Prüf- und Zertifizierungsstelle
im BG-PRÜFZERT

Datum/Date: 17.09.2015
SOt/Apf

UNTERSUCHUNGSBERICHT

RESEARCH REPORT

Nr./No.: 2015 21227

1.	**Auftraggeber/** ***Customer***	EUCHNER GmbH & Co. KG Kohlhammerstr. 16 70771 Leinfelden-Echterdingen
2.	**Untersuchungsobjekt/** ***Research specimen***	Betriebsartenwahl unter Nutzung des EKS FSA als Zugangssystem
	Hersteller/ ***Manufacturer***	s.o.
	Bezeichnung/ ***Designation***	Untersuchungsbericht zur Bewertung eines Verfahrens zur Realisierung der Betriebsartenwahl an Maschinen unter Nutzung des EKS FSA als Zugangssystem
	Kennzeichnung/ ***Marking***	EKS FSA
	Weitere Angaben/ ***Further details***	
3.	**Betreiber/** ***Operating company***	

4. Purpose

The manufacturer commissioned IFA to evaluate a procedure for realizing operating mode selection on machines using the EKS FSA (Electronic Key System For Safety Applications) as the access system. The aim is to evaluate whether safety equivalent to operating mode selection via an electromechanical operating mode selector switch can be achieved with the aid of the EKS FSA – in combination with a PLC, an HMI (human-machine interface) and an F-PLC – while observing the specifications for safe software-based parameter assignment described in DIN EN ISO 13849-1 :2008, section 4.6.4.

5. Description

A procedure for operating mode selection on machines using the EKS FSA as the access system is to be realized.

The EKS FSA is an Electronic-Key system, which consists of an Electronic-Key adapter and an Electronic-Key. The Electronic-Key adapter is a read/write system with integrated interface electronics. The Electronic-Key has a read/write and fixed-code memory area in which the serial number of the Electronic-Key is stored. When the Electronic-Key is configured, data relevant for access to operating mode selection can be stored in addition to other data in the programmable memory area.

The authorization level for operating mode selection is stored in a data word in the Electronic-Key's programmable memory area. To protect against falsification, the valid data words possess a Hamming distance of h= 8. The authorization level stored on the Electronic-Key corresponds to the hierarchically highest operating mode that the Electronic-Key holder is authorized to select.

If the machine has only three or fewer operating modes, the authorization level can be alternatively stored in a data byte. In this case, the Hamming distance h = 5

In addition to a data interface, the EKS FSA features an additional semiconductor relay output that is switched off as long as there is no Electronic-Key in the Electronic-Key adapter or if the Electronic-Key cannot be read.

The EKS FSA is connected to the PLC via the data interface for transmission of the data relevant for operating mode selection. The semiconductor relay output is linked with a safe input of the F-PLC. The PLC forwards the data of the EKS FSA to the HMI and, via changing marker words, to the F-PLC. The data received are checked for validity here. Based on the authorization level, the user can select an operating mode on the HMI and forward it to the F-PLC. Via a read-back and confirmation procedure, the selected operating mode is verified and any errors are detected on selection of data transmission.

The operating mode is switched safely and the safety functions required for the operating mode are activated via the F-PLC.

Access system Selection system Activation system Touchscreen for operating mode selection Bus activation in safety PLC Machine Signal Control system

