

SISTEMA – the software utility for evaluation of safety-related parts of control systems

What is SISTEMA capable of?

The SISTEMA software utility (Safety Integrity Software Tool for the Evaluation of Machine Applications) provides developers and testers of safety-related machine controls with comprehensive support in the evaluation of safety in the context of EN ISO 13849-1. The tool, which runs on Windows, enables users to model the structure of the safety-related parts of control systems (SRP/CS) based upon the "designated architectures", and ultimately permits automated calculation of the reliability values at various levels of detail, including that of the attained Performance Level (PL).

Relevant parameters such as the risk parameters for determining the required performance level (PL_r), the category of the SRP/CS, measures against common-cause failures (CCF) on multi-channel systems, the average component quality ($MTTF_d$) and the average test quality (DC_{avg}) of components and blocks, are entered step by step in input dialogs. Once the required data have been entered into SISTEMA, the results are calculated and displayed instantly. A practical advantage for the user is that each parameter change is reflected immediately on the user interface with its impact upon the entire system. Users are spared time-consuming consultation of tables and calculation of formulae (calculation of the $MTTF_d$ by means of the "parts count" method, symmetrization of the $MTTF_d$ for each channel, estimation of the DC_{avg} , calculation of the PFH and PL , etc.), since these tasks are performed by the software. This enables the user to vary parameter values and to assess the effects of changes with little effort. The final results can be printed out in a summary document.

How is SISTEMA used?

SISTEMA processes basic elements from a total of six hierarchy levels:

The project (PR), the safety function (SF), the subsystem (SB), the channel (CH)/test channel (TE), the block (BL) and the element (EL). The relationship between them is shown briefly in Figure 1.

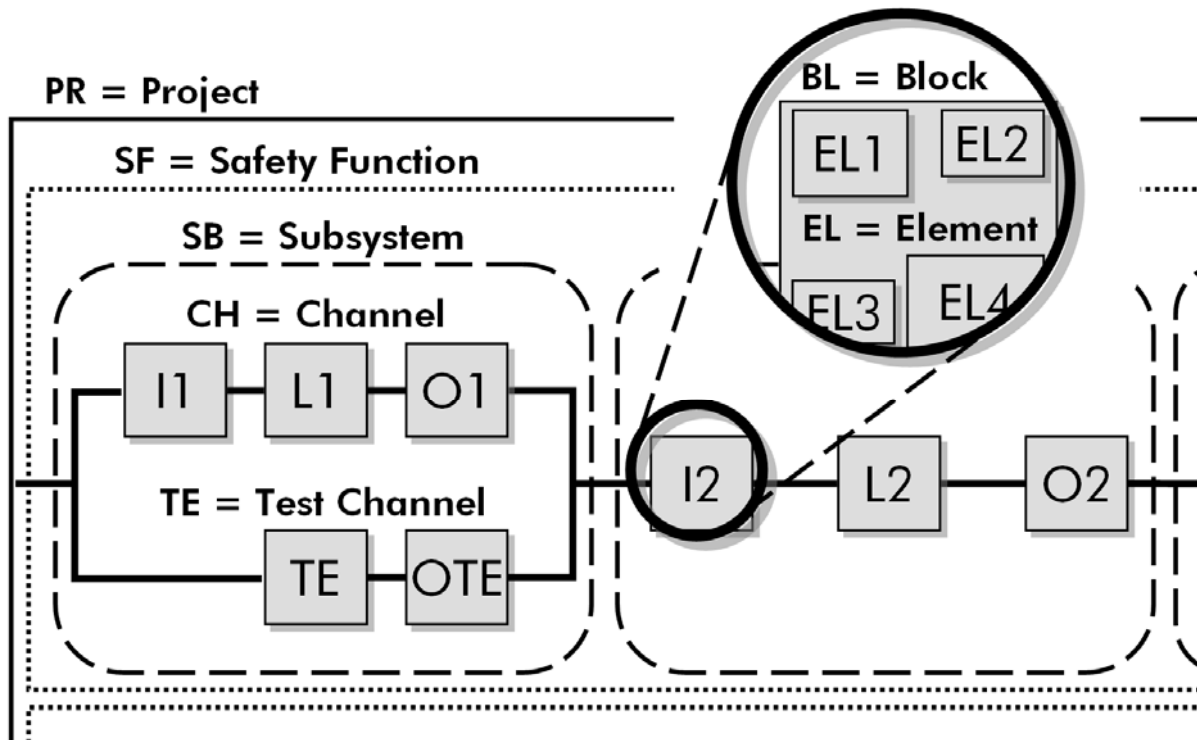


Figure 1: Hierarchy levels considered in SISTEMA

The user first opens a project, after which he can define the machine/dangerous point which is to be analysed. Finally, all required safety functions are assigned to the project. The safety functions can be defined and documented by the user, and a PL_r assigned to them. The PL actually attained by the parameterized SRP/CS is determined automatically from the subsystems which – in a series arrangement – execute the safety function. Each subsystem is based upon a designated architecture from the standard, as a function of the selected Category. The architecture determines, among other things, whether the control system is of single-channel, single-channel-tested or redundant design, and whether a special test channel must be considered during evaluation. Each channel can in turn be subdivided into any desired number of blocks, for which the user enters either an $MTTF_d$ value and a DC value directly or, on the lowest hierarchy level, the values for the individual components of which the block is composed.

User-friendly library functions complete SISTEMA's functionality. The libraries supplied contain certain standard elements; blocks and complete subsystems can however be extended as desired by the user. Where available from manufacturers for their components, additional library modules can be installed retrospectively as an option.

