

Practical solutions for safety-related application programming

SOFTEMA

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

SOFTEMA@dguv.de

www.dguv.de/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 DGVU funded the project FP0319, in which a method was 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

_Nr	_SFK	_Beschreibung	_Schutz	_BMK	_NQuit	_SQuit	Q1	B1	B2	B3	_PLr	_Reaktionszeit	_Priorität	_Betriebsart	_Sperr	_Validierung	_Kommentar
SF1		Wenn Not-Halt EMST betätigt, dann Motor M1 abschalten, Motor M2 abschalten, Motor M3 abschalten, mit Quittertaster ACK quittieren	Not-Halt	EMST			ACK Quittertaster	M1	M2	M3		100ms		1 B0 Alle		OK	
SF2		Wenn Schutzstür SG1 geöffnet, dann Motor M1 abschalten, mit Quittertaster ACK quittieren	Schutzstür	SG1								100ms		2 B1 Automatik		not OK	
SF3		Wenn Schutzstür SG2 geöffnet, dann Motor M2 abschalten, mit Quittertaster ACK quittieren	Schutzstür	SG2								100ms		2 B1 Automatik		OK	
SF4		Wenn Schutzstüren SG2 und SG3 geöffnet, dann Motor M1 abschalten, mit Quittertaster ACK quittieren	Schutzstüren	SG2 & SG3								100ms		2 B1 Automatik		OK	
SF5		Wenn Sicherheitsrelais Schmelblauf SL_SG2 betätigt, dann Motor M3 abschalten, mit Quittertaster ACK quittieren	Sicherheitsrelais	SL_SG2								100ms		2 B1 Automatik		not OK	

Figure 1. List of safety functions in SOFTEMA

_Nr	_Betriebs	_Test	I7	I5	I6	I3	I4	I1	I2	I8	I11	I12	_SF_Prio	_SF_Nam	O1	O3	O4	O2	_Sperr	_Verfikat	_Validieru
C0			1	1	1	1	1	1	1	1	1	0	0	ALLOK	ON	ON	ON	ON		OK	OK
C1	B0: Alle	C0	1	1	1	1	1	1	1	1	1	0	0	SF1 (1) Wenn Not-Halt	OFF IM1:	OFF IM1:	NOP	OFF IM1:		OK	OK
C2	B1: Automatik	C0	1	0	0	1	1	1	1	1	1	0	0	SF2 (2) Wenn Schutzstür	OFF IM2:	NOP	NOP	NOP		OK	OK
C3	B1: Automatik	C0	1	1	1	0	0	1	1	1	1	0	0	SF3 (2) Wenn Schutzstür	NOP	OFF IM3 and IM4:	NOP	NOP		OK	OK
C4	B1: Automatik	C0	1	1	1	0	0	0	0	1	1	0	0		NOP	NOP	NOP		OK	OK	
C5	B1: Automatik	C0	1	1	1	0	0	1	1	1	1	0	0		NOP	NOP	OFF IM3:		OK	OK	
C6	B2: Einrichtbet	C8	1	1	1	0	0	1	1	1	1	1	1		ON not IM5:	OFF IM5:	NOP		OK	OK	
C7	B2: Einrichtbet	C8	1	1	1	0	0	1	1	1	1	0	0		ON not IM5:	OFF IM5:	NOP		OK	OK	
C8	B2: Einrichtbet	C0	1	1	1	0	0	1	1	1	1	0	0	TF1 (2) SG2 offen, SG3	NOP	OFF	ON	NOP		OK	OK
C9	B2: Einrichtbet	C8	1	1	1	0	0	1	1	1	1	1	1	TF2 (2) SG2 offen, SG3	NOP	OFF	ON	NOP		OK	OK

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)
- 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

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:

- Tables, columns and rows 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

_Nr	_Beschreibung	_Referenzblatt	_Validierung	_Kommentar	_Kommentar_Prüfen
Wurden die Aktivitäten durchgeführt?					
V1	Validierung Sicherheitsfunktionen (D1)	A1 Sicherheitsfunktionen	not OK		
V2	Validierung IO-Check (D1)	A2.4 IO-Liste	OK		
V3	Validierung normativer Anforderungen (D1)	A4 Anforderungen	OK		
V4	Verifikation der Modularchitektur (V1)	B3 Modularchitektur	OK		
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		OK		
V9	Prüfung der Sensoren		OK		
Ist die Dokumentation komplett?					
D1	Dokumentation des V-Modells aus diesem Excel-Dokument		OK		
D2	PDF-Ausdruck aller sicherheitsrelevanten Software inkl. Checksumme		OK		
D3	PDF-Ausdruck der Hardwarekonfiguration (mit allen Einstellungen) inkl.		OK		
D4	Archivierung der Handbücher aller Systemkomponenten		OK		
D5	PDF-Ausdruck der Konfiguration von Peripheriegeräten inkl. Checksummen		OK		
D6	Abnahmevorschriften der Hersteller (z.B. Parametrierung von		OK		
D7	Einzeltastende Vorgaben aus C-Normen		OK		

Figure 3. Validation sheet of a project in SOFTEMA