Prüf- und Zertifizierungsstelle
im BG-PRÜFZERT

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

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***	Betriebsartenwahl unter Nutzung des EKS light FSA als Zugangssystem
	Hersteller/ ***Manufacturer***	s.o.
	Bezeichnung/ ***Designation***	Verfahren zur Realisierung der Betriebsartenwahl an Maschinen unter Nutzung des EKS light FSA als Zugangssystem
	Kennzeichnung/ ***Marking***	EKS light FSA
	Weitere Angaben/ ***Further details***	–
3.	**Betreiber/** ***Operating company***	–

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

4. Veranlassung

Das IFA wurde vom Hersteller beauftragt, ein Verfahren zur Realisierung der Betriebsartenwahl an Maschinen unter Nutzung des EKS light FSA als Zugangssystem zu bewerten. Es soll evaluiert werden, ob mithilfe des EKS light FSA – in Verbindung mit einer Sicherheits-SPS (SSPS), einem HMI (Human Machine Interface) und einer SPS – eine der Betriebsartenwahl per elektromechanischem Betriebsartenwahlschalter gleichwertige Sicherheit erreicht werden kann. Dabei soll auch bewertet werden, ob das EKS Light FSA im Hinblick auf seine Funktion als Zugangssystem die strukturellen Anforderungen der Kategorie 3 nach DIN EN ISO 13849-1 erfüllt.

5. Beschreibung

Beim EKS light FSA handelt es sich um ein elektronisches Schlüsselsystem, bestehend aus Lesegerät und elektronischem Schlüssel. Das Lesegerät besitzt eine integrierte Auswerteelektronik und Schnittstellen zur Datenausgabe. Auf dem Schlüssel sind ein Betriebsmodus, eine Zugriffsstufe, eine Zugriffscodierung, eine Seriennummer und eine Prüfsumme über die auf dem Schlüssel vorhandenen Daten gespeichert.

Die Zugriffsstufe ist in einem Datenwort gespeichert. Zur Sicherung gegen Verfälschung besitzen die gültigen Datenwörter eine Hammingdistanz von h = 8. Die Zugriffsstufe entspricht dabei einer von fünf möglichen Betriebsarten und der hierarchisch höchsten Betriebsart, zu deren Wahl der Schlüsselbesitzer berechtigt ist.

Die Auswertung der Schlüsseldaten (unter anderem Berechnung und Vergleich der Prüfsummen) erfolgt redundant über zwei Prozessoren. Das Ergebnis der Auswertung wird zwischen den Prozessoren über kreuzweisen Datenvergleich überprüft.

Neben einer 4-Bit-parallelen Schnittstelle (Ausgänge A, B, C und D) und einem Strobe-Ausgang (STR) verfügt das Lesegerät des EKS light FSA über einen Halbleiter-Relaisausgang LA. Über die Ausgänge A-D und STR wird durch den ersten Prozessor die Information geliefert, ob ein gültiger Schlüssel gesteckt und welche Zugriffsstufe dem Schlüssel zugeordnet ist. Dabei werden je nach Zugriffsstufe jeweils einer der fünf Ausgänge auf High gesetzt und die anderen Ausgänge abgeschaltet. Der Ausgang LA liefert durch den zweiten Prozessor redundant die Information, ob – unabhängig von der Berechtigungsstufe – ein gültiger Schlüssel gesteckt ist. Beim Entfernen des Schlüssels werden sämtliche Ausgänge und der Schaltkontakt abgeschaltet.

Die Ausgänge A bis D, STR und LA werden an sichere Eingänge der SSPS angeschlossen. Die SSPS prüft die Plausibilität der empfangenen Daten. Eine Plausibilität liegt dann vor, wenn – bei gestecktem Schlüssel – einer der fünf Ausgänge A bis D und STR sowie LA oder – bei gezogenem Schlüssel – keiner der Ausgänge des EKS light FSA auf High gesetzt ist. Wird durch Eingangssignale plausibel – sowohl bezüglich des zeitlichen Ablaufs als auch der gesetzten Eingänge – ein gültiger Schlüssel angezeigt, wird die übermittelte Zugriffsstufe in der Codierung als Datenwort (Hammingdistanz h = 8) über die SPS an das HMI übermittelt. Auf Basis der

