[IFA Logo]

Testing and certification body in
BG-PRÜFZERT

Datum/Date: 13.07.2016
SOt/Apf

UNTERSUCHUNGSBERICHT

RESEARCH REPORT

Nr./No.: 2015 24741

1, Auftraggeber/ ***Customer***	EUCHNER GmbH & Co. KG Kohlhammerstr. 16 70771 Leinfelden-Echterdingen
2. Untersuchungsobjekt/ ***Research specimen***	Selection of the operation mode using the EKS light FSA as an access system
Hersteller/ ***Manufacturer***	see above
Bezeichnung/ ***Designation***	Procedure for operation mode selection on machines using the EKS light FSA as an access system
Kennzeichnung/ ***Marking***	EKS light FSA
Weitere Angaben/ ***Further details***	—
3. Betreiber/ ***Operating Company***	-

4. Purpose

The manufacturer commissioned IFA to evaluate a procedure for realizing operation mode selection on machines using the EKS light FSA as the access system. The aim is to evaluate whether safety that is equivalent to operation mode selection via an electromechanical operation mode selector switch can be achieved with the aid of the EKS light FSA – in combination with a safety PLC (SPLC), an HMI (human-machine interface) and a PLC. During this task it is also to be evaluated whether the EKS Light FSA meets the structural requirements of category 3 according to DIN EN ISO 13849-1 in relation to its function as an access system.

5. Description

The EKS light FSA is an Electronic-Key system, which consists of a reader and an Electronic-Key. The reader has integrated evaluation electronics and interfaces only for data output. An operating state, an access level, an access code, a serial number and a checksum covering the data on the Electronic-Key are saved on the Electronic-Key.

The access level is saved in a data word. To protect against corruption, valid data words possess a Hamming distance of h= 8. The access level corresponds to one of five possible operation modes and the hierarchically highest operation mode that the Electronic-Key holder is authorized to select.

The Electronic-Key data are evaluated (including calculation and comparison of the checksums) redundantly via two processors. The result of the evaluation is checked between the processors via cross-wise data comparison.

Along with a 4-bit parallel interface (outputs A, B, C and D) and a strobe output (STR), the reader for the EKS light FSA has a semiconductor relay output LA. The first processor provides, via the outputs A-D and STR, information on whether a valid Electronic-Key is inserted and which access level is assigned to the Electronic-Key. Here, depending on the access level, one of the five outputs is set to high and the other outputs shut down. Via the second processor the output LA provides information on whether an Electronic-Key is inserted – independent of the authorization level. All outputs and the switching contact are shut down on the removal of the Electronic-Key.

The outputs A to D, STR and LA are connected to safe inputs on the SPLC. The SPLC checks the plausibility of the data received. Plausibility is present if – with an Electronic-Key inserted – one of the five outputs A to D and STR as well as LA or – with Electronic-Key removed – none of the outputs on the EKS light FSA is set to high. If a valid Electronic-Key is indicated plausibly – both in relation to the timing and the outputs set – by the input signals, the access level transferred in the coding as data word (Hamming distance h = 8) is sent via the PLC to the HMI. The operator can select an operation mode on the HMI based on the access level received.

The operation mode is sent to the SPLC, checked there for plausibility with the access level received by the reader, and returned to the HMI for further confirmation by the operator. Via the read-back and confirmation procedure using changing coding and continuous plausibility checks by the SPLC, the selected operation mode is verified and any errors on selection or data transmission detected. The procedure corresponds to safe parameter entry according to DIN EN ISO 13849-1. To cover stuck-at faults in all components involved, the same procedure is also applied with the Electronic-Key removed. Here the acknowledgment is provided automatically by the HMI. Any faults in the HMI are detected due to the difference in the acknowledgment signals with the Electronic-Key inserted and removed. The operation mode is switched safely and the safety functions required for the operation mode are activated via the SPLC.

