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**

IFA
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

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 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

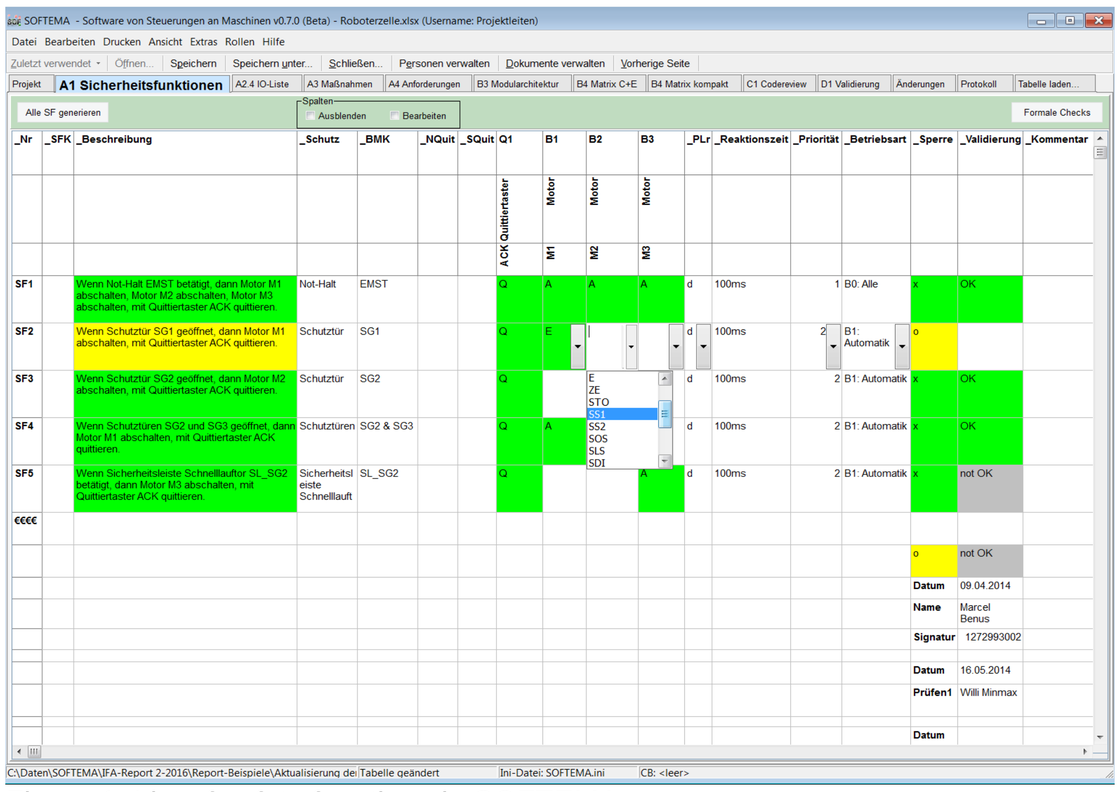

Figure 1. List of safety functions in SOFTEMA

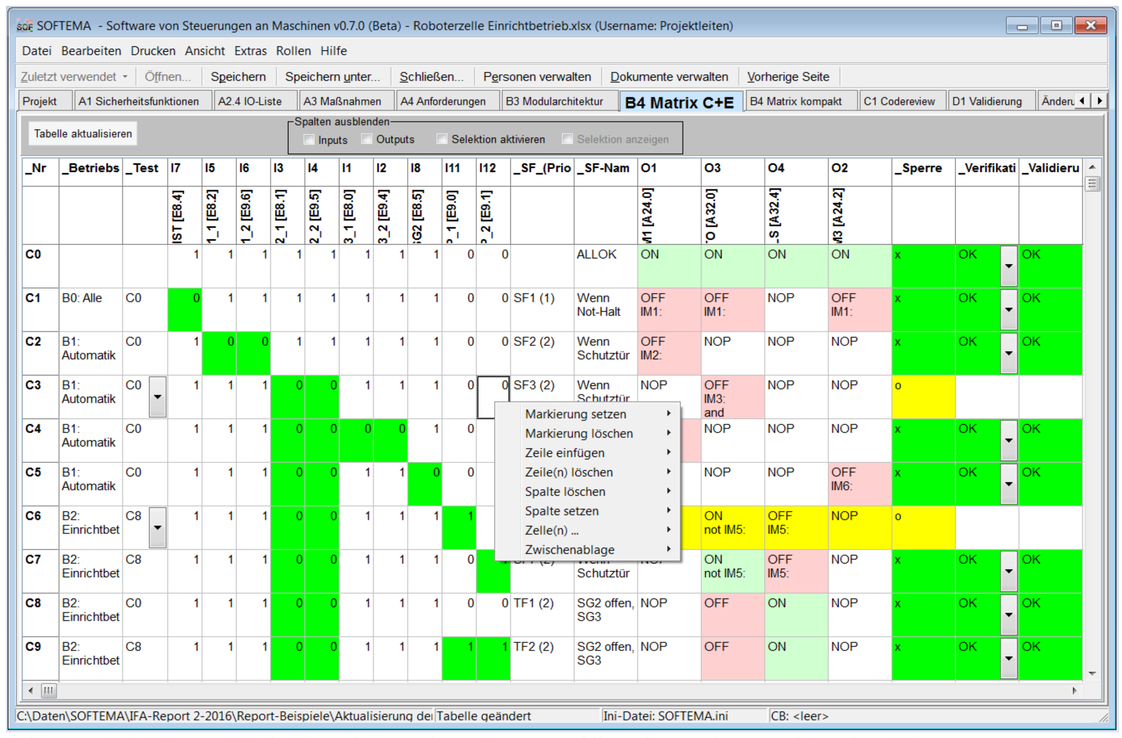