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

empfangenen Zugriffsstufe kann der Bediener auf dem HMI eine Betriebsart auswählen. Die Betriebsart wird an die SSPS gesendet, dort auf Plausibilität mit der durch das Lesegerät empfangenen Zugriffsstufe überprüft, und zur erneuten Bestätigung durch den Bediener an das HMI zurückgesandt. Über das Rücklese- und Bestätigungsverfahren unter Verwendung wechselnder Codierungen und kontinuierlicher Plausbilitätsprüfungen durch die SSPS wird die angewählte Betriebsart verifiziert und etwaige Fehler bei Anwahl oder Datenübertragung erkannt. Das Verfahren entspricht einer sicheren Parametereingabe nach DIN EN ISO 13849-1. Zur Aufdeckung von Stuck-At-Fehlern in allen beteiligten Komponenten wird das gleiche Verfahren auch bei gezogenem Schlüssel angewandt. Hier erfolgt die Quittierung durch das HMI automatisch. Durch die Verschiedenheit der Quittierungssignale bei gestecktem und gezogenem Schlüssel werden etwaige Fehler im HMI sicher erkannt. Die sichere Umschaltung der Betriebsart und die Aktivierung der für die Betriebsart erforderlichen Sicherheitsfunktionen erfolgt über die SSPS.

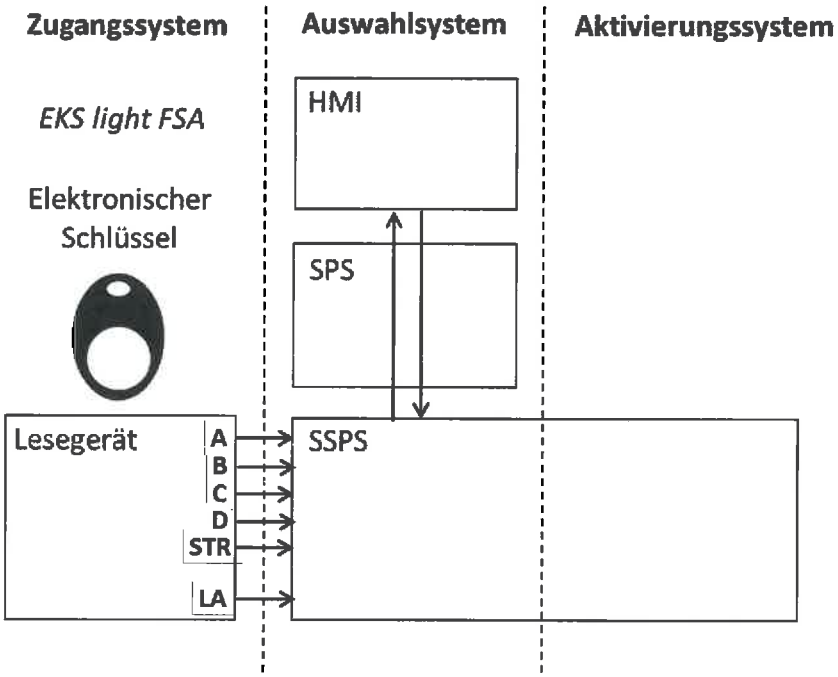

Abbildung 1: Prinzipschaltbild der Betriebsartenwahl

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

6. Sicherheitstechnische Bewertung

Für die sicherheitstechnische Bewertung wird die Komponentenstruktur des vorgestellten Verfahrens in drei funktionale Bestandteile aufgegliedert (siehe Abbildung 1).

6.1. Zugangssystem

Anforderungen

Das Zugangssystem ist der Teil der Wahleinrichtung, der die Möglichkeit zur Betriebsartenwahl auf bestimmte Personengruppen einschränkt und eine versehentliche oder missbräuchliche Betätigung des Auswahlsystems verhindert. Da die Anwahl jeder Betriebsart mit der Aktivierung anderer Sicherheitsfunktionen einhergeht, wird das Zugangssystem als sicherheitsrelevant betrachtet.

