SISTEMA 3.0

Overview of the main innovations

This information is intended to support users in their first steps with SISTEMA 3.0 when converting projects or creating new projects and will help them to explore the new features described in a systematic way.

Table of contents

1   Introduction

The main innovations in SISTEMA 3.0 have been undertaken for the following reasons:

- Changes to the 4th edition of the standard EN ISO 13849-1:2023 [1], described in the IFA information [2]. SISTEMA 2.x relates to the 3rd edition of the standard (EN ISO 13849-1:2015).

- Update of the Firebird version used by SISTEMA (from Firebird version 2.5 to 5.0)

- Suggestions for improvement that have been received in the meantime (e.g. the option of downgrading "yellow" messages to "green" (see 5.1))

In principle, the calculation method according to the simplified procedure for estimating the performance level for subsystems (bar chart) is not affected by the revision of standard EN ISO 13849. The adaptations of the standard [1] are implemented by SISTEMA through additional verifications, so that new messages may be generated for SISTEMA 2.x projects after opening in SISTEMA 3.x. We recommend that you check these messages carefully and compare them with the changes to standard [1]. The Common Cause Failure (CCF) and, in particular, the Diagnostic Coverage (DC) measures have been described more precisely. Please check your data to ensure that the measures you have been using are still applicable and evaluated correctly.

SISTEMA 2.x projects are compatible and can be opened with SISTEMA version 3.x. The SISTEMA 3.x file format is adapted during this process and is not backwards compatible. Should you have any questions, please contact our support team at SISTEMA@dguv.de.

Chapter 2 begins with a detailed description of the conversion of Version 2.x projects and libraries. The following chapters, 3 and 4, explain the new data fields and the changes resulting from the 4th revision of EN ISO 13849-1. Finally, new features, for example those based on suggestions for improvement, and other topics will be presented.

2   Conversion of projects and libraries of version 2.x

The project and library files of SISTEMA Version 1.x are no longer supported and need to be converted to a SISTEMA Version 2.x format (using a SISTEMA Version 2.x). The project and library files of Versions 2.x and 3.x are fundamentally different and will be converted automatically when opened. The old files will always be kept. The behavior is as follows:

- When **project files** in the old format are opened, SISTEMA 3.x will convert them while importing. During this process, a message box appears with information on the differences between the versions. The notes on any automatically set or added data should be observed.

  The converted project should now be saved. SISTEMA does not allow the old project file to be overwritten; a new project file name must be specified.

- Opening a library file created with version 2.x is followed by a dialogue asking whether the file should be converted using the 'SISTEMA Library Version Converter' tool. After you have confirmed the question, the conversion tool opens. Your library file is automatically added at the top list of the tool. Please check the destination directory. By clicking the 'Start conversion' button, you can start the conversion process. You can use the 📊&🖥 buttons to add the converted file to your SISTEMA library and to close the tool.

  - **Protected libraries will not be converted**; an error message will appear if you try to do so. These files can only be converted from a non-protected version.

  - The source file remains untouched by the conversion tool. The converted file receives an additional suffix '_SSM300'. You can customize these and other settings in the tool settings. For more details on the tool, see the following chapter 2.1.

2.1   "SISTEMA Library Version Converter" in detail

SISTEMA 3.x libraries are using Firebird 5, whereas SISTEMA 2.x libraries are using Firebird 2.5. These Firebird versions are not compatible, and a conversion is required.

In the SISTEMA library manager (tab 'Edit') you will find the tool "SISTEMA Library Version Converter" (Figure 1). It opens automatically if you try to open an older SISTEMA library with SISTEMA 3.x. The tool needs to be used to convert SISTEMA 2.x libraries.

In addition, the tool can be found in the SISTEMA program directory in the subfolder `SLBConvertingTool` (`SLBConvertingTool.exe`) in cases where a conversion needs to be performed on a different computer, for example.

It is important to make sure that the libraries to be converted and the target directory are located on the local hard drive. An error message will appear if the library files are on a network drive.

Description of the conversion process:

- You can use the button 🗄 to add as many SISTEMA databases as you like to the upper list (1).

