

SISTEMA 2.0

Overview of the main innovations

Overview

This information refers to SISTEMA 2.0 with the first published release version 2.0.6.

1 Introduction

The main innovations of SISTEMA 2.0 have been undertaken for the following reasons:

- Changes in the 3rd edition of EN ISO 13849-1:2015 [1], described in IFA Information [2]. SISTEMA 1.x.x refers to the 2nd edition of the standard.
- Implementation of an import interface and additional user interface for parameter libraries in the format of the VDMA¹ Standard Sheet 66413 [3]
- Extension of the data format (values and text fields) as a result of suggestions for improvement by users
- Further functions requested by users.

This information starts off by describing the conversion of projects and libraries of Version 1.x.x. The ensuing chapters present the innovations to the structure of a SISTEMA 2.0 project and describe the modified tabs for projects, subsystems, blocks and elements. Anyone reading this information can load a project in SISTEMA 2.0 or issue a new project in parallel and systematically explore the described innovations. Further chapters describe the innovations in the other parts of the SISTEMA interface and finally deal with the remaining topics.

2 Conversion of projects and libraries of Version 1.x.x

The project and library files of Versions 1.x.x and 2.x.x are fundamentally different, so projects and libraries first have to be converted from the old to the new format. After this, files in Format 2.x.x can no longer be opened with the older SISTEMA Versions 1.x.x. After conversion, the old files still exist. The procedure is however different:

- When **project files** are opened in the old format, SISTEMA 2.x.x converts them straight into the new format when reading them into the main memory. A message window on the different versions appears. Note must be taken of any reference to automatically set or added data.
The converted project can now be saved in a new project file in the new format. The old project file is protected from overwriting. If the project is closed without saving, no converted project file is created.
- When **library files** in the old format are opened, a query window on conversion appears. SISTEMA 2.x.x then converts this library straight into the new format when reading it into the main memory and additionally saves the converted library **automatically under the original**

¹ VDMA: German Mechanical Engineering Industry Association (www.vdma.org)

name. The original file is saved as a backup file in the old format under the name “<OldFileName>_Backup.slb”. Another message window appears for this.

In rare cases when projects and libraries are converted, some text fields have to be capped (see Chapter 3). These cappings are recorded and message windows to this effect appear. These text fields can then be adapted in the original file and converted again. Write-protected libraries cannot be converted.

3 Modification of the data structure, tables and data fields

For the already outlined reasons for developing SISTEMA 2.0, there has been a large increase in the number of data fields. In addition, in Version 1.1.9 there was already a change in character representation to Unicode. Characters are now represented not by one byte, but by four. This means that SISTEMA is also accessible to languages with an extended character set. In SISTEMA 2.0, a Japanese version is included.

The XML data structure of the project file has been simplified. The data are listed in a small number of XML tables. Projects can thus be read and written faster.

The SQL data structure of the SISTEMA library, on the other hand, has been extended by several tables in order to store the many additional data fields. The SQL tables of the SISTEMA libraries are technically limited to 64 kB per table by the “Firebird” licence-free database component employed. Regrettably, a number of documentation/text fields therefore had to be shortened in the format of the projects and libraries. This is reported during conversion.

4 Update of “Firebird” database component to Version 2.5

Due to the change to Unicode character representation, it was necessary to also update the “Firebird” database component from the existing Version 1.5 to Version 2.5. When SISTEMA is used with local libraries, this update has no effect. However, if libraries are read via a data server, the data server has to be updated. All these innovations are described in detail in the Version 2.0 of the SISTEMA Cookbook 2.

5 Project

The new functions and data fields for the project are described in the following:

Documentation tab: The new data fields are:

- Creation date: SISTEMA enters the original date of project creation here.
- Project status: In the selection list, a term for the state of project handling can be selected or a user’s own term can be entered.
- Project number: A number can be entered for project identification.
- Project version: A version number can be entered for project status.
- Authors: New term for the old “Author” field. Several names can be entered.
- Project managers: The names of several managing persons can be entered.
- Inspectors: The names of several inspecting persons can be entered.