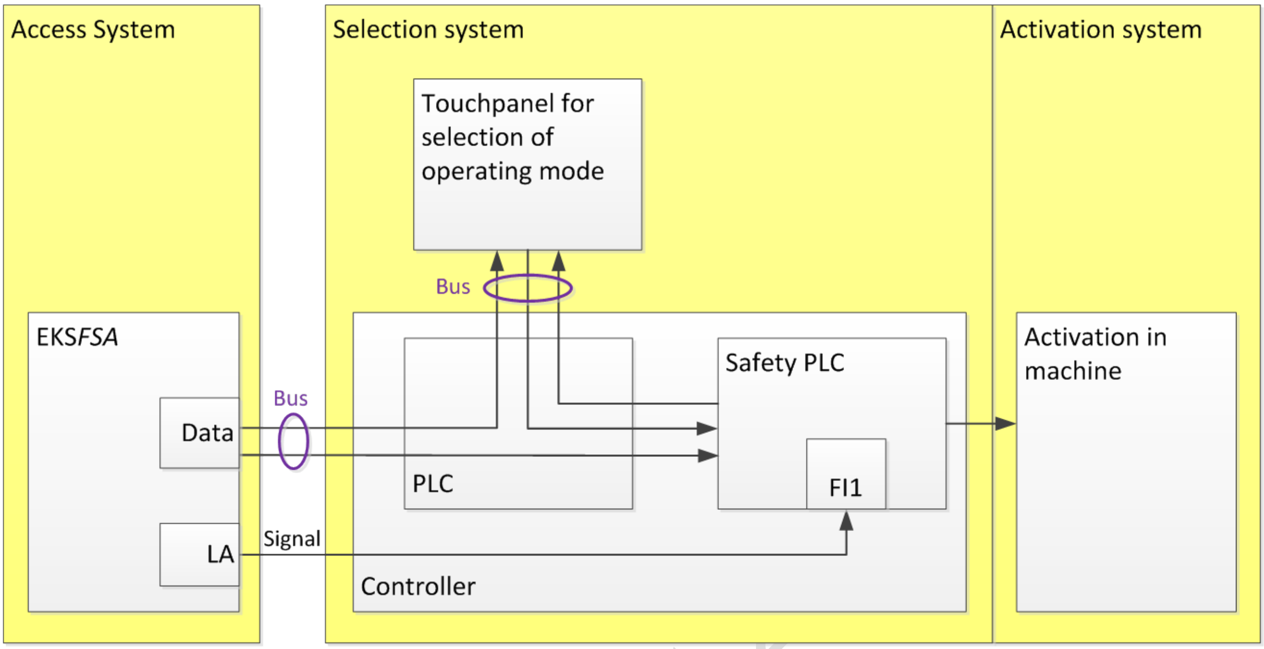

Figure 1: Schematic diagram of operating mode selection

6. Procedure description

EKS FSA / PLC

When an Electronic-Key is inserted into the reader, the Electronic-Key data are forwarded to the PLC via the data interface. The semiconductor relay output is set to High. After evaluation of the checksums has been completed with a positive result in the PLC, the authorization level of the Electronic-Key is forwarded to the HMI and to the F-PLC.

The data interface is set to zero and the semiconductor relay output is switched off when the Electronic-Key is removed. The PLC performs a checksum calculation based on the data received. Zero is expected as the result of this calculation. If the checksum result is correct, the zero is forwarded to the HMI and to the F-PLC.

HMI

Depending on the authorization level read in, the HMI displays the operating modes that the operator is authorized to select. After selection of the operating mode, the selected operating mode is sent to the F-PLC. The F-PLC sends feedback about the stored operating mode to the HMI, where the operator must acknowledge it. The acknowledged operating mode is sent to the F-PLC. The procedure corresponds to safe parameter input according to DIN EN ISO 13849-1:2008 (see section 7.2).

When the Electronic-Key is removed, the screen for operating mode selection is blocked on the HMI. An empty data word is returned as feedback of the HMI and is forwarded to the F-PLC. The F-PLC returns feedback to the HMI, which in turn acknowledges the received zero by returning an empty data word.

F-PLC

As soon as the signal changes from zero to one at the safe input, a time expectation until receipt of the authorization level from the PLC is started in the F-PLC. When the authorization level is received, it is checked whether the data authorize selection of an operating mode, i.e. whether the authorization level is greater than zero.

