Prüf- und Zertifizierungsstelle
im BG-PRÜFZERT

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

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***	Verfahren 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***	

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 FSA (Electronic Key System For Safety Applications) als Zugangssystem zu bewerten. Es soll evaluiert werden, ob mithilfe des EKS FSA – in Verbindung mit einer SPS, einem HMI (Human Machine Interface) und einer SSPS – und unter Beachtung der in DIN EN ISO 13849-1:2008, Abschnitt 4.6.4 beschriebenen Vorgaben zur sicheren softwarebasierten Parametrierung eine der Betriebsartenwahl per elektro-mechanischem Betriebsartenwahlschalter gleichwertige Sicherheit erreicht werden kann.

5. Beschreibung

Es soll ein Verfahren zur Realisierung der Betriebsartenwahl an Maschinen unter Nutzung des EKS FSA als Zugangssystem realisiert werden.

Beim EKS FSA handelt es sich um ein elektronisches Schlüsselsystem, bestehend aus Schlüsselaufnahme und elektronischem Schlüssel. Die Schlüsselaufnahme ist ein Schreib-/Lesesystem mit integrierter Schnittstellenelektronik. Beim Schlüssel handelt es sich um einen elektronischen Schlüssel mit Schreib-/Lese- und Festcode-Speicherbereich, in dem die Seriennummer des Schlüssels hinterlegt ist. Im programmierbaren Speicherbereich können bei Konfiguration des Schlüssels neben weiteren Daten die für den Zugang zur Betriebsartenwahl relevanten Daten gespeichert werden.

Die Berechtigungsstufe für die Betriebsartenwahl wird in einem Datenwort auf dem programmierbaren Speicherbereich des Schlüssels gespeichert. Zur Sicherung gegen Verfälschung besitzen die gültigen Datenwörter eine Hammingdistanz von h = 8. Die auf dem Schlüssel gespeicherte Berechtigungsstufe entspricht dabei der hierarchisch höchsten Betriebsart, zu deren Wahl der Schlüsselbesitzer berechtigt ist.

Verfügt die Maschine lediglich über drei oder weniger Betriebsarten, kann alternativ eine Speicherung der Berechtigungsstufe in einem Datenbyte erfolgen. In diesem Fall beträgt die Hammingdistanz h = 5.

Das EKS FSA verfügt neben einer Datenschnittstelle über einen zusätzlichen Halbleiter-Relaisausgang, der abgeschaltet ist, solange sich kein Schlüssel in der Schlüsselaufnahme befindet oder der Schlüssel nicht gelesen werden kann.

Über die Datenschnittstelle ist das EKS FSA zur Übermittlung der für die Betriebsartenwahl relevanten Daten an die SPS angebunden. Der Halbleiter-Relaisausgang ist mit einem sicheren Eingang der SSPS verknüpft. Die SPS sendet die Daten des EKS FSA an das HMI sowie über wechselnde Merkerworte an die SSPS weiter. Hier findet eine Prüfung der erhaltenen Daten auf Gültigkeit statt. Auf Basis der Berechtigungsstufe kann der Benutzer auf dem HMI eine Betriebsart anwählen und an die SSPS weiterleiten. Über ein Rücklese- und Bestätigungsverfahren wird die angewählte Betriebsart verifiziert und etwaige Fehler bei Anwahl oder Datenübertragung erkannt.

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Die sichere Umschaltung der Betriebsart und die Aktivierung der für die Betriebsart erforderlichen Sicherheitsfunktionen erfolgt über die SSPS.