“Safety function” tab: There are no new data fields or functions. The sorting of the list can be changed by clicking on the column headers “Name”, “Type” etc.

6 Safety function

The new functions and data fields for the safety function are described in the following:

“Documentation” tab: In the selection list for the data field “Type of safety function”, further types have been added. Also included is a separate safety function for “Power failure”. The new data fields are:

- Reaction and behaviour in the event of a power failure: New term for the old “Reaction” field. The behaviour in the event of a power failure is also to be described here.
- Operating mode: The operating mode(s) in which the safety function is active is/are to be presented here (see SISTEMA Cookbook 6 [4]).
- Demand rate: The rate at which the safety function is demanded is to be entered here [4].
- Running-on time: The running-on time in which the hazard is switched off is to be entered here [4].
- Priority: Sometimes one safety function has priority over another safety function [4]. The priority can be entered here.

“PL_r” tab: In the option “Determine PL_r value from risk graph”, the data fields “Documentation” and “Document” have been added in order to document the risk assessment and the selected risk parameters.

It is now possible to enter the probability of occurrence of the hazardous event (see Chapter 10 in [2]). To this end, the display of this option has to be activated in the menu “Edit -> Options -> Expert settings”. In this tab, the probability of occurrence can then be given with the option fields “unknown”, “low” or “high”. In the data fields “Documentation” and “Document”, the reasons must be stated. A low probability of occurrence causes the PL_r determined in the risk graph to be reduced by a step. This is indicated in the message window with a yellow warning message. If the probability of occurrence is set to “low” or “high”, these data fields are always indicated regardless of the options setting.

“PL” tab: There are no new data fields or functions.

“Subsystems” tab: There is an additional button “VDMA library” with which the new window for VDMA libraries is opened in order to select a subsystem. Here, too, the list sorting can be changed by clicking on the column headers “Name”, “PFH_D” etc. There are additional columns for the new input fields “Reference designator” and “Use case” (see Chapter 7).

7 Subsystems

The new functions and data fields for subsystems are described in the following:

“Documentation” tab: The new data fields are:

- Reference designator: The subsystem’s reference designator can be entered here.
- Inventory number: A subsystem’s internal inventory/type number or the like can be entered here.

Among them are new data fields for details of devices:

- Device manufacturer: Manufacturer of subsystem/device/component.
- Device identifier: Unique identifier of the subsystem/device/component, awarded by the manufacturer.
- Device group: Category/identifier of the subsystem/device/component, awarded by the manufacturer, e.g. sensor, position switch, safety PLC or the like.

- Part number: Order/article/part number of the subsystem/device/component, awarded by the manufacturer.
- Revision: To distinguish between different revisions of the subsystem/device/component, awarded by the manufacturer.
- Function: Assignment of the subsystem/device/component to one or more functions, awarded by the manufacturer.
- Use case: Naming of the specific use case of the subsystem/device/component, awarded by the manufacturer. Examples: single-channel, dual-channel, with brake control, without brake control, or the like.
- Description of the use case: More detailed account of the above-mentioned use case.

The device details can be shown and hidden to the right of the heading “Device details” by clicking on the triangle. If a device/component is copied from a VDMA library, these data fields and the associated reliability parameters are write-protected.

In the menu “Edit -> Options -> View” it is possible to activate indication of the reference designator and/or inventory number and/or use case in the project tree in square brackets in front of the subsystem name. It is then possible to search and filter on the basis of these details.

“PL” tab: In the option fields there are two new methods of PL determination:

- Enter the SIL or PFH_D value directly: Values for subsystems conforming to IEC standards for functional safety (e.g. IEC 62061, IEC 61508, IEC 61496) can be entered here, see IFA information [2], Chapter 4, and ISO/TR 23849 [5]. The stating of a category has been eliminated.
- Determine the PL or PFH_D value ... (simplified method in accordance with Section 4.5.5): The new simplified method can thus be applied, see IFA information [2], Chapter 5. Tabs for the input of MTTF_D values are hidden accordingly.