As soon as the F-PLC has received the operating mode selected on the HMI, it is checked whether the selected operating mode is a valid operating mode and whether the operator is authorized to select it based on the authorization level. If the check produces a positive result, the operating mode is returned to the HMI for acknowledgment. After acknowledgment of the operating mode, it is checked whether the acknowledged operating mode matches the previously selected operating mode. If the check produces a positive result, the operating mode is activated in the machine control system by the F-PLC. If an error is detected, the F-PLC enters an error mode that – unless a permanent error exists – can be exited only by removing the Electronic-Key.

When the Electronic-Key is removed, a time expectation until the data are received from the PLC is started after a corresponding signal change at the safe input. Both the EKS FSA data and the data sent by the HMI are checked to determine whether they correspond to the expected value of zero. Only then is an empty data word returned to the HMI, which acknowledges blocking of the operating mode selection window by returning a zero. If an error is detected, the F-PLC enters an error mode that – unless a permanent error exists – can be exited only by inserting an Electronic-Key again.

The selected operating mode remains active when the Electronic-Key is removed.

7. Safety evaluation

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

7.1. Access system

Requirements

The access system assists in restricting access to operating mode selection to certain groups of people and in preventing unintentional or improper selection of an operating mode. At the same time, the assigned authorization level allows each Electronic-Key holder to access only certain operating modes, thereby restricting the group of people authorized to select these operating modes to specially trained personnel.

As the selection of each operating mode is associated with the activation of other safety functions, the access system is considered to be relevant for safety.

In case of operating mode selection with an electromechanical selector switch, the access system corresponds to the key. Owing to the mechanical key coding, each key can access the selection of only certain operating modes. As a rule, the electrical part of the access system in electromechanical operating mode selector switches is designed with single-fault tolerance, so that a single fault cannot lead to a loss of safety – in this case to unintentional activation of an operating mode.

Organizational measures intended to prevent access to operating mode selection by unauthorized persons must also be regarded as being relevant for safety. These measures are to be given a low evaluation in case of operating mode selection by electromechanical switch, because access is not logged and practical experience has shown that keys to operating mode selector switches are frequently left inserted.

The EKS FSA must provide safety that is at least equivalent to that ofan access system to the electromechanical operating mode selector switch 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 operating mode selector switch with a different selection facility that "restricts the use of certain functions of the machinery to certain categories of operator."

Evaluation

The EKS FSA comprises the access system to operating mode selection. According to an inspection report from BG ETEM (German Social Accident Insurance Institution for the energy, textile, electrical and media products sectors) (inspection certificate 12023) dated 20 February 2013, the EKS FSA meets the structural requirements of category 3 according to DIN EN ISO 13849-1:2008. The residual error probability for an undetected falsification of a data word, and for any unintentional selection of an operating mode resulting from this, can be additionally limited by the selected Hamming distance to 1.2 x 10-12 per hour (h = 8) or to 5.43 x 10-9 per hour (h = 5).

The organizational measures when the EKS FSA is used are to be given a higher evaluation, because the chip can store personal data of the operator in addition to the authorization level and thereby permits traceable logging of access to operating mode selection. Access to the configuration software for programming the Electronic-Keys is password protected. Tampering with the Electronic-Key data is additionally made more difficult by the serial number stored on the Electronic-Key during production being part of checksum formed via the Electronic-Key data. In addition, the range for checksum formation can be set as required. It can be assumed that these measures largely prevent misuse of or unintentional access to operating mode selection.

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

7.2. Selection system

Requirements

The selection system defines the operating mode activated in the control system by the F-PLC. Operating mode selection is therefore a parameter assignment process.

The specifications for software-based parameter assignment according to DIN EN ISO 13849-1:2008, section 4.6.4, are to be used for the safety evaluation of the selection system. Accordingly, it must be ensured that the integrity of all data used for parameter assignment is maintained. This must be achieved by employing the following measures:

- Check of the range of valid inputs
- Management of data falsification prior to data transmission
- Management of the effects of deviations during the parameter transmission process
- Management of the effects of transmitting incomplete parameters
- Management of the effects of errors and failures of the hardware and software of the tool used for parameter assignment

The input parameters must also be confirmed. In this case, the operating mode to be selected must be confirmed. This must be performed by return transmission of the data that were or are to be modified to the parameter assignment tool, as well as subsequent confirmation by a sufficiently trained person and an automatic check by the parameter assignment tool.