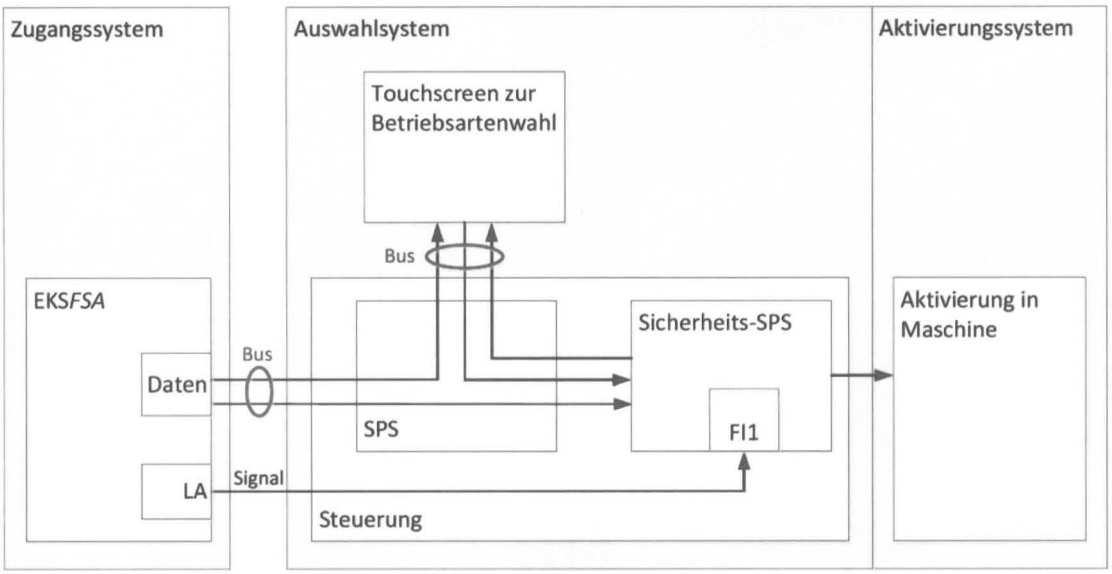

Abbildung 1: Prinzipschaltbild der Betriebsartenwahl

6. Verfahrensbeschreibung

EKS FSA / SPS

Bei Stecken eines Schlüssels in das Lesegerät werden die Schlüsseldaten über die Datenschnittstelle an die SPS weitergeleitet. Der Halbleiter-Relaisausgang wird auf High gesetzt. Nach positiv abgeschlossener Auswertung der Prüfsummen in der SPS wird die Berechtigungsstufe des Schlüssels an das HMI sowie an die SSPS weitergeleitet.

Bei Entfernen des Schlüssels wird die Datenschnittstelle auf Null gesetzt und der Halbleiter-Relaisausgang abgeschaltet. Auf Basis der erhaltenen Daten führt die SPS eine Prüfsummenberechnung durch, als deren Ergebnis eine Null erwartet wird. Bei korrektem Prüfsummenergebnis wird die Null an das HMI und an die SSPS weitergeleitet.

HMI

Auf dem HMI werden in Abhängigkeit der eingelesenen Berechtigungsstufe die Betriebsarten angezeigt, zu deren Anwahl der Bediener berechtigt ist. Nach Anwahl der Betriebsart wird die gewählte Betriebsart an die SSPS gesendet. Die SSPS sendet eine Rückmeldung über die gespeicherte Betriebsart an das HMI zurück, wo sie vom Bediener quittiert werden muss. Die quittierte Betriebsart wird an die SSPS geschickt. Das Verfahren entspricht einer sicheren Parametereingabe nach DIN EN ISO 13849-1:2008 (siehe Abschnitt 7.2).

Bei entferntem Schlüssel wird auf dem HMI das Bild zur Betriebsartenwahl gesperrt. Als Rückmeldung des HMI wird ein leeres Datenwort zurückgegeben und an die SSPS

weitergeleitet. Die SSPS sendet eine Rückmeldung an das HMI zurück, welches die empfangene Null wiederum mit Rücksendung eines leeren Datenworts quittiert.

