Practical solutions for safety-related application programming

SOFTEMA

Michael Huelke, Albert Janik, Andy Lungfiel Institute for Occupational Safety and Health (IFA)

Background

- Manufacturers of machinery are increasingly using application programming of safety controls in order to implement safety functions
- The ISO 13849-1 and IEC 62061 standards define requirements concerning the development of softw. employed for safety functions
- Few examples and proposals for implementation of these requirements have been published to date
- The DGUV funded the project FP0319, in which a method was



Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

SOFTEMA@dguv.de

www.dguv.de/ifa

uletzt	verwendet	Öffnen	Speicherr	n Speichern <u>u</u> nt	ter <u>S</u> chlie	ßen P <u>e</u> r	sonen ve	rwalten	<u>D</u> okur	mente ver	walten	Vorherige Se	eite						
ojekt	A1 Sic	herheitsf	unktione	A2.4 IO-Liste	A3 Maßnah	men A4 Anf	orderunge	n B3 N	Iodularch	itektur	B4 Matrix	C+E B4 Ma	atrix kom	pakt C1 Codere	view D1 V	alidierung Änd	derungen	Protokoll 1	abelle laden
Alle	SF generiere	ı			Spalten Ausblend	en 🗖 Bea	arbeiten]											Formale Chec
Nr .	_SFK _Be	schreibung			_Schutz	_вмк	_NQuit	_SQuit	Q1	B1	B2	B3	_PLr	_Reaktionszeit	_Priorität	_Betriebsart	_Sperre	_Validierung	_Kommenta
									Quittiertaster	Motor	Motor	Motor							
									ACK	¥	M2	W3							
iF1	Wen abso abso	n Not-Halt EM halten, Motor halten, mit Qu	IST betätigt, M2 abschalt uittiertaster A	dann Motor M1 ten, Motor M3 ACK quittieren.	Not-Halt	EMST			Q	A	A	A	d	100ms	1	B0: Alle	x	ОК	
F2	Wen abso	n Schutztür S halten, mit Qu	G1 geöffnet uittiertaster A	, dann Motor M1 ACK quittieren.	Schutztür	SG1			Q	E	•	•	d 🗸	100ms	2	B1: Automatik 🖵	0		
SF3	Wen absc	n Schutztür S halten, mit Qu	G2 geöffnet uittiertaster A	, dann Motor M2 ACK quittieren.	Schutztür	SG2			Q		E ZE STO		d	100ms	2	B1: Automatik	x	ОК	
6F4	Wen Moto quitti	n Schutztürer r M1 abschalt eren.	n SG2 und S en, mit Quitt	G3 geöffnet, dann tiertaster ACK	Schutztüren	SG2 & SG3			Q	A	SS1 SS2 SOS SLS		d	100ms	2	B1: Automatik	x	ок	
F5	Wen betät Quitt	n Sicherheitsl igt, dann Moto iertaster ACK	eiste Schne or M3 abscha quittieren.	Illauftor SL_SG2 alten, mit	Sicherheitsl eiste Schnelllauft	SL_SG2			Q		SDI	A	d	100ms	2	B1: Automatik	x	not OK	
€€€																			
																	0	not OK	
																	Datum Name	09.04.2014 Marcel	
																	Signatur	Benus 1272993002	
																	Datum	16.05.2014	
																	Prüfen1	Willi Minmax	
																	Datum		

developed and evaluated with reference to examples from industry

- This IFA matrix method can be used to specify, validate and document the application software in accordance with the standards. Besides this procedure, other equally valid methods doubtless exist by means of which the requirements can be met
- IFA published a report 2/2016 "Safety-related application programming"
- In order for the IFA matrix method to be implemented efficiently, the IFA is developing SOFTEMA, a free software tool (like SISTEMA)
- In the summer of 2018, the IFA has been launching SOFTEMA in beta test at about hundred of German companies. The English version will be planned from 2020