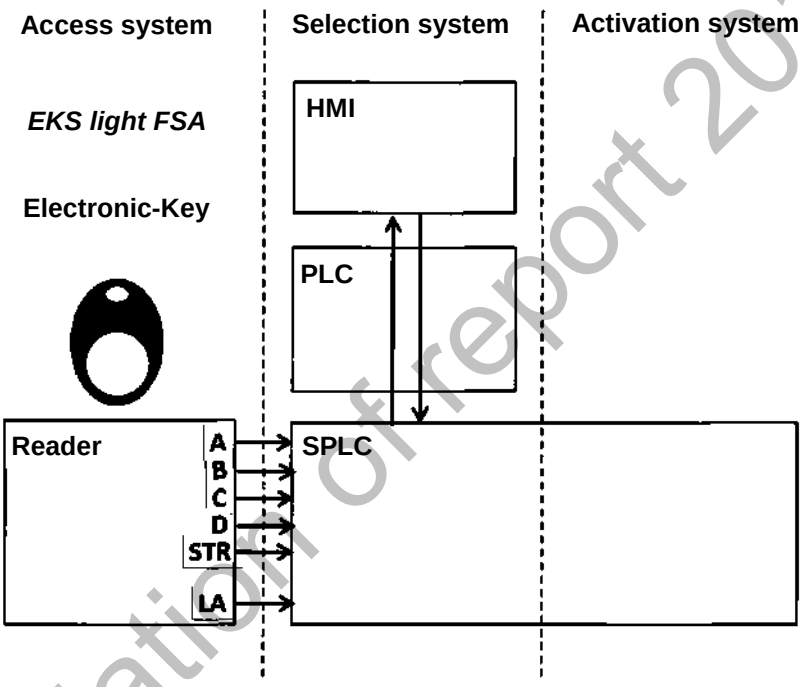

Figure 1: Schematic diagram of operation mode selection

6. Safety assessment

For the purpose of a safety assessment, the component structure for the procedure described is divided into three functional components (see Figure 1).

6.1. Access system

Requirements

The access system is the part of the selection device that restricts operation mode selection to specific groups of persons and prevents unintentional or improper actuation of the selection system. As the selection of each operation mode is associated with the activation of other safety functions, the access system is considered to be relevant for safety.

On electromechanical selection devices, the access is realized by the Electronic-Key. Here the selection of only specific operation modes can be enabled by mechanical coding on the Electronic-Key. In addition, there are organizational measures that are intended to restrict the access to the Electronic-Key or the Electronic-Keys to a specific group of persons.

The EKS light FSA must provide safety that is at least equivalent to that of an electromechanical operation mode selector switch access system. This requirement arises from Machinery Directive 2006/42/EC, section 1.2.5., which leaves it up to the user's discretion whether to replace the operation mode selector switch with a different selection device that "restricts the use of certain functions of the machinery to certain categories of operator."

Assessment

The access system for operation mode selection is formed by the EKS light FSA. During the study, the switching principle and the software for the reader were subjected to an assessment. The agreement of the access level transferred via the interfaces to the SPLC with the access level actually saved in the Electronic-Key was not assessed. Instead, the switching principle and the software were assessed for the following function: only if a valid Electronic-Key is inserted in the reader is the insertion of a valid Electronic-Key signaled on the outputs of the first and the second channel.

The assessment produced the following result: the EKS light FSA meets, as an access system for the safety function operation mode selection, the structural requirements of category 3 according to DIN EN ISO 13849-1 in relation to the function defined in the last section.

The following characteristics contribute to this assessment:

- The Electronic-Key data are evaluated in the EKS light FSA in two different processors with different software
- Both processors have dedicated overvoltage monitoring

- One of the processors also has low voltage monitoring

In relation to the software the following points are to be noted:

- The software in the processors has been implemented in different programming languages
- The data are read from the Electronic-Key by the first processor using a single channel. The reading process is monitored by the second processor. During the read process all Electronic-Key data are transferred to the second processor.
- The Electronic-Key data are evaluated redundantly on both processors.
- The first processor sets the outputs A-D, STR independent of the second processor. Before the second processor activates the output LA1/LA2, the results of the evaluation are cross-compared. If the results of the evaluation do not match, the outputs A-D, STR are reset by the first processor.

Due to the characteristics described, the EKS light FSA can be assessed in relation to the function described above as single-fault tolerant.

Safety at least equivalent to the access system for operation mode selection via a conventional key is hereby confirmed for the EKS light FSA.

6.2. Selection system

Requirements

The selection system defines the operation mode which the activation system is to activate in the control system.

In electromechanical selection devices the selection system corresponds to the manually actuated switch knob; the position of this knob is transmitted mechanically, e.g., via a shaft and cams to the electrical contact elements.

In electronic selection devices the selection system is generally realized via a user interface. The operation mode to be activated in the machine control is defined by the operator via the user interface and possibly further electronic components. As here in general standard components are used, categorization of a selection system realized in this manner as PL c or higher is only possible with additional measures. One possibility is offered by section 4.6.4 of the standard in which the requirements for software-based parameterization are defined. As the operation mode selection via an electronic selection system is equivalent to software-based parameterization, the stated section of the standard can be used for the safety-related assessment of this selection system. The procedure described there covers the selection of the operation mode by the operator, the check in the safe control system on the operation mode selected and the confirmation of the operation mode selected by the operator. In this way it is ensured that the integrity of the data used for the parameterization is retained along the communication channel and corruption detected.