SSPS

Sobald auf dem sicheren Eingang ein Signalwechsel von Null auf Eins erfolgt, startet in der SSPS eine Zeiterwartung, bis die Berechtigungsstufe von der SPS erhalten wird. Bei Erhalt der Berechtigungsstufe wird überprüft, ob aufgrund der Daten eine Berechtigung zur Auswahl einer Betriebsart vorliegt, d.h. ob die Berechtigungsstufe größer als Null ist.

Sobald die SSPS die auf dem HMI angewählte Betriebsart erhalten hat, wird überprüft, ob die gewählte Betriebsart einer gültigen Betriebsart entspricht und der Bediener auf Basis der Berechtigungsstufe zu deren Anwahl berechtigt ist. Bei positivem Prüfabschluss wird die Betriebsart an das HMI zur Quittierung zurückgegeben. Nach Quittierung der Betriebsart wird überprüft, ob die quittierte mit der zuvor angewählten Betriebsart übereinstimmt. Bei positivem Prüfabschluss wird die Betriebsart von der SSPS in der Maschinensteuerung aktiviert. Bei einem erkannten Fehler geht die SSPS in einen Fehlermodus, welcher – sofern kein dauerhafter Fehler vorliegt – nur durch Ziehen des Schlüssels verlassen werden kann.

Bei Entfernen des Schlüssels wird nach entsprechendem Signalwechsel auf dem sicheren Eingang eine Zeiterwartung gestartet, bis die Daten von der SPS erhalten werden. Sowohl die Daten des EKS FSA als auch die vom HMI gesendeten Daten werden überprüft, ob sie je dem Erwartungswert Null entsprechen. Nur dann wird ein leeres Datenwort an das HMI zurückgegeben, das mit der Rücksendung einer Null das Sperren des Fensters zur Betriebsartenwahl quittiert. Bei einem erkannten Fehler geht die SSPS in einen Fehlermodus, welcher – sofern kein dauerhafter Fehler vorliegt – nur durch erneutes Stecken eines Schlüssels verlassen werden kann.

Die angewählte Betriebsart bleibt bei Ziehen des Schlüssels weiterhin aktiv.

7. Sicherheitstechnische Bewertung

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

7.1. Zugangssystem

Anforderungen

Mithilfe des Zugangssystems wird der Zugang zur Betriebsartenwahl auf bestimmte Personengruppen beschränkt und eine versehentliche oder missbräuchliche Anwahl einer Betriebsart verhindert. Gleichzeitig ist es möglich, durch die vergebene Berechtigungsstufe jedem Schlüsselinhaber den Zugang nur auf bestimmte Betriebsarten zu erlauben und so den zur Anwahl dieser Betriebsarten berechtigten Personenkreis auf speziell geschultes Personal einzuschränken.

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Da die Anwahl jeder Betriebsart mit der Aktivierung anderer Sicherheitsfunktionen einhergeht, wird das Zugangssystem als sicherheitsrelevant betrachtet.

Bei der Betriebsartenwahl mit elektro-mechanischem Wahlschalter entspricht das Zugangssystem dem Schlüssel. Durch mechanische Codierung des Schlüssels kann mit jedem Schlüssel nur der Zugang zur Anwahl bestimmter Betriebsarten möglich. In der Regel ist der elektrische Teil des Zugangssystems bei elektro-mechanischem Betriebsartenwahlschaltern einfehlersicher aufgebaut, sodass ein einfacher Fehler nicht zu einem Verlust der Sicherheit, in diesem Fall zur unbeabsichtigten Aktivierung einer Betriebsart führen kann.

Als sicherheitsrelevant sind ebenfalls die organisatorischen Maßnahmen zu bewerten, die verhindern sollen, dass Unbefugte Zugriff auf die Betriebsartenwahl erhalten. Diese Maßnahmen sind bei der Betriebsartenwahl per elektro-mechanischem Schalter nur niedrig zu bewerten, da Zugriffe nicht protokolliert werden, und die Praxis zeigt, dass Betriebsartenwahlschlüssel oft steckengelassen werden.

