode. This completely switches off the machine.	Leads to complete shutdown of the machine

Table 2

Of the six different, mutually independent faults in Table 2, 4.5 (only partial detection is assumed for one of the faults) are detected. The diagnostic coverage for the pushbuttons is therefore 83%.

The structure for subsystem 1 is mapped in SISTEMA.

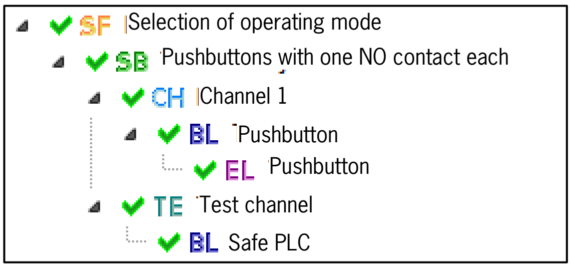
SF Selection of operating mode
SB Pushbuttons with one NO contact each
CH Channel 1
BL Pushbutton
EL Pushbutton
TE Test channel
BL Safe PLC

Figure 13

A value of 100 years can be entered directly as the MTTFd for the safe PLC in the test channel.

With the stated values, the following values result for subsystem 1.
Category: 2
$MTTF_d$: 100 years (high)
DC_{avg}: 83% (low)
CCF: this must be verified by the application’s creator and must produce a result of a least 65 points.
PL: d
PFH_d: 2.99E-07
Important: The specified PFH_d must be calculated for the number of changes in the selection of operating mode for each application. The specified PFH_d is calculated for 36,500 actuations per year.

Selection system: subsystem 2 – safe PLC

The MSC-CB from EUCHNER is subsystem 2. EUCHNER confirms category 4, PL e and a PFH_d value of 6.1 E-09 for this system.
Important: The software in the safe PLC must be created as per PL d according to EN ISO 13849-1 and must be validated correspondingly.

Selection system: result for subsystems 1 and 2

With the values assumed above, the resulting PFH_d for both subsystems together is 3.85 E-07, which corresponds to PL d.

Activation system

Activation system: subsystem 3

The activation system is not considered here. It can be calculated as a separate subsystem and added to the PFH_d of subsystems 1 and 2.

Important note – please observe carefully!

This document is intended for a design engineer who possesses the requisite knowledge in safety engineering and knows the applicable standards, e.g. through training for qualification as a safety engineer. Only with the appropriate qualification is it possible to integrate the introduced example into a complete safety chain.

The example represents only part of a complete safety chain and does not fulfill any safety function on its own. In order to fulfill a safety function, the energy switch-off function for the hazard location and the software within the safety evaluation must also be considered, for example.

The introduced applications are only examples for solving certain safety tasks for protecting safety doors. The examples cannot be comprehensive due to the application-dependent and individual protection goals within a machine/installation.

If questions concerning this example remain open, please contact us directly.

In accordance with Machinery Directive 2006/42/EC, the design engineer of a machine or installation is obligated to perform a risk assessment and take measures to reduce the risk. When doing this, the engineer must comply with the applicable national and international standards. Standards generally represent the current state of the art. Therefore, the design engineer should continuously inform himself about changes in the standards and adapt his considerations to them. Relevant standards include EN ISO 13849 and EN 62061. This application must be regarded only as assistance for the considerations about safety measures.

The design engineer of a machine/installation has the obligation to assess the safety technology him/herself. The examples must not be used for assessment, because only a small excerpt of a complete safety function was considered in terms of safety engineering here.

In order to be able to use the safety switch applications correctly on safety doors, it is indispensable to observe the standards EN ISO 13849-1, EN ISO 14119 and all relevant C-standards for the respective machine type. Under no circumstances does this document replace the engineer's own risk assessment, and it cannot serve as the basis for a fault assessment.

Particularly in case of fault exclusion, it must be noted that this can be performed only by the design engineer of a machine or installation and requires a reason. General fault exclusion is not possible. More information about fault exclusion can be found in EN ISO 13849-2.

Changes to products or within assemblies from third-party suppliers used in this example can lead to the function no longer being ensured or the safety assessment having to be adapted. In any event, the information in the operating instructions on the part of EUCHNER, as well as on the part of third-party suppliers, must be used as the basis before this application is integrated into an overall safety function. If contradictions should arise between the operating instructions and this document, please contact us directly.

Use of brand names and company names

All brand names and company names stated are the property of the related manufacturer. They are used only for the clear identification of compatible peripheral devices and operating environments in relation to our products.