SOFTEMA – Getting Started

1   Introduction

This publication describes the first steps involved in using the SOFTEMA software assistant and provides references to the website and publications of the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA). All of the IFA publications mentioned can be downloaded as PDF files in German and will also be available in English in the future. Aside from a few exceptions, printed versions of the publications are not available. The majority of the links mentioned in this publication can also be accessed via the help menu in SOFTEMA.

2   Introduction to SOFTEMA – Downloading and installing

The SOFTEMA software assistant supports the assessment of the safety of control systems within the framework of the DIN EN ISO 13849-1 standard. It is becoming increasingly common for manufacturers of machinery to implement the safety features of their machines using programmable safety controllers. As a result, the functional safety of the controllers also relies on application programs that have undergone extensive development and testing. A key requirement set out in the relevant standards (e.g. DIN EN ISO 13849-1) is that these programs must be developed according to a structured work process and measures aimed at avoiding faults must be taken.

As part of a project funded by the German Social Accident Insurance (DGUV) (FF-FP 0319 "Standard-compliant development and documentation of safety-related application software in machine and plant construction"), the Hochschule Bonn-Rhein-Sieg University of Applied Sciences established a practically applicable development method. This matrix method developed by the IFA is used for the specification, validation and testing of safety-related application programs. This method requires multiple tables to be completed for different development phases.

On the basis of project IFA 5137, the machine control software application named SOFTEMA was developed for automated application of the tables used as part of the IFA matrix method. The purpose of SOFTEMA is to assist both machine manufacturers during the development of these programs and external bodies during the inspection and testing of such programs. The functions of SOFTEMA are intended to assist in reducing and detecting input errors and to generate documentation for programming and tests. The efficient and error-free modification of specifications and application software is a key aspect of SOFTEMA. It is intended to raise awareness of the IFA matrix method, and in doing so,assist the standard-compliant development of safety-related application software in the machine and plant construction sector.

You can find basic descriptions and specialist articles about SOFTEMA on the SOFTEMA homepage under "Further information". On this page, you can also download the latest version of SOFTEMA. The software components used in SOFTEMA and the system requirements are listed on the SOFTEMA homepage. You can also register for the SOFTEMA newsletter here, as well as within SOFTEMA itself (Section 7).

https://www.dguv.de/ifa/index-2.jsp

In general, it is always recommended that you use the latest version of the program. With each new version, software faults are patched and the functionality and usability of the software is improved. Multiple versions of SOFTEMA can be installed on one computer. To do this, the installation folders must be given different names. Example:

- SOFTEMA Version 1.0.0 is installed in the folder C:\Program Files\SOFTEMA100 and

- Version 1.3.0 is installed in the folder C:\Program Files\SOFTEMA130.

When SOFTEMA is launched for the first time, a prompt appears asking the user to specify a working folder. A default folder is pre-selected in the user profile. However, the user can also select a different folder. An example file and a project template is copied to this working folder. However, after this, project files can also be created and processed in other folders.

The installation folder contains a README file. This file can also be viewed via the SOFTEMA help menu. You can find further information on installing and uninstalling SOFTEMA in the section "SOFTEMA – Frequently Asked Questions/FAQ" at www.dguv.de/webcode/m1365190 or in SOFTEMA in the "Help → SOFTEMA FAQ" menu.

Licence information: SOFTEMA is classified as freeware and is approved for commercial use, for teaching purposes and for private use. SOFTEMA can be passed on to third parties. It is recommended that new users then register via the SOFTEMA menu. Modification of SOFTEMA or hosting of SOFTEMA on external servers for download is not permitted.

Exclusion of liability: Care has been taken in production of the software, which corresponds to the state of the art. It is made available to users free of charge. The liability of the IFA/DGUV is limited to intent and gross negligence (Section 521 German Civil Code) or with regard to material defects and legal defects (Sections 523 and 524 German Civil Code) to fraudulent concealment of such defects.

The IFA undertakes to keep its homepage free from viruses. Nevertheless, no guarantee can be given that the software and information provided are virus-free. Users are therefore advised to take appropriate security precautions and to use a virus scanner prior to downloading software, documentation or information.

Accessibility: The Declaration on Accessibility describes any barriers to the use of the software.

3   Introduction to the EN ISO 13849 standard on control systems

An important prerequisite for working with SOFTEMA is that the EN ISO 13849 series of standards, especially the software safety requirements in Section 7 of the standard, have been read and understood. The IFA provides information about this series of standards.

The IFA Report 2/2016 provides a general introduction to the topic "Safety-related application software for machinery" with ten SOFTEMA examples to download.

4   Engineering workflow in SOFTEMA

The typical engineering workflow when using SOFTEMA is outlined below. Processes and tips are described in "SOFTEMA Cookbooks". You can find basic descriptions of the SOFTEMA user interface, functions and data structures in SOFTEMA Cookbook 1 (Menu HELP → SOFTEMA COOKBOOK 1). The SOFTEMA Cookbook 2 (Menu "Help → SOFTEMA Cookbook 2") describes the steps for using SOFTEMA throughout the development process (V-Model).

https://www.dguv.de/ifa/index-2.jsp

For subsequent software specification of a safety function, the protective devices and actuators used in this function must be known. Therefore, an exact definition of the safety functions is essential for the subsequent steps (see SISTEMA Cookbook 6 and its examples).