For the options where the user determines a PL from parameters of the components, it must be confirmed that the basic requirements relating to the PL are observed and implemented. This is done in the list beneath the option fields by ticking the requirements (Figure 1).

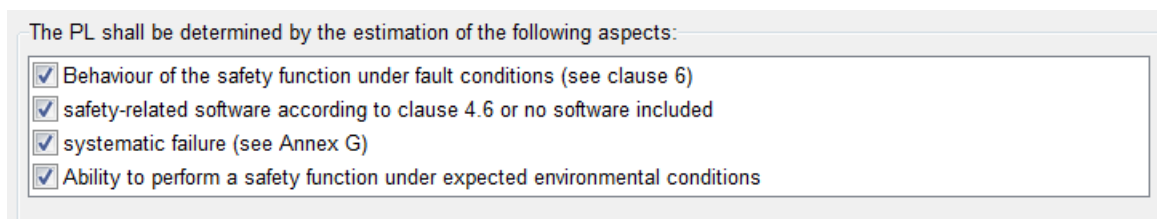


Figure 1: Requirements for determination of a PL

With the new selection list “Software suitable up to PL”, it is possible to state

- that no application software is present (default “n.a.”) or
- up to which PL an application software (e.g. a safety PLC²) is suitable (“a” to “e”). The according requirements are derived from the clause 4.6 of the standard. If this PL is lower than PL a or has not yet been assessed, “-” can be selected in the list. If this PL is lower than the values for PL (from PFH_D) achieved by the hardware assessment, the latter is downgraded to the PL, for which the software is suitable. A green information message appears to this end.

² PLC: Programmable Logic Control

“Category” tab: There is a new category option “unknown”. This is also the new default setting for newly defined subsystems. No channels are indicated yet for this category selection. A red error message draws attention to this.

A new data field is indicated for Category 2:

- Reduced test frequency (1/25): This is a new option for calculating test frequencies lower than 1/100, which increases the PFH_D by 10 % (IFA information [2], Chapter 4). A green information message appears to this effect.

Some of the category requirements have been extended, reformulated and supplemented with information texts in order to present the requirements of the standard with greater precision. The new requirements are:

- “Accordance with relevant standards to withstand the expected influences”
- All additional category requirements for the new simplified method in accordance with Section 4.5.5 of the standard. These texts start with “(4.5.5)”. Figure 2 shows an example of category 2.

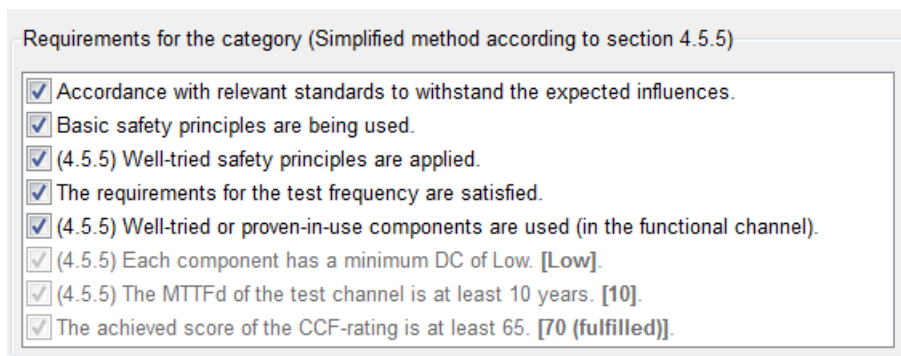


Figure 2: Example of category requirements for the simplified method in accordance with Section 4.5.5 of the standard

“MTTF_D” tab: For the option “Enter MTTF_D value directly” there is a new documentation field. To prevent a faulty input, this very rarely required option can now only be activated via the menu “Edit -> Options -> Expert settings”.