Bei elektromechanischen Wahleinrichtungen wird der Zugang durch den Schlüssel realisiert. Hier kann durch eine mechanische Codierung des Schlüssels die Anwahl nur bestimmter Betriebsarten freigegeben werden. Hinzu kommen organisatorische Maßnahmen, die den Zugriff auf den oder die Schlüssel auf bestimmte Personenkreise einschränken sollen.

Das EKS light FSA muss eine dem Zugangssystem elektromechanischer Betriebsartenwahlschalter mindestens gleichwertige Sicherheit aufweisen. Diese Anforderung ergibt sich aus der Maschinenrichtlinie 2006/42/EG, Abschnitt 1.2.5., die es dem Anwender freistellt, den Betriebsartenwahlschalter durch eine andere Wahleinrichtung zu ersetzen, durch den „die Nutzung bestimmter Funktionen der Maschine auf bestimmte Personenkreise beschränkt werden kann".

Bewertung

Das Zugangssystem zur Betriebsartenwahl wird gebildet durch das EKS light FSA. Im Rahmen der Untersuchung wurden das Schaltungsprinzip und die Software des Lesegeräts einer Bewertung unterzogen. Die Übereinstimmung der über die Schnittstellen zur SSPS übertragenen mit der auf dem Schlüssel tatsächlich gespeicherten Zugriffsstufe wurde nicht bewertet. Stattdessen wird das Schaltungsprinzip und die Software auf folgende Funktion hin bewertet: Nur, wenn ein gültiger Schlüssel am Lesegerät gesteckt ist, wird auf den Ausgängen des ersten <u>und</u> des zweiten Kanals das Stecken eines gültigen Schlüssel signalisiert.

Die Bewertung kommt zu folgendem Ergebnis: Das EKS light FSA erfüllt als Zugangssystem der Sicherheitsfunktion Betriebsartenwahl im Hinblick auf die im letzten Abschnitt definierte Funktion die strukturellen Anforderungen der Kategorie 3 nach DIN EN ISO 13849-1.

Zu dieser Bewertung tragen folgende Eigenschaften bei:

- Die Auswertung der Schlüsseldaten im EKS light FSA erfolgt auf zwei unterschiedlichen Prozessoren mit unterschiedlicher Software
- Beide Prozessoren verfügen über eine eigene Überspannungsüberwachung

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

- Einer der Prozessoren verfügt zusätzlich über eine Unterspannungs-überwachung

Bezüglich der Software sind folgende Punkte anzumerken:

- Die Software auf den Prozessoren wurde in jeweils unterschiedlichen Programmiersprachen implementiert
- Das Einlesen der Daten vom Schlüssel erfolgt einkanalig durch den ersten Prozessor. Der Einleseprozess wird vom zweiten Prozessor überwacht. Während des Einlesevorgangs werden alle Schlüsseldaten an den zweiten Prozessor übertragen.
- Die Auswertung der Schlüsseldaten erfolgt redundant auf beiden Prozessoren.
- Der erste Prozessor setzt die Ausgänge A-D, STR unabhängig vom zweiten Prozessor. Bevor der zweite Prozessor den Ausgang LA1/LA2 aktiviert, findet ein Kreuzvergleich der Ergebnisse der Auswertung statt. Bei Nicht-Übereinstimmung der Ergebnisse der Auswertung werden die Ausgänge A-D, STR durch den ersten Prozessor zurückgesetzt

Aufgrund der beschriebenen Eigenschaften kann das EKS light FSA in Bezug auf die oben beschriebene Funktion als einfehlersicher bewertet werden.

Für das EKS light FSA wird eine dem Zugangssystem bei der Betriebsartenwahl per konventionellem Schlüssel mindestens gleichwertige Sicherheit bestätigt.

6.2. Auswahlsystem

Anforderungen

Das Auswahlsystem legt die Betriebsart fest, welche durch das Aktivierungssystem in der Steuerung aktiviert werden soll.

Bei elektromechanischen Wahleinrichtungen entspricht das Auswahlsystem dem handbetätigten Schaltknopf, dessen Stellung z.B. über eine Achse und Nockenscheiben mechanisch auf die elektrischen Kontaktelemente übertragen wird.