For a new project, the user opens an empty, but already formatted project template ("__SOFTEMA_Template__.xlsx"), which is located in the working folder selected during installation, and saves this with a different file name.

In order to be able to make any changes in this document, users with corresponding roles (authorisations) must first be set up. To do this, the "Admin" of the project must log in under EXTRAS → USER MANAGEMENT. Initially the login information is as follows:

Admin user name: Admin
Password: admin
Answer to security question: Sankt Augustin

The password must be changed after the first log-in!

You can find more information about the role concept in SOFTEMA Cookbook 1 in Section 4.10. User management is described in detail in Section 4.11.

As a registered user with appropriate authorisations, you can now begin working on the project file.

After filling in the project description ("Project" table), the user enters the safety functions in table "A1 safety functions" along with their characteristics, such as PL_r, operating mode, priority etc. The input and output signals are entered in table "A2.4 IO list" with variable names and hardware/network addresses. In all tables, external content can also be copied and pasted via the clipboard.

The catalogue of measures to avoid faults and the programming rules can be selected and adjusted in table "A3 measures". The tables "A3 measures" and "A4 requirements" should be pre-filled in advance in the project template. The safety functions, peripheral hardware and IO list are used to create the list of required functional modules for the preprocessing and control level. These should be managed in table "B3 module architecture".

With these preparations, the table "B4 matrix C+E" can be filled in (Figure 1). This is carried out using the buttons for automatic updating of IO signals and safety functions.

https://www.dguv.de/ifa/index-2.jsp

Figure 1: Matrix C+E in SOFTEMA

The actual software specification is then carried out in table "B4 Matrix C+E" through

- Assignment of the input signals to the individual safety functions; and

- Entry of the logic linking the signals for the switching operations to the output signals.

The latter is required for the coding of the control logic. A specialised editor is available to assist with this linking process. For comprehensive projects, the compact view in table "B4 Matrix compact" can be useful. The user creates this table simply by using the update function, which converts the table "B4 Matrix C+E" automatically. By this point at the latest, all available functions for formal verification of the tables mentioned should be used to be able to discover and correct omissions, duplicates and contradictions.

Following the verification of all input documents and the specification process described above, the coding of the program can take place. The code is also verified. This process is documented in detail in a number of tables and is also summarised in the "C1 Codereview" table. The program is then validated, which is also documented in detail in a number of tables and summarised in the "D1 validation" table. In tables C1 and D1, the questions can be adjusted and added to as required. People that subsequently check the project can document their work and add comments.

In the event of modifications to the safety functions or the I/O signals, the changes from tables A1 and A2.4 are automatically updated in the specification tables and reviewed by the user. All modifications are first highlighted in yellow. The highlighting is manually removed after the repeated coding, verification and validation of these modifications is complete.

5   Further information about SOFTEMA

This publication "SOFTEMA – Getting Started" is available at http://www.dguv.de/webcode/m1365189 or can be accessed in SOFTEMA in the menu HELP → GETTING STARTED. It is

https://www.dguv.de/ifa/index-2.jsp

continuously updated.

The SOFTEMA error list continuously documents known errors for the installed SOFTEMA version and a possible remedy. It can be accessed in SOFTEMA in the menu HELP → SOFTEMA ERROR LIST.

6 Registration, updates and SOFTEMA newsletter

A newsletter is published occasionally about the SOFTEMA software. When downloading the software, you can sign up for the newsletter on the SOFTEMA homepage and it is sent to the email address entered. No further data iscollected.

This newsletter informs readers about new program versions and further information concerning the use of SOFTEMA. However, critical software errors are also announced via the newsletter. The user should make sure that the IFA email address SOFTEMA@dguv.de is not blocked by a spam filter or the like. At the end of each newsletter, users have the opportunity to delete their email address from the registration database.

In SOFTEMA in the HELP → NEWSLETTER MANAGEMENT menu, users can still register for the newsletter anytime, register with a new email address, or unsubscribe from the newsletter.

From within SOFTEMA, the command HELP → CHECK VERSION can also be used to check whether a newer version of SOFTEMA is available.

7 Support and training

SOFTEMA can also be used for commercial purposes free of charge. For this reason, the IFA is only able to offer a limited level of support. Please send any questions regarding installation, information about program faults or suggestions for improvement to: SOFTEMA@dguv.de.

Due to time constraints, the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) is unable to offer company training sessions. It only provides training for employees of the German social accident insurance institutions. Some German social accident insurance institutions may offer training. Searching the internet for "training", "seminar" and "SOFTEMA" brings up several external training providers.

Authors: Albert Bohlscheid, Andy Lungfiel, Martin Ulrich, Dr Michael Huelke
Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA),
Sankt Augustin