“DC_{avg}” tab: There are no new data fields or functions. To prevent a faulty input, the very rarely required option “Enter DC_{avg} value directly” can now only be activated via the menu “Edit -> Options -> Expert settings”.

“CCF” tab: For the tab there are new “Documentation” and “Document” fields that are indicated in both options of this tab. The points are now indicated in the same place for both options. The CCF measures are also switched over when the language is switched (see Chapter 12). New measures have not been added, but instead texts have been brought into line with the new version of the standard.

“Blocks” tab: There is an additional “VDMA library” button for opening the new window for VDMA library to select a block. Here, again, the sorting of the list can be changed by clicking on the column header “Name”, “DC” etc. Beyond this, there are no new data fields or functions. There are additional columns for the new input fields “Reference designator” and “Use case”.

8 Channel

There are no new data fields, but instead an additional “VDMA library” button for opening the new window for VDMA library to select a block. Here, again, the sorting of the list can be changed by clicking on the column header “Name”, “DC” etc. There are additional columns for the new input fields “Reference designator” and “Use case”.

9 Block/element

Unlike Versions 1.x.x, the data fields of blocks and elements are now identical. The same functions are available in both object types, so blocks can always be converted into elements and vice versa. This is done by drag & drop or by copy/move via the clipboard. If a block contains subordinate elements, it cannot be converted into an element. A block can still be configured as a directory for elements. The option fields of the block then have to be changed over to “Determine $MTTF_D/DC$ value from elements”. As a result, it is possible, firstly, to enter a small number of components as blocks with little effort and, secondly, to structure a very large number of components as elements in blocks. When a new block is defined, the latter – departing from the procedure of Versions 1.x.x – is generated as a component without subordinate elements.

The new functions and data fields for block and element are described together in the following:

“Documentation” tab: The new data fields have already been described as “Device details” of the subsystems (Chapter 7). Here again, the reference designator and inventory number can be indicated in the project tree. The additional data fields are:

- Technology: The selection list is now also available for the block.
- Category: According to VDMA Standard Sheet 66413 [3], a category can now also be given for a standard component.

“ $MTTF_D$ ” tab: There is a new documentation field. The following options are available:

- Determine $MTTF_D$ value from elements: only available in the block and unchanged.
- Enter $MTTF_D$ value directly: unchanged, now also with “Typical component values” in the block.
- Determine $MTTF_D$ value from B_{10D}/B_{10} value: what is new here is that via the selection list a B_{10} value can also be entered together with the new parameter RDF [%] (Ratio of Dangerous Failures, see VDMA Standard Sheet 66413). Relationship: $B_{10D} = B_{10}/RDF$.

The n_{op} parameters are now stored in the project. If the n_{op} value is entered directly, the parameters are reset (to value 0). With the new button “Reset n_{op} ”, the parameters are also reset and the n_{op} value set to its initial value “INF” (infinite). As a result, the error message “Please enter a real positive number as the n_{op} value” appears. This is of interest for model projects and library objects as the n_{op} value has to be entered in accordance with the application. In the n_{op} editor, values previously entered – for other components – can be loaded again into the data fields with the button “Load last values”.

- Determine $MTTF_D$ value from Lambda/ $MTTF/MTBF$ and RDF value: via the selection list a Lambda, $MTTF$ or $MTBF$ value can be entered together with the new parameter RDF [%] (Ratio of Dangerous Failures, see VDMA Standard Sheet 66413). Relationships: $MTTF_D = MTTF/RDF$, $MTTF_D = MTBF/RDF$ and $MTTF_D = 1/Lambda \cdot RDF$.

The list of “Typical component values” has been modified in accordance with the changes to the standard, see IFA information [2], Chapter 11. The text describing the selected component is copied at the same time by means of a new button “OK – load selection and copy description to clipboard” so that it can then be pasted in a documentation field, for example.

“DC” tab: The following options are available:

- Determine DC value from elements: only available in the block and unchanged.
- Enter DC value directly: available unchanged.
- Select applied measures to evaluate DC: there is a new documentation field, otherwise unchanged.