- For the conversion, the specified target directory (2) is used.

- The conversion process is started using the 'Start Conversion' (3) button.

- All libraries that were successfully converted are added to the list below (4).

- The conversion process is logged. Messages relating to the process can be found in the lower area (5).
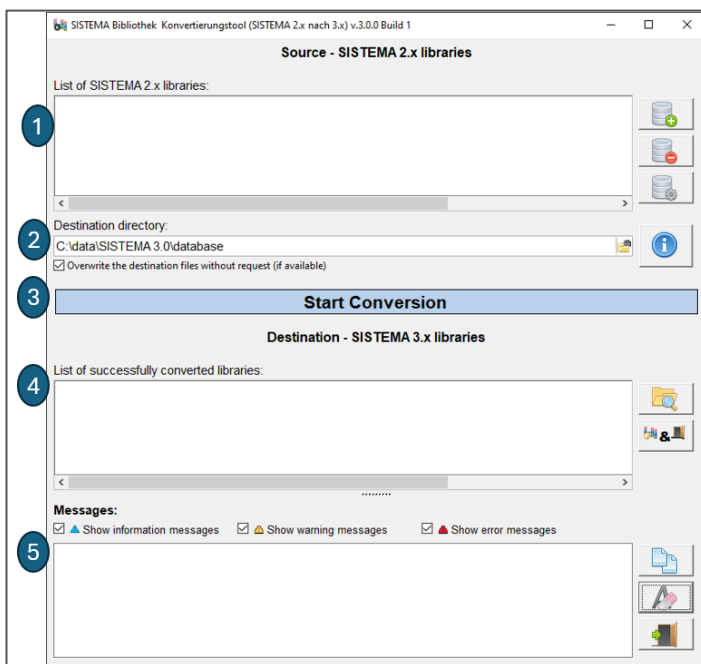

Figure 1: SISTEMA Library Version Converter

You can change the suffix used for the filename of the converted SISTEMA 3.x library in the settings. The default is `'_SSM300'`, which means that a file `'Bibliothek_v1.slb'` is given the name `'Bibliothek_v1_SSM300.slb'`.

In the settings 🗄, you can also define that the target files will be created in the directory of the source files. The default setting is that one target directory (2) is used for all source files.

2.2   Notes regarding the update of the 'Firebird' database to version 5.0

SISTEMA uses the free Firebird database to store its libraries. The Firebird version 2.5 used by SISTEMA 2.x has been discontinued. With SISTEMA 3.x and the associated changes, the software was updated to the current Firebird version 5.0.

This update has no impact on the use of local libraries in SISTEMA. Library files from SISTEMA version 2.x are automatically converted as described in Section 2. If libraries are provided via a database server, this **server must be updated to *Firebird 5.0 x86*.** In addition, only library files that have already been updated can be used in SISTEMA 3.x via a Firebird server.

The topic of *network libraries* is described in detail in *SISTEMA Cookbook 2* [6]. If you have any questions or encounter any problems, please contact us at SISTEMA@dguv.de.

3 Adjustment of the data structure, tables and data fields

Because of the further development from SISTEMA 2.x to SISTEMA 3.x, the number of data fields has increased further.

- Similar to the fourth revision of DIN EN ISO 13849-1, the German term 'Subsystem' was renamed 'Teilsystem' in SISTEMA.

- A new data field, 'Interfaces', has been added to the safety function (see Section 7.3.1 in [1]).

- In addition to the new data fields required by the standard, such as 'EMI', which are described in detail in Chapter 4, a document field has been added to the existing documentation field to allow a document to be linked.

- For the subsystem, an additional documentation and document field has been added specifically for entering a performance level in relation to qualitative aspects (e.g. software / SRASW).

If you are a developer and need more details about the changes to the data structure, please feel free to contact us at SISTEMA@dguv.de.

4 Amendments resulting from the 4th revision of EN ISO 13849-1 (December 2023)

4.1 PFH$_D$ now PFH (as of SISTEMA 2.1.x)

The previous definition of the PFH as 'probability of a dangerous failure per hour' was changed to the 'average frequency of a dangerous failure per hour' (see 3.1.5.8 in [1]). In this context, the index 'D' for dangerous was removed in order to achieve an alignment with IEC standards for functional safety.