The software modules involved in coding/decoding and displaying the safety-relevant data must have a diverse design in order to avoid systematic failures.

The software for parameter assignment on the HMI and PLC must be verified according to the following specifications:

- Verification of the correct setting for every safety-related parameter
- Verification that the safety-related parameters have been checked for plausibility
- Verification that unauthorized modification of safety-related parameters
- has been prevented
- Verification that parameter assignment data are generated and processed so that errors cannot lead to a loss of the safety function

The selected operating 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 operating mode selector switch must be clearly identifiable.

Evaluation

The operating mode selection system is formed by PLC, HMI and F-PLC.

The procedure for return transmission of the selected operating mode and its subsequent confirmation by the operator and check by the F-PLC as described in chapter 6 complies with the parameter assignment procedure required in DIN EN ISO 13849-1:2008, section 4.6.4.

The check over the range of valid inputs is performed in the F-PLC by a comparison between the selected operating mode and the authorization level stored on the Electronic-Key. Falsified or incomplete data are detected via the selected Hamming distance of the valid data words and via continuous monitoring of the selected parameters in the F-PLC 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 AP000169.7, the requirement for a diversity of components contained in DIN EN ISO 13849-1:2008 is also regarded as having been met in an equivalent manner. Systematic failures are managed.

Only in the case of storage of the authorization level in a data byte and with a Hamming distance of h = 5 is it possible to select automatic mode unintentionally if there is an error in the HMI. However, since automatic mode is the mode with the highest safety requirements and does not require any special operator authorization, this is regarded as being an error in the safe direction and thus as being non-critical.

The parameter assignment 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 13849-1:2008, section 4.6.4. In case of machines according to Appendix IV of Machinery Directive 2006/42/EC, the software may have to be verified by an inspection authority.

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

7.3. Activation system

Requirements

The actual safety function, namely “activation of the safety functions required for the selected operating 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) of the F-PLC is created, measures must be taken in accordance with the PLr to avoid systematic errors according to DIN EN ISO 13849-1 :2008, section 4.6.3. The software must be validated according to section 9.5 of EN ISO 13849-2:2013.

Evaluation

The F-PLC forms the activation system for operating 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 :2008, section 4.6.3. The software must be additionally validated according to section 9.5 of EN ISO 13849-2:2013.

The PFH of the activation system corresponds to the PFH of the F-PLC used for activation of the operating mode. If the aforementioned measures are taken in accordance with the PL of the F-PLC and are successfully validated when the SRASW is created, then the PL of the F-PLC used can be assumed as the PL of the activation system.

8. Conclusion

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

Actual execution of the operating mode selection safety function is performed by the activation system, with the selection system defining the operating 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 operating mode.

With application of the procedure described and under the conditions stated in chapter 7, the Performance Level of the activation system can be assumed as the Performance Level of the operating mode selection safety function.

9. Dokumente

- AP000169.1 Definition of the Electronic-Key structure on an EKS Electronic-Key, V2, 09.2015
- AP000169.2 Setting up the EKM software as a programming station V2, 09.2015
- AP000169.3 EKS Profibus on Siemens S7-300 – reading in EKS Electronic-Keys, V2, 09.2015
- AP000169.4 EKS Profinet on Siemens S7-300 – reading in EKS Electronic-Keys, V2, 09.2015
- AP000169.5 EKS on Siemens S7-300 – checking CRC, V2, 09.2015
- AP000169.6 EKS with data interface – information transfer to machine manufacturers, V2, 09.2015
- AP000169.7 EKS FSA on Siemens S7-300 – operating mode selection with touchscreen, V2, 09.2015
- Inspection certificate 12023, BG ETEM, 20 February 2013

IFA – Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

By order Technical auditor:	Reviewed by:
Dipl.-Ing. Ralf Apfeld	B.Sc. Stefan Otto