uletz	verwendet	- Ö <u>f</u> fr	nen	Spe	ichern	Sp	eicher	n <u>u</u> nte	r	<u>S</u> chli	eßer	n	P <u>e</u> r	sonen verwa	lten <u>D</u> oku	umente ve	walten	Vorherige Se	eite			
rojekt	A1 Siche	rheitsfun	ktionen	A2	.4 10-Li	ste	A3 Ma	ßnahn	nen	A4 Aı	nforde	erung	en	B3 Modularch	itektur B	4 Matri	x C+E	B4 Matrix ko	mpakt	C1 Codereview	D1 Validierung	g Änderu ◀
Tabe	lle aktualisier	en				ſ	palten	ausble uts	nden- Outp	outs		Selel	ktion a	aktivieren	Selektion ar	nzeigen		-				
_Nr	_Betriebs	_Test	17	15	16	13	14	11	12	18	ľ	11	112	_SF_(Prio	_SF-Nam	01	O3	04	02	_Sperre	_Verifikati	_Validieru
			ST [E8.4]	_1 [E8.2]	_2 [E9.6]	_1 [E8.1]	_2 [E9.5]	_1 [E8.0]	_2 [E9.4]	G2 [E8.5]		_1 [E3.U]	_2 [E9.1]			11 [A24.0]	0 [A32.0]	S [A32.4]	13 [A24.2]			
C0			1	1	1	1	N .	1	1	1	1	0	(D	ALLOK	ON	ON	ON	ON	x	OK 🗸	ОК
C1	B0: Alle	C0	0	1	1	1		1	1	1	1	0	(0 SF1 (1)	Wenn Not-Halt	OFF IM1:	OFF IM1:	NOP	OFF IM1:	x	OK 🗸	ОК
C2	B1: Automatik	C0	1	C	0 0	1		1	1	1	1	0	(0 SF2 (2)	Wenn Schutztür	OFF IM2:	NOP	NOP	NOP	x	ОК	ОК
C3	B1: Automatik	C0 🗸	1	1	1	C) ()	1	1	1	0	(SF3 (2)	Wenn Schutztür	NOP	OFF IM3: and	NOP	NOP	0		
C4	B1: Automatik	C0	1	1	1	C) () (0	0	1	0	3	Markieru Zeile ein	ing setzen ing löschen ifügen	•	NOP	NOP	NOP	x	ОК	ОК
C5	B1: Automatik	C0	1	1	1	C) (1	1	0	0		Zeile(n) Spalte lö	löschen öschen	+	NOP	NOP	OFF IM6:	x	OK 🗸	ОК
C6	B2: Einrichtbet	C8 🗸	1	1	1	() ()	1	1	1	1		Spalte se Zelle(n)	etzen	•	ON not IM5:	OFF IM5:	NOP	o		
C7	B2: Einrichtbet	C8	1	1	1	C) ()	1	1	1	0		Zwische	Schutztür	·····	ON not IM5:	OFF IM5:	NOP	x	ОК	ОК
8	B2: Einrichtbet	C0	1	1	1	C) ()	1	1	1	0	(0 TF1 (2)	SG2 offen, SG3	NOP	OFF	ON	NOP	x	ОК	ОК
C9	B2: Einrichtbet	C8	1	1	1	C) ()	1	1	1	1		1 TF2 (2)	SG2 offen, SG3	NOP	OFF	ON	NOP	x	OK 🗸	ОК

Figure 1. List of safety functions in SOFTEMA

SOFTEMA characteristics and functions

- Users can create/modify their own specific project file templates
- SOFTEMA opens only one project file at a time for the specification and documentation of one application program
- Multiple instances of SOFTEMA can however be opened in order for multiple application programs to be worked on simultaneously
- SOFTEMA uses the Microsoft Excel (*.xlsx) format for its project files
- The files can be edited either in SOFTEMA or in Microsoft Excel itself

SOFTEMA will initially support the following functions:

Figure 2. C&E-Matrix for the software specification of a project in SOFTEMA

SOFTEMA engineering procedure

- General descriptions of the data structures: SOFTEMA Cookbook 1
- For a new project, open an empty but preformatted project template
- Complete the project description ("Project" table)
- Enter all safety functions in "A1 safety functions" table (Fig. 1)
- Enter/import the input and output signals in the "A2.4 IO list" table
- The catalogue of measures for error avoidance and the programming rules can be selected and adjusted in the "A3 Measures" table
- Required function blocks for the preprocessing/actuator operation level can be managed in the "B3 Module architecture" table
- Following these preparations, the "B4 Matrix C+E" table can be completed by automatic updating (Fig. 2)

- Tables, columns and rows can be can be added and adjusted in the project file according to the specific use
- Automatic updating of tables following modification of input data
- Formal verification of tables (for missing, conflicting or double entries)
- Management of project members and role-based user permissions
- Support during verification, validation, testing and modification
- Dedicated editors for the different forms of cell content
- Management of documents and changes
- Specific print functions and reports

sor SO	FTEMA - Software von Steuerungen an Maschinen v0.7.0 (Beta) - Roboterzelle Einri	chtbetrieb.xlsx (Username: Projel	ktleiten)			×	
Datei	Bearbeiten Drucken Ansicht Extras Rollen Hilfe						
Zuletz	t verwendet - Öffnen Speichern Speichern unter Schließen Perse	onen verwalten Dokumente ver	rwalten <u>V</u> orherige	e Seite			
Projek	t A1 Sicherheitsfunktionen A2.4 IO-Liste A3 Maßnahmen A4 Anforderungen E	3 Modularchitektur B4 Matrix C+	E B4 Matrix kompa	akt C1 Codereview	D1 Validierung Änd	Änd ◀ ▶	
_Nr	_Beschreibung	_Referenzblatt	_Validierung	_Kommentar	_Kommentar_Prüfen		
	Wurden die Aktivitäten durchgeführt?						
V1	Validierung Sicherheitsfunktionen (D1)	A1 Sicherheitsfunktionen	not OK				
V2	Validierung I/O-Check (D1)	A2.4 IO-Liste	ОК				
V3	Validierung normativer Anforderungen (D1)	A4 Anforderungen	ОК				
V4	Verifikation der Modularchitektur (V1)	B3 Modularchitektur	ОК				
V5	Verifikation der Matrix (V1)	B4 Matrix C+E	not OK				
V6	Validierung Matrix (D1)	B4 Matrix C+E	not OK			_	
V7	Verifikation Codereview	C1 Codereview	not OK				
V8	Prüfung der Peripheriegeräte		ОК				
V9	Prüfung der Sensoren		ОК				
	Ist die Dokumentation komplett?	1	1				
D1	Dokumente des V-Modells aus diesem Excel-Dokument		ОК				
D2	PDF-Ausdruck aller sicherheitsrelevanten Software inkl. Checksumme		ОК				
D3	PDF-Ausdruck der Hardwarekonfiguration (mit allen Einstellungen) inkl.		ОК				
D4	Archivierung der Handbücher aller Systemkomponenten		ОК				
D5	PDF-Ausdruck der Konfiguration von Peripheriegeräten inkl. Checksummen		ОК				
D6	Abnahmevorschriften der Hersteller (z.B. Parametrierung von		ОК				
D7	Einzuhaltende Vorgaben aus C-Normen		ОК			-	
C:\Dat	en\SOFTEMA\IFA-Report 2-2016\Report-Beispiele\Aktualisierung der Tabelle geänd	dert Ini-Datei: SOFTE	EMA.ini CB:	<leer></leer>	1		
Fin	uro 2 Validation aboat of a project						

• The software specification is then produced in the matrix by entry of the logic, linking the input signals to the output signals (Fig. 2, right) • Following specification and its verification, the program can be coded • Verification of the code is summarized in "C1 Code review" table Program validation is documented in "D1 Validation" table (Fig. 3) • All modifications are highlighted in the table (Fig. 1+2, yellow cells). The highlighting is deleted manually when coding, verification and validation of these modifications has been completed again