In the library of DC measures, two measures have been deleted, see IFA information [2], Chapter 12. When Versions 1.x.x are converted, these measures are nevertheless retained in the project.

- Redundant shut-off path with no monitoring of the actuator (DC = 0%)
- Redundant shut-off path with monitoring of one of the actuators either by logic or by test equipment (DC = 90%).

“Elements” tab: Only available in the block. There is an additional button “VDMA library” for opening the new window for VDMA libraries in order to select an element. Here again, the sorting of the list can be changed by clicking on the column headers “Name”, “DC” etc. Beyond this, there are no new data fields or functions. There are additional columns for the new input fields “Reference designator” and “Use case”.

10 Field of application

Nothing of SISTEMA 2.0's field of application has changed. The program supports the assessment of parts of control systems as defined in EN ISO 13849-1. Nevertheless, parts of control systems with the parameters SIL/PFH_D, which are assessed in accordance with IEC standards, can be entered in SISTEMA. The standard [1] explains that subsystems of an SRP/CS can also be designed in accordance with other standards on functional safety (e.g. IEC 62061, IEC 61508, IEC 61496). After “translation” of a SIL into a PL in accordance with Table 4 of the standard, they can be integrated as a subsystem. ISO/TR 23849 [5] also explains this.

11 Terms, formula symbols and abbreviations

Some of the abbreviations used in SISTEMA have been modified in line with the changes to the standard [2] and, for instance, the index for “dangerous” changed into a capital D (PFH_D, MTTF_D, B_{10D} and T_{10D}).

12 Switching languages

The texts for CCF and DC measures are now automatically adapted to the currently selected language of SISTEMA. Self-defined requirements are not translated. This procedure can be changed via the option “Expert settings -> Use the selected language for CCF and DC measures”.

13 Report

The additional data fields and options are also presented in the report. This report can be created as an overview or as a detailed reporting with numerous new print options (Figure 3).