4.2 Limitation of the formula for MTTF$_D$ calculation via the B$_{10D}$

The value for T$_{10D}$ may only be a maximum of twice as large as T$_{10}$ (see C.4.2 [1]). This restriction applies to the blocks and elements of SISTEMA.

4.3 Additional information regarding normative references

SISTEMA now provides important information from the standard, such as 'Complex components... shall not be considered as equivalent to well-tried', in the form of a tooltip that appears when the cursor is hovered over an entry (Figure 2). In addition, many existing messages have been revised and supplemented with references to the sections in which the normative background can be found (Figure 3).
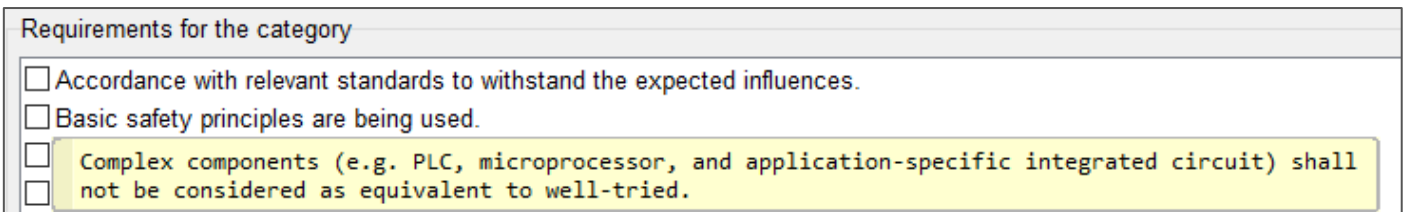

Figure 2: Additional information using pop-ups
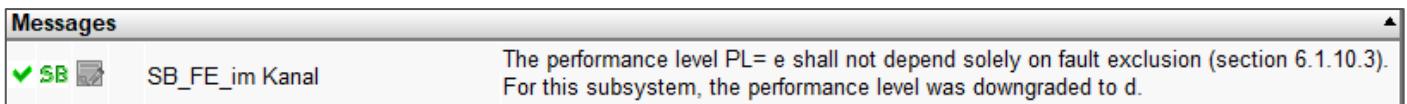
Figure 3: SISTEMA message with reference to section in the standard

4.4 Descriptions regarding PL / Category requirements and CCF / DC measures revised

The descriptions of the PL and Category requirements and of the CCF and DC measures have been revised and SISTEMA has changed accordingly. In the process, they have been made much more specific and additional information has been added (see standard [1]). SISTEMA shows additional information as a tooltip /pop-up when you hover the cursor over an entry (Figure 2, Figure 5, Figure 4).

Figure 4: CCF measures with additional information

Figure 5: DC measure with additional information on the notes

4.5 SRASW and other qualitative aspects

The possibility of entering a performance level (PL) at the subsystem level that results from qualitative aspects (such as software / SRASW) now has its own fields for documentation and a document (Figure 6). The abbreviation 'n.a.' (not applicable) has been renamed to the more common spelling 'n/a' with the same meaning. The entry 'n/a' means that there are no qualitative aspects.

Figure 6: Input PL of qualitative aspects such as software

4.6 Electromagnetic immunity (EMI)

SISTEMA now implements the topic of electromagnetic immunity (EMI) from Annex J of EN ISO 13849-1 as follows:

On the level of the safety function, you can:

    a) select a route (A, B, C or D) or
    b) specify that each subsystem should select its own approach to EMI or
    c) specify that EMI is not necessary

If you have specified that a choice shall be made at the subsystem level for this safety function, you will find the same choices a) and c) there; see Figure 7.

SISTEMA offers the documentation field and an additional document for you to document possible details concerning the electromagnetic immunity and the selected route.