Bei elektronischen Wahleinrichtungen wird das Auswahlsystem in der Regel über eine Benutzerschnittstelle realisiert. Über die Benutzerschnittstelle und eventuell weitere elektronische Komponenten wird durch die Bedienperson die in der Maschinensteuerung zu aktivierende Betriebsart festgelegt. Da hier in der Regel Standardkomponenten zum Einsatz kommen, ist eine Einstufung eines in dieser Art realisierten Auswahlsystems in PL c oder höher nur mit zusätzlichen Maßnahmen möglich. Eine Möglichkeit bietet Abschnitt 4.6.4 der Norm, in dem Vorgaben zur softwarebasierten Parametrisierung genannt werden. Da die Betriebsartenwahl über ein elektronisches Auswahlsystem einer softwarebasierten Parametrisierung gleichkommt, kann der genannte Abschnitt der Norm für die sicherheitstechnische Bewertung dieses Auswahlsystems herangezogen werden. Das dort beschriebene Verfahren umfasst die Auswahl der Betriebsart durch die Bedienperson, die Prüfung der ausgewählten Betriebsart in der sicheren Steuerung sowie die Bestätigung der

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

ausgewählten Betriebsart durch die Bedienperson. Dadurch wird sichergestellt, dass die Integrität der für die Parametrisierung verwendeten Daten entlang der gesamten Kommunikationskette aufrechterhalten bleibt und Verfälschungen erkannt werden. Insbesondere wird vermieden, dass ein Fehler in einer der Komponenten der Wahleinrichtung zur Anwahl oder Bestätigung einer falschen Betriebsart führen kann.

Die angewählte Betriebsart muss dem Benutzer angezeigt werden. Diese Forderung ergibt sich aus der Maschinenrichtlinie 2006/42/EG, Abschnitt 1.2.5 und der Forderung, dass jede Stellung des Betriebsartenwahlschalters deutlich erkennbar sein muss.

Bewertung

Das Auswahlsystem zur Betriebsartenwahl wird gebildet durch SPS, HMI und Sicherheits-SPS.

Das für die Auswahl der Betriebsart angewandte Verfahren der Rückübertragung der angewählten Betriebsart, deren nachfolgende Bestätigung durch den Bediener und Überprüfung durch die SSPS genügt dem in der DIN EN ISO 13849-1, Abschnitt 4.6.4 geforderten Verfahren zu Parametrisierung.

Die Kontrolle über den Bereich gültiger Eingaben erfolgt in der SSPS durch Abgleich der gewählten Betriebsart mit der an die SSPS übertragenen Berechtigungsstufe. Verfälschte oder unvollständige Daten werden über die gewählte Hammingdistanz der gültigen Datenwörter und die kontinuierliche Kontrolle der an der Benutzerschnittstelle angewählten Parameter in der SSPS in sicherer Technik erkannt.

Eine zuverlässige Fehlererkennung in HMI und SPS wird vor allem dadurch erreicht, dass die Codierung der übertragenen Parameter mit jedem Verfahrensschritt wechselt. Auf diese Weise wird ein fehlerbedingtes wiederholtes Senden eines Datenwortes als Fehler erkannt. Bei korrekter Anwendung des Verfahrens und der von der Firma Euchner im Dokument AP000200-01.4 vorgestellten Codierung wird auch die in DIN EN ISO 13849-1 enthaltene Forderung nach einer Diversität der Komponenten als in gleichwertiger Weise erfüllt betrachtet. Systematische Ausfälle werden beherrscht.

Die Erstellung der Software zur Parametrisierung muss durch den Anwender durchgeführt werden. Die Firma Euchner beschreibt hierzu lediglich das anzuwendende Verfahren. Entsprechend muss auch die Verifikation der Software nach DIN EN ISO 13849-1, Abschnitt 4.6.4 durch den Anwender erfolgen. Bei Maschinen nach Anhang IV der Maschinenrichtlinie 2006/42/EG ist gegebenenfalls eine Verifikation der Software durch eine Prüfstelle erforderlich.