Das EKS FSA muss eine dem Zugangssystem elektro-mechanischer Betriebsarten-wahlschalter 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 FSA. Nach einem Inspektionsbericht der BG ETEM (Inspektionsbescheinigung 12023) vom 20.02.2013 erfüllt das EKS FSA die strukturellen Anforderungen der Kategorie 3 nach DIN EN ISO 13849-1:2008. Zusätzlich kann durch die gewählte Hammingdistanz die Restfehlerwahrscheinlichkeit für eine unerkannte Verfälschung eines Datenworts und eine unter Umständen daraus resultierende unbeabsichtigte Anwahl einer Betriebsart auf $1{,}2 \cdot 10^{-12}$ pro Stunde (h = 8) bzw. $5{,}43 \cdot 10^{-9}$ pro Stunde (h = 5) begrenzt werden.

Die organisatorischen Maßnahmen sind beim Einsatz des EKS FSA höher zu bewerten, da auf dem Chip neben der Berechtigungsstufe auch persönliche Daten des Bedieners gespeichert werden können, die es ermöglichen, einen Zugriff auf die Betriebsartenwahl rückführbar zu protokollieren. Der Zugriff auf die Konfigurationssoftware zur Programmierung der Schlüssel ist passwortgeschützt. Ein Manipulieren der Schlüsseldaten wird zusätzlich dadurch erschwert, dass die bei der Herstellung fest auf dem Schlüssel gespeicherte Seriennummer Bestandteil der über die Schlüsseldaten gebildeten Prüfsumme ist. Zusätzlich kann der Bereich der Prüfsummenbildung individuell eingestellt werden. Es ist davon auszugehen, dass diese Maßnahmen einen missbräuchlichen oder unberechtigten Zugang zur Betriebsartenwahl weitestgehend unterbinden.

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

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

7.2. Auswahlsystem

Anforderungen

Durch das Auswahlsystem wird die Betriebsart festgelegt, welche durch die SSPS auf der Steuerung aktiviert wird. Bei der Auswahl der Betriebsart handelt es sich daher um einen Vorgang der Parametrisierung.

Für die sicherheitstechnische Bewertung des Auswahlsystems sind die Vorgaben zur softwarebasierten Parametrisierung nach DIN EN ISO 13849-1:2008, Abschnitt 4.6.4 heranzuziehen. Danach muss sichergestellt sein, dass die Integrität aller für die Parametrisierung verwendeten Daten aufrechterhalten bleibt. Dies muss durch Anwendung folgender Maßnahmen erreicht werden:

- Kontrolle des Bereiches gültiger Eingaben
- Beherrschung von Datenverfälschungen vor der Datenübertragung
- Beherrschung der Auswirkungen von Abweichungen beim Prozess der Parameterübertragung
- Beherrschung der Auswirkungen beim Übertragen unvollständiger Parameter
- Beherrschung der Auswirkungen von Fehlern und Ausfällen der Hardware und Software des für die Parametrisierung verwendeten Werkzeugs

Darüber hinaus muss eine Bestätigung der Eingabeparameter erfolgen, in diesem Fall die Bestätigung der anzuwählenden Betriebsart. Dies muss durch Rückübertragung der modifizierten bzw. zu modifizierenden Parameter zum Parametrisierungswerkzeug sowie deren nachfolgende Bestätigung durch eine ausreichend geschulte Person und eine automatische Überprüfung durch das Parametrisierungswerkzeug geschehen.

Die an der Codierung/Decodierung der sicherheitsrelevanten Daten sowie deren Anzeige beteiligten Softwaremodule müssen zur Verhinderung systematischer Ausfälle diversitär ausgeführt sein.

Die Software zur Parametrisierung auf HMI und SPS muss nach folgenden Vorgaben verifiziert werden:

- Verifikation der korrekten Einstellung für jeden sicherheitsbezogenen Parameter;
- Verifikation, dass die sicherheitsbezogenen Parameter auf Plausibilität überprüft werden;
- Verifikation, dass unbefugte Modifikation von sicherheitsbezogenen Parametern verhindert ist;
- Verifikation, dass die Daten einer Parametrisierung so erzeugt und verarbeitet werden, dass Fehler nicht zu einem Verlust der Sicherheitsfunktion führen können.

