SISTEMA: a Tool for the Easy Application of the Control Standard EN ISO 13849-1

Dr. Michael Huelke, BGIA – Institute for Occupational Safety and Health of the German Social Accident Insurance, Division 5: Accident prevention – Product safety
Michael Hauke, BGIA, Division 5: Accident prevention – Product safety
Jan Pilger, BGIA, Division 5: Accident prevention – Product safety

SISTEMA: ein Tool zur einfachen Anwendung der Steuerungsnorm EN ISO 13849-1

In der neuen Norm für sicherheitsbezogene Steuerungen, EN ISO 13849-1:2006, werden bewährte deterministische Merkmale der Kategorien und neue Anforderungen zur Ausfallwahrscheinlichkeit auf praktikable Weise miteinander kombiniert. Das BGIA unterstützt die Einführung und Anwendung dieser Norm durch die Entwicklung und Bereitstellung der kostenlosen Software "SISTEMA". Das Tool unterstützt Maschinenhersteller, Steuerungshersteller und Prüfstellen bei der Gestaltung, Integration und Bewertung von sicherheitsbezogenen Teilen von