Figure 7: EMI input with information on the selection options

4.7 Category 2 system

According to a current requirement of the standard, each part of the functional channel (input unit, logic and output unit) shall have at least a diagnostic coverage level of "low" (DC at least 60%) (see 6.1.3.2.4 in [1]). In SISTEMA, this check is performed across all blocks of the functional channel. In order to divide the functional channel into input unit, logic and output unit when entering data in SISTEMA, three blocks can be created with this division and subordinate parts can be implemented as elements of the corresponding blocks. The elements are not checked for a minimum "low" diagnostic coverage. Note that the MTTFD and DC of the blocks should always be determined using the elements.

Furthermore, the maximum Performance Level that can be achieved for Category 2 is PL d (see 6.1.3.2.4 in [1]).

4.8 Alternative / simplified method for PL/PFH calculation without MTTF$_D$

The method previously known as the "Simplified method to Section 4.5.5" has been renamed the "Alternative method to Section 6.1.9". There are fundamental changes, and the user has to verify whether this method may continue to be used (see 6.1.9 [1]). The PL requirements descriptions in SISTEMA have been updated accordingly.

This method now differentiates between input/output parts and logic parts. A new input field is available in SISTEMA for this decision (see Figure 8), which is used to adjust the requirements for the PL and the category.

Figure 8: PL determination using the alternative method according to section 6.1.9

Note: A subsystem of a SISTEMA 2.x project that uses this method will be marked red after the update. This is due to the new PL requirement "The good engineering practice method given in C.2 cannot be applied for the components". The user must comply with this requirement.

4.9   Fault exclusion – PLe

The topic of fault exclusion was revised in the standard [1] (Section 6.1.10). Among other things, the requirement "PL e shall not be solely based on fault exclusion" was added. The emphasis here is on "solely".

Within SISTEMA, a subsystem for which a fault exclusion "FE" has been defined is consistently reduced to PL d and a corresponding "green" message is generated (see Figure 9).

Figure 9: Fault exclusion on subsystem, automatic reduction to PL d

You can remove the "link" between PL/SIL and PFH and manually set the PL to PL e if you do not want this reduction to PL d. SISTEMA will generate a "yellow" message for these cases (see Figure 10).

If a fault exclusion is made in a channel on a block or element, SISTEMA generates a yellow message, which can be documented and, if desired, downgraded to green (see Figure 11).
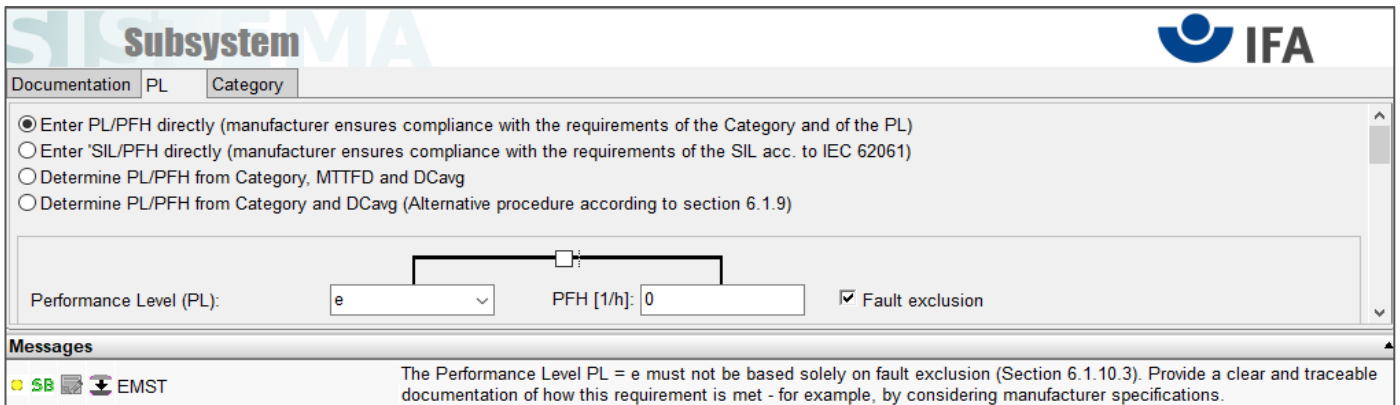
Figure 12: Fault exclusion of a channel in a multi-channel subsystem
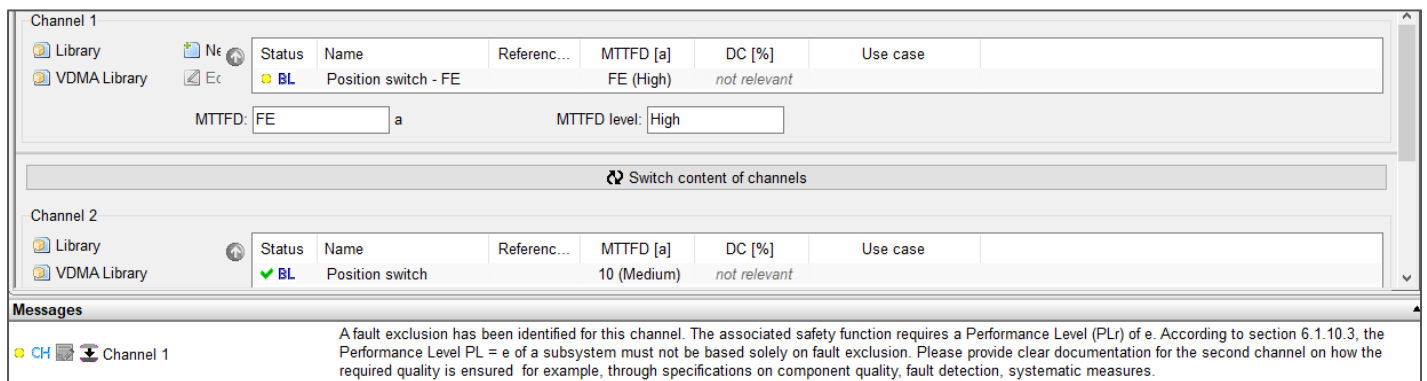
Figure 11: Error exclusion on block (or element)

If a channel consists of one or more parts with fault exclusions, the channel itself will also indicate a fault exclusion (MTTFD = FE). If PL e is attained for this subsystem (Category 3 or 4) and the associated safety function requires a PLr = e, SISTEMA generates a "yellow" message for the channel (see Figure 12). You should document clearly how the required quality is assured for the second channel – for example by means of information on the part quality, fault detection and systematic measures.
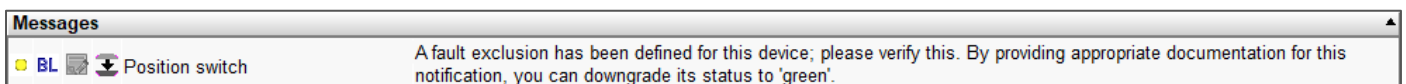
Figure 10: Fault exclusion on subsystem with PL e

5   General adjustments in SISTEMA (usability)

5.1   SISTEMA SISTEMA messages – Documentation and downgrade from yellow to green

All SISTEMA messages can optionally be documented. After documentation, only yellow messages can be downgraded to green. This new feature meets a practical need and makes it possible to achieve the green status for a project.

In the list of messages, you will find one or possibly two new symbols (⬚ and ⬚), that are grayed out as long as no information has been stored.

The symbol ⬚ is only visible for yellow messages. You can add or remove the documentation by double-clicking on the symbol or via the context menu (right-click) (see Figure 13) of the list entry. If documentation has been added, the symbol turns colored ⬚, the same applies to the downgrading to green symbol ⬚.

An overview of all documented messages can be found in the PL tab of the safety function (see Figure 14).
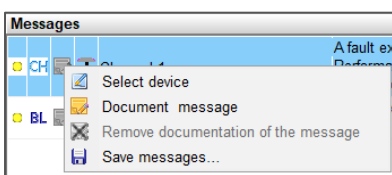

Figure 13: Context menu of a message in the list of messages

In the summary, you will find a list of all documented messages on the first few pages below the safety functions. This list is part of every summary and cannot be hidden.

Figure 14: Overview of the documented messages is available in the "PL" tab of the safety function

All yellow messages are notes from SISTEMA that you should carefully review. For example, for wear-prone components that need to be replaced during the 20-year mission time of the machine, this means that this information is important for the machine operator and should be documented in the manual. You can now document the corresponding measure and change the message to green. Please note that it is only possible to change yellow messages and only after entering documentation.

References to the standard [1] have been added to many messages. All references to sections always relate to the fourth revision of the standard [1]. SISTEMA does not replace assessment in line with the standard. SISTEMA supports use of the standard. All entries made in SISTEMA therefore assume knowledge and understanding of the standard [1].

5.2   Category requirements

SISTEMA has adjusted the texts generated for the requirements in the category. For example, the text "MTTFD is at least low or medium or high" has been shortened to "MTTFD is at least Low".

In the case that a DC-requirement is only achieved by exceeding the 5% tolerance of the standard (see Table 7 [1]), the description was adapted to make this more transparent, see Figure 15.
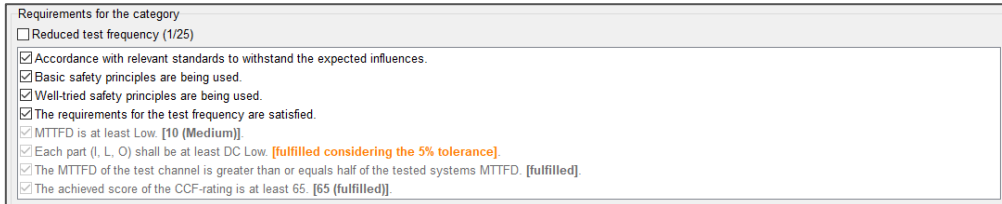

Figure 15: Note on consideration of the 5% tolerance

5.3   Show "Device identifier" in tree structure

The "Device identifier" field of a subsystem, block or element can be displayed in the tree structure through "Options / View".

5.4   Multiple start of SISTEMA possible

SISTEMA can be started multiple times, which also simplifies the use of SISTEMA on a terminal server (details can be found in SISTEMA Cookbook 3 [6]).

You can also start an older version of SISTEMA and use SISTEMA 3.x at the same time. In this case, SISTEMA 2.x has to be started first, then SISTEMA 3.x. If you have any questions, please contact us at SISTEMA@dguv.de.

5.5   Documentation easier to edit

Each documentation field has a "pencil" or a "magnifying glass" (for read-only access) in the lower right corner, which can be used to display the field in a separate window for editing if necessary (see Figure 16).
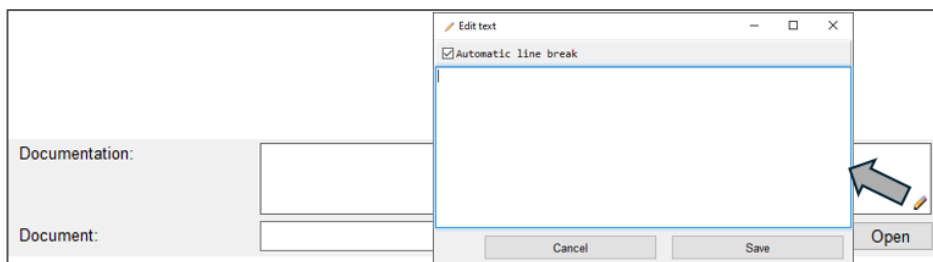

Figure 16: Edit documentation in a separate window

5.6   CCF and DC measures - Only normative measures available

SISTEMA no longer allows you to create your own measures. Instead, you can store a document here to describe individual measures in detail if required. During then import of older projects or libraries, existing custom measures will be converted (see below).

The CCF and DC measures were revised and described in more precise terms in the 4th revision. Check in detail whether your measures are still in line with the standard.

User-defined measures need to be described in the documentation fields. If a user-defined measure or, for example, a measure from EN ISO 13849-1:2006 that was removed with the next revision of the standard (e.g. "Redundant shutdown path with monitoring of one of the drive elements either by the logic or by a test device = 90%"), SISTEMA will automatically enter this in the documentation field for DC and set the DC value determination to "direct input". During the conversion of the data, a corresponding message will be generated.

5.7   Graphical representation of the PFH value achieved

On the level of the safety functions, the "PL" tab shows the achieved PL and PFH value in a graphic (see Figure 17).
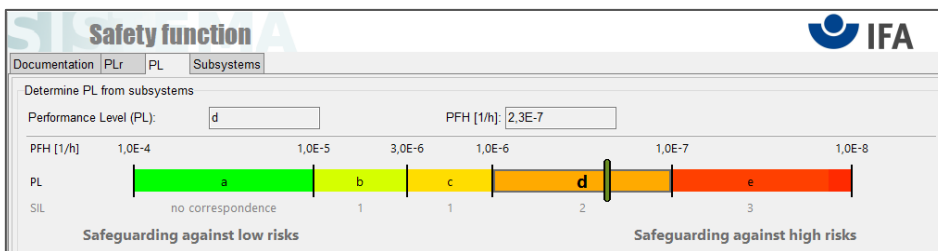

Figure 17: Graphical representation of the PL / PFH values in SISTEMA 3.x

5.8   Summary / Report

All new data fields have been added to the summary.

On the last page, you can store your own contact details. To do this, use the "Contact details" button in the print options for the summary (see Figure 18).
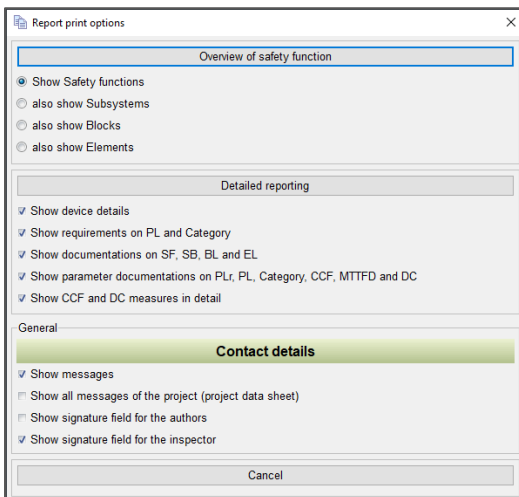

Figure 18: Print option of the summary - contact details

The contact details are used to store the address of the company or the person who is responsible for the SISTEMA project.

6   Scope

The scope of SISTEMA 3.x has remained unchanged: the program supports the evaluation of control parts according to EN ISO 13849-1. Nevertheless, control parts with the characteristic values SIL/PFH, which were evaluated according to IEC standards, can be transferred to SISTEMA. The standard [1] explains that subsystems of an SRP/CS can also be designed in accordance with other functional safety standards (e.g. IEC 62061, IEC 61508, IEC 61496).

7   Conclusion

Version 3 of SISTEMA has been improved in line with feedback from practice and adapted to the new requirements and possibilities created by the 4th edition of DIN EN ISO 13849-1.

Other IFA guidance documents on EN ISO 13849 are going to be successively adapted to the changes in the standard, too, and made available on IFA's web site: Safety of machine controls to EN ISO 13849. The PLC turntable [3] continues to be valid and the IFA-Report 02/2017 will be published in its new edition as IFA-Report 01/2025 [5], also adapted to the new version of the standard. The circuit examples described there will be published in the form calculated with SISTEMA 3.0 [4].

8   Bibliography

[1]   ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (04.23).

[2]   Hauke, M.; Bömer, T., Büllesbach, K.H.: Fourth edition of EN ISO 13849-1. Most important new features in 2023 at a glance. Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), ed.: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV) 2023 https://publikationen.dguv.de, Webcode p022540

[3]   Schaefer, M.; Hauke, M.: Performance Level Calculator - PLC. 5th edition. Edited by: Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), Sankt Augustin 2015 https://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/performance-level-calculator/index.jsp

[4]   Practical aids for "Safety of machine control systems to EN ISO 13849" http://www.dguv.de/webcode/e89507

[5]   IFA-Report 02/2017 and successor IFA-Report 01/2015 http://www.dguv.de/webcode/e89507

[6]   SISTEMA Cookbooks http://www.dguv.de/webcode/e109249

Authors: Andy Lungfiel, Michael Hauke, Paul Rempel
Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA),
Sankt Augustin