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.

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Bewertung

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

Das in Kapitel 6 beschriebene Verfahren der Rückübertragung der angewählten Betriebsart, deren nachfolgende Bestätigung durch den Bediener und Überprüfung durch die SSPS genügt dem in der DIN EN ISO 13849-1:2008, 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 auf dem Schlüssel hinterlegten Berechtigungsstufe. Verfälschte oder unvollständige Daten werden über die gewählte Hammingdistanz der gültigen Datenwörter und die kontinuierliche Kontrolle der 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 AP000169.7 vorgestellten Codierung wird auch die in DIN EN ISO 13849-1:2008 enthaltene Forderung nach einer Diversität der Komponenten als in gleichwertiger Weise erfüllt betrachtet. Systematische Ausfälle werden beherrscht.

Einzig bei der Speicherung der Berechtigungsstufe in einem Datenbyte und einer Hammingdistanz von h = 5 kann es bei einem Fehler im HMI zu einer unbeabsichtigten Anwahl des Automatikbetriebs kommen. Da der Automatikbetrieb jedoch die Betriebsart mit den höchsten Sicherheitsanforderungen ist und keine speziellen Berechtigungen des Bedieners erfordert, wird dies als Ausfall in die sichere Richtung betrachtet und somit als unkritisch bewertet.

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 13849-1:2008, 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.

7.3. Aktivierungssystem

Anforderungen

Auf dem Aktivierungssystem wird die eigentliche Sicherheitsfunktion, die „Aktivierung der für die ausgewählte Betriebsart erforderlichen Sicherheitsfunktionen" ausgeführt. Hierfür wird in Abhängigkeit der ausführenden Komponenten ein PL vergeben. Der

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

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 13849-1:2008, Abschnitt 4.6.3 angewandt werden. Die Software muss nach Abschnitt 9.5 der EN ISO 13849-2:2013 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 13849-1:2008, Abschnitt 4.6.3 genannten Maßnahmen dem Anwender. Zusätzlich muss die Software entsprechend Abschnitt 9.5 der EN ISO 13849-2:2013 validiert werden.

Die PFH des Aktivierungssystems entspricht der PFH der für die Aktivierung der Betriebsart verwendeten SSPS. Werden bei der Erstellung der SRASW die oben genannten Maßnahmen entsprechend des PL der SSPS angewendet und erfolgreich validiert, kann als PL des Aktivierungssystems der PL der verwendeten SSPS angesetzt werden.

8. Fazit

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 7 genannten Bedingungen der Perfomance Level des Aktivierungssystems angesetzt werden.

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

9. Dokumente

- AP000169.1 Definition der Schlüsselstruktur auf einem EKS-Schlüssel, V2, 09.2015
- AP000169.2 Einrichten der EKM Software als Programmierplatz, V2, 09.2015
- AP000169.3 EKS-Profibus an Siemens S7-300-EKS Schlüssel einlesen, V2, 09.2015
- AP000169.4 EKS-Profinet an Siemens S7-300 – EKS Schlüssel einlesen, V2,09.2015
- AP000169.5 EKS an Siemens S7-300 – CRC prüfen, V2, 09.2015
- AP000169.6 EKS mit Datenschnittstelle – Weitergabe von Informationen an Maschinenbauer, V2, 09.2015
- AP000169.7 EKS FSA an Siemens S7-300 – Betriebsartenwahl mit Touchscreen, V2, 09.2015
- Inspektionsbescheinigung 12023, BG ETEM, 20.02.2013

IFA – Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Im Auftrag
Fachzertifizierer:

Dipl.-Ing. Ralf Apfeld

Prüfer:

B.Sc. Stefan Otto