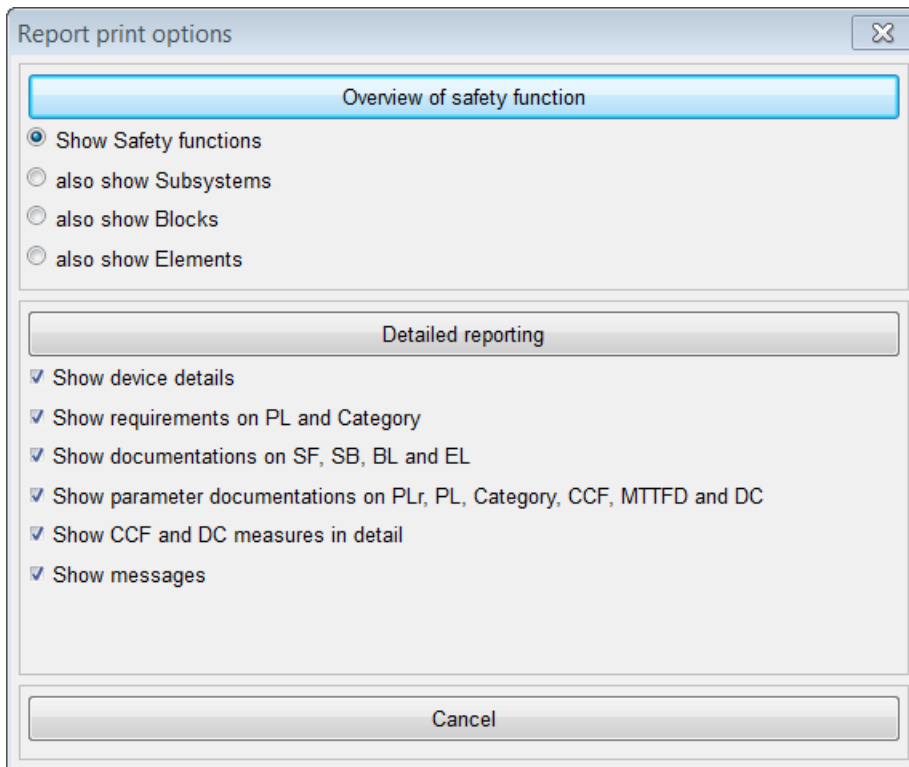


Figure 3: Report print options

14 Further changes

Limitation of $MTTF_D$ for each channel: The limitation of $MTTF_D$ for each channel to 100 years has been raised to 2500 years for Category 4 subsystems. This is now the standard setting in SISTEMA 2.0. In the menu “Edit -> Options -> Expert settings”, the capping in Category 4 can be lowered to the former value of 100 years.

Test rate in Category 2: Category 2 used to be exclusively subject to the rule of a demand rate $\leq 1/100$ of the test rate. Alternatively, testing can now take place immediately when a safety function is required if the total time for identifying the failure and restoring the machine to a safe state (the machine is usually stopped) is shorter than the time for achieving the hazard. This has been supplemented in the demands for Category 2. A reduced test rate (demand rate $\leq 1/25$ of the test rate) can be set in the subsystem in the “Category” tab (see Chapter 7).

The **validation of the project file in XML format** against a schema file is now performed directly by SISTEMA. No additional Windows DLL file (MSXML4.dll) is necessary any more.

There are **additional messages in the messages window** that report a possibly missing or incorrect data input.

In **Category 2 the output of the test channel must introduce a safe state for $PL_r d$** which is upheld until the error has been remedied. A green message to this effect appears.

15 Changes in the window for SISTEMA libraries

Compared to Version 1.1.9, there have been no changes to the user interface for libraries over and above the technical changes in the data structure and harmonised formula symbols. The tabs in this

user interface are the same as the tabs for project processing and, as described in the chapters above, have also been extended.

Compared to the earlier SISTEMA versions (before 1.1.9), the selection of object types has been changed. The subsystem, block and element object types can now be indicated via separate buttons. In the buttons, the number of the objects contained in the library is presented in brackets (Figure 3). The new “Filter” and “Search” functions can be used on the list of objects.

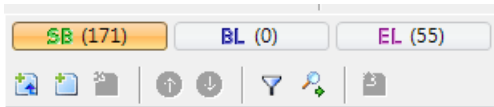


Figure 4: Selection of object types in the window for SISTEMA libraries

The list of libraries has been restructured and the applicable functions in this list have been added to. A library’s information field can now only be displayed as a separate window by means of a command. All these innovations are described in the SISTEMA Cookbook 5 (Version 2) at length.

16 New window for VDMA libraries

To read in parameter libraries in the format of VDMA Standard Sheet 66413 [3], a new import interface and an additional user interface have been realised as dedicated windows. The main functions are described briefly in the following. All these innovations are presented in detail in the SISTEMA Cookbook 5 (Version 2). Detailed information on VDMA Standard Sheet 66413 is available at the VDMA [3].

The new window is opened with the command “VDMA library”. Parameter libraries are opened locally or directly – without a data server – via the network and are presented in the left navigation window, sorted according to manufacturer (Figure 4). This list of libraries is stored and the indicated libraries can be re-loaded with a mouse-click. Each library (symbol “LB”) contains devices (symbol “De”) of just one manufacturer. Each device can be entered with one or more use cases. A use case is the lowest object in this hierarchy. The symbol in front of a use case is a combination of the four device types (numbers 1 to 4 as per Standard Sheet) and the SISTEMA symbols for subsystem (green SB), block (blue B) and element (violet E). The last-named SISTEMA symbols indicate how the use case can be inserted in SISTEMA.

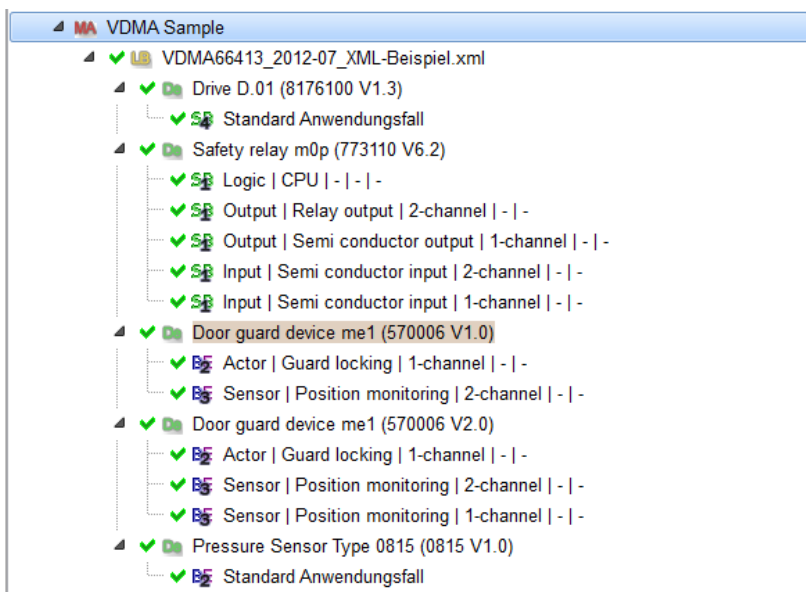


Figure 5: Indication of a parameter library in the format of VDMA Standard Sheet 66413

Each use case contains precisely one set of parameters and documentation fields (as described above in some cases for subsystems, blocks and elements). Use cases for devices can be copied to the right place for the use case by drag & drop or with the actions “SISTEMA - Project” or “SISTEMA - Library” in SISTEMA projects or SISTEMA libraries.

Parameter libraries in the format of VDMA Standard Sheet 66413 can only be read by SISTEMA. An editor for producing such parameter libraries is not envisaged in SISTEMA nor explicitly desired by the Work Group for VDMA Standard Sheet 66413.

17 Conclusion

In its Version 2, SISTEMA has been improved on the basis of user requests and brought into line with the new possibilities created by the 3rd edition of EN ISO 13849-1. In addition, a new import interface and an additional user interface for reading in parameter libraries in the format of VDMA Standard Sheet 66413 [3] have been implemented.

Other IFA application aids relating to EN ISO 13849 are being gradually brought into line with the new version of the standard and made available at <http://www.dguv.de/ifa/13849e>. The PLC Disc [6] is already available in a revised version. Reports 2/2008e and 7/2013e are being brought into line with the new version of the standard and their sample circuitries are calculated with SISTEMA 2.0 [7].

18 Literature

- [1] EN ISO 13849-1: Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design (12.2015)
- [2] Hauke, M.; Apfeld, R.; Bömer, T.; Huelke, M.; Rempel, P.; Ostermann, B.: Amendment of EN ISO 13849-1, A survey of the essential improvements in 2015. Ed.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2015
http://www.dguv.de/medien/ifa/en/prae/en13849/amendment_1_of_13849-1.pdf
- [3] Functional Safety – Universal data format for safety-related values of components or parts of control systems. VDMA Standard Sheet 66413. Ed.: Verband Deutscher Maschinen- und Anlagenbau, Frankfurt am Main
<http://ea.vdma.org/en/article/-/articleview/949939>
- [4] Apfeld, R.; Hauke, M.; Otto, S.: The SISTEMA Cookbook 6: Definitions of safety functions: What is important? Version 1.1 (EN). Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2015 <http://www.dguv.de/webcode/e109249>
- [5] ISO/TR 23849: Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery (04.2010)
- [6] Schaefer, M.; Hauke, M.: Performance Level Calculator – PLC. 5th edition. Hrsg.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2015
<http://www.dguv.de/webcode/e20892>
- [7] Practical solutions on „Safety of machine controls to EN ISO 13849“
<http://www.dguv.de/ifa/13849e>

Authors: Michael Huelke, Andy Lungfiel, Michael Hauke
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA),
Sankt Augustin