In particular, an incorrect operation mode due to a fault in one of the components of the selection device for selection or confirmation is prevented.

The selected operation mode must be displayed to the user. This requirement arises from Machinery Directive 2006/42/EC, section 1.2.5, and from the requirement that each position of the operation mode selector switch must be clearly identifiable.

Assessment

The operation mode selection system is formed by PLC, HMI and safety PLC.

The procedure used for the selection of the operation mode involving the return transmission of the selected operation mode and its subsequent confirmation by the operator and check by the SPLC satisfies the procedure required for parameterization in DIN EN ISO 13849-1, section 4.6.4.

The monitoring over the range of valid entries is performed in the SPLC by the comparison of the selected operation mode with the authorization level transferred to the SPLC. Corrupt or incomplete data are detected via the selected Hamming distance of the valid data words and via continuous monitoring of the parameters selected on the user interface in the SPLC using failsafe technology.

Reliable error detection in the HMI and PLC is achieved above all by means of the fact that the coding of the transmitted parameters changes with every step of the procedure. In this way, repeated transmission of a data word due to an error is detected as error. With correct application of the procedure and with the coding introduced by Euchner in the document AP000200-01.4, the requirement for component diversity contained in DIN EN ISO 13849-1 is also considered as having been met in an equivalent manner. Systematic failures are controlled.

The parameterization software must be created by the user. Euchner merely describes the procedure to be used for this purpose. Accordingly, the user is also responsible for verifying the software according to DIN EN ISO 13849-1, section 4.6.4. For machines according to Appendix IV of Machinery Directive 2006/42/EC, the software may have to be verified by a notified body.

If the operation mode cannot be displayed to the operator on the HMI after selection, the user must ensure that the operation mode is indicated to the operator by other, clearly visible means.

6.3. Activation system

Requirements

The actual safety function, specifically the “activation of the safety functions required for the selected operation mode,” is performed on the activation system.

A PL is assigned for this purpose, depending on the executing components. The required PL of the safety function results from the risk assessment or from the requirements of the applied product standard.

Additionally, when the safety-related application software (SRASW) for the SPLC is written, measures must be taken to suit the PL_r to avoid systematic errors according to DIN EN ISO 13849-1, section 4.6.3. The software must be validated according to section 9.5 of DIN EN ISO 13849-2.

Assessment

The SPLC forms the activation system for operation mode selection.

The user must create the safety-related software. Euchner merely describes the procedure to be used for this purpose. Accordingly, it is the user's responsibility to take the measures stated in DIN EN ISO 13849-1, section 4.6.3. In addition, the software must be validated according to section 9.5 of DIN EN ISO 13849-2.

The average probability of a dangerous failure of the operation mode selection safety function is formed from the PFH_D of the SPLC used as the activation system. It is a prerequisite that the aforementioned measures are taken to suit the PL of the SPLC and are successfully validated when the SRASW is written.

7. Conclusion

The EKS light FSA meets, as an access system, the structural requirements of category 3 according to DIN EN ISO 13849-1. It is therefore single-fault tolerant. The agreement of the access level transferred with the access level saved in the Electronic-Key was not assessed.

Given correct implementation and the selection of suitable components, the procedure presented by Euchner is suitable for performing the operation mode selection safety function with a level of safety at least equivalent to that of operation mode selection via an electromechanical operation mode selector switch.

Actual execution of the operation mode selection safety function is performed by the activation system, with the selection system defining the operation mode as a parameter of the safety function. The safety function is defined as follows here: activation of the safety functions required for the respective operation mode.

With application of the procedure described and under the conditions stated in chapter 6, the Performance Level of the activation system can be assumed as the Performance Level of the operation mode selection safety function.

8. Documents

- AP000200-01.4 EKS Light FSA on Siemens S7-300 – operation mode selection with touchscreen, V2, 31.03.2016
- LP-KPL AUSWERTUNG FSA (Schaltplan) [LP-KPL EVALUATION (circuit diagram)], V1, 23.06.2015
- Software EKS Light FSA, V15

IFA – Institut für Arbeitsschutz der Deutschen
Gesetzlichen Unfallversicherung

By order
Technical auditor:

[Signature]
Dipl.-Ing. Ralf Apfeld

Reviewed by:

[Signature]
B.Sc. Stefan Otto