Kann die Betriebsart dem Bediener nach Anwahl auf dem HMI nicht angezeigt werden, so ist durch den Anwender sicherzustellen, dass die Betriebsart dem Bediener der Maschine auf einem anderen, deutlich sichtbaren Weg angezeigt wird.

6.3. Aktivierungssystem

Anforderungen

Auf dem Aktivierungssystem wird die eigentliche Sicherheitsfunktion, die „Aktivierung der für die ausgewählte Betriebsart erforderlichen Sicherheitsfunktionen“ ausgeführt.

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Hierfür wird in Abhängigkeit der ausführenden Komponenten ein PL vergeben. Der erforderliche PL der Sicherheitsfunktion ergibt sich aus der Risikoanalyse oder den Anforderungen der verwendeten Produktnorm.

Zusätzlich müssen bei Erstellung der sicherheitsbezogenen Applikationssoftware (SRASW) der SSPS entsprechend des PL_r Maßnahmen zur Vermeidung systematischer Fehler nach DIN EN ISO 13849-1, Abschnitt 4.6.3 angewandt werden. Die Software muss nach Abschnitt 9.5 der DIN EN ISO 13849-2 validiert werden.

Bewertung

Das Aktivierungssystem zur Betriebsartenwahl wird durch die SSPS gebildet.

Die sicherheitsbezogene Software muss durch den Anwender erstellt werden. Die Firma Euchner beschreibt hierzu lediglich das anzuwendende Verfahren. Entsprechend obliegt die Anwendung der in DIN EN ISO 13849-1, Abschnitt 4.6.3 genannten Maßnahmen dem Anwender. Zusätzlich muss die Software entsprechend Abschnitt 9.5 der DIN EN ISO 13849-2 validiert werden.

Die mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls der Sicherheitsfunktion Betriebsartenwahl wird aus der PFH_D der als Aktivierungssystem verwendeten SSPS gebildet. Voraussetzung ist, dass bei der Erstellung der SRASW die oben genannten Maßnahmen entsprechend des PL der SSPS angewendet und erfolgreich validiert werden.

7. Fazit

Das EKS light FSA erfüllt als Zugangssystem die strukturellen Anforderungen der Kategorie 3 nach DIN EN ISO 13849-1. Eine Einfehlersicherheit ist damit gegeben. Die Übereinstimmung der übertragenen mit der auf dem Schlüssel gespeicherten Zugriffsstufe wurde nicht bewertet.

Das von der Firma Euchner vorgestellte Verfahren ist dazu geeignet, bei korrekter Implementierung und geeigneter Auswahl der Komponenten die Sicherheitsfunktion Betriebsartenwahl mit einer der Betriebsartenwahl per elektro-mechanischem Betriebsartenwahlschalter mindestens gleichwertigen Sicherheit auszuführen.

Die eigentliche Ausführung der Sicherheitsfunktion Betriebsartenwahl erfolgt durch das Aktivierungssystem, wobei das Auswahlsystem die Betriebsart als Parameter der Sicherheitsfunktion festlegt. Die Sicherheitsfunktion wird dabei wie folgt definiert: Aktivierung der für die jeweilige Betriebsart erforderlichen Sicherheitsfunktionen.

Als Performance Level der Sicherheitsfunktion Betriebsartenwahl kann unter Anwendung des beschriebenen Verfahrens und den in Kapitel 6 genannten Bedingungen der Perfomance Level des Aktivierungssystems angesetzt werden.

D-53757 Sankt Augustin *Tel.:(02241)231-02* *Fax:(02241)231-2234* *email: ifa@dguv.de* *UB 7*

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

8. Dokumente

- AP000200-01.4 EKS Light FSA an Siemens S7-300 – Betriebsartenwahl mit Touchscreen, V2, 31.03.2016
- LP-KPL AUSWERTUNG FSA (Schaltplan), V1, 23.06.2015
- Software EKS Light FSA, V15

IFA – Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Im Auftrag
Fachzertifizierer:

Dipl.-Ing. Ralf Apfeld

Prüfer:

B.Sc. Stefan Otto