Figure 2. C&E-Matrix for the software specification of a project in SOFTEMA

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:

- 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

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

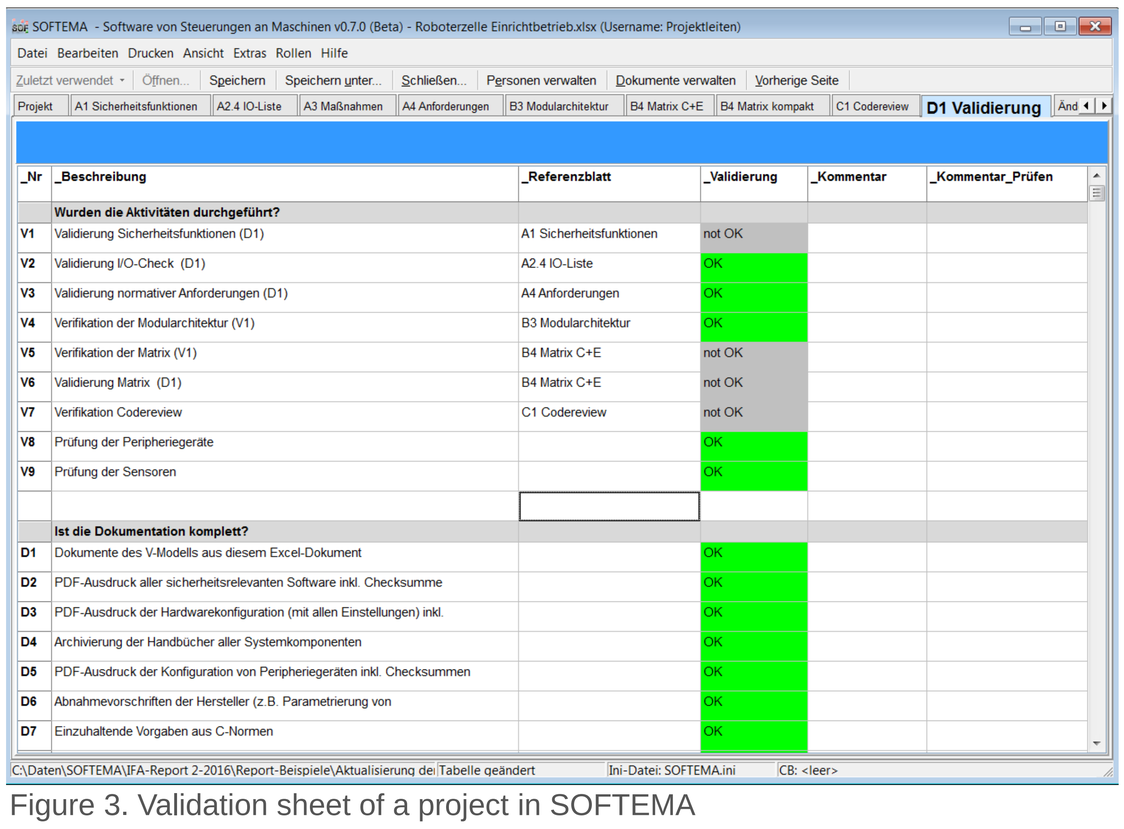

Figure 3. Validation sheet of a project in SOFTEMA