The SISTEMA user interface

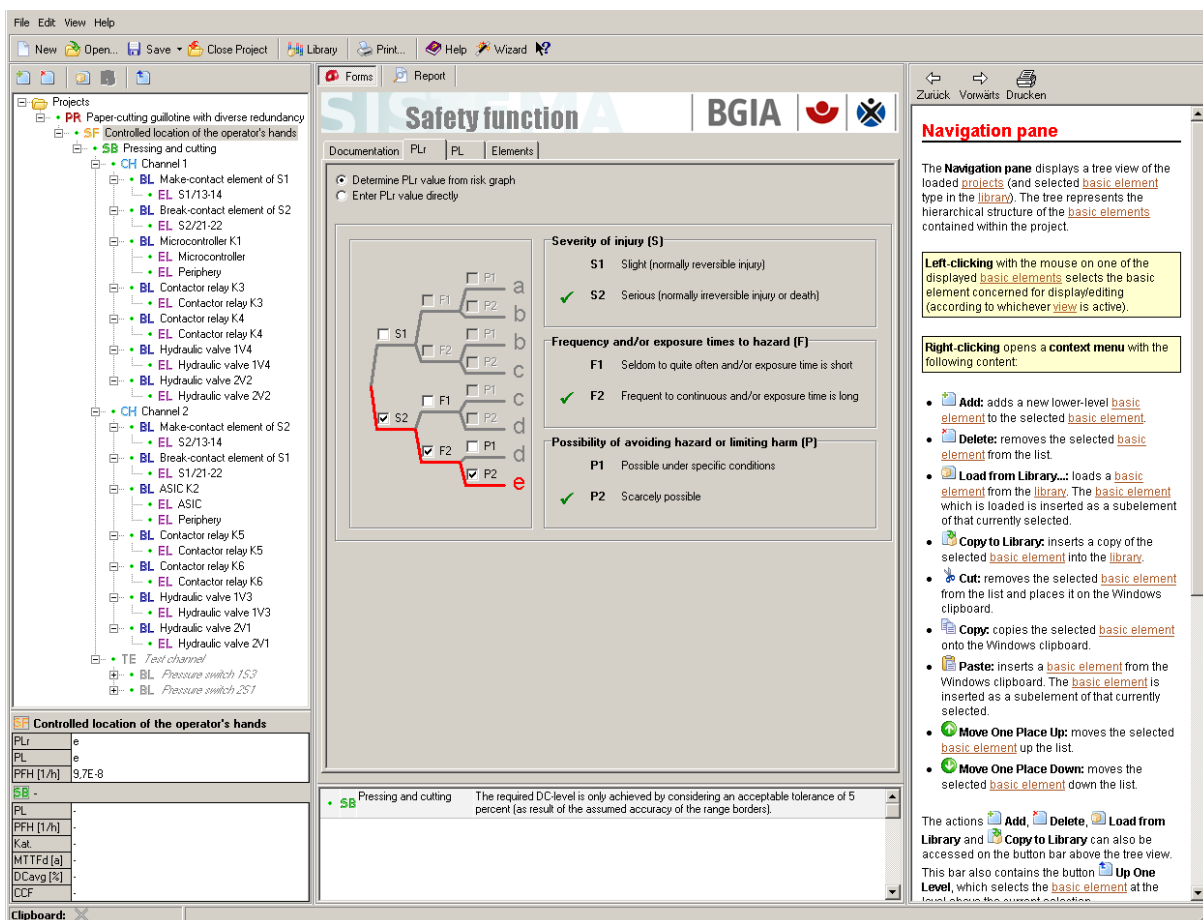


Figure 2: SISTEMA user interface

The SISTEMA user interface is divided into four areas (see Figure 2). The greater part of the interface is occupied by the workspace in the centre. Depending upon which view is active, the workspace contains an editable input dialog or a partial view of the overview document. The content of the active view is determined by the basic element selected from the hierarchy described above, and is selected from a tree view on the left-hand side. Each branch in the tree view represents one basic element. Basic elements can be created, deleted, moved or copied in the tree view. The details of the selected basic element are entered in the input dialog in the editing view. Each input dialog is further sub-divided into different areas by tabs. The final tab in each input dialog contains a table summarizing all lower-level branches and listing the main information. If, for example, the user has marked a block in the tree view, this table shows all elements contained within it, together with their $MTTF_d$ and DC values.

The tree view also shows status information for each basic element. The status information takes the form of a coloured dot adjacent to the branch. A red dot indicates that a condition of the standard is not satisfied, that a limit value is exceeded, or that a general inconsistency is present owing to which a required value cannot be

calculated. A warning is output in this case. A yellow dot indicates a non-critical message (e.g. a basic element has not yet been named). All other basic elements are marked with a green dot. The colour marking is also always inherited to the branches higher up in the hierarchy, red having the highest and green the lowest priority. All warnings and information concerning the active basic element are displayed in the message window below the workspace.

The area below the tree view shows the main context information for the selected basic element. This information comprises the PL , PFH , $MTTF_d$, DC_{avg} and CCF of the higher-level subsystem, and the PL_r , PL and PFH of the higher-level safety function (this applies, of course, only to basic elements on lower hierarchy levels). The consequences of any changes to the displayed parameters are thus displayed immediately to the user.

In addition to its flexibility, the SISTEMA user interface is notable for its ease of use and intuitiveness. Context help on the right-hand side facilitates the learning process. The wizard supplied with the application offers further help: it supports new users step by step in the virtual modelling of their control systems, and assures rapid access.

Where can SISTEMA be obtained from?

The SISTEMA software can be downloaded from the BGIA's website <http://www.dguv.de/bgja> under Webcode e34183. Following registration, the tool will be available as freeware for use and distribution free of charge. The modification of SISTEMA is not permitted. Versions in other languages than German and English are to follow. Up-to-date information and additional help for EN ISO 13849-1 can be found at <http://www.dguv.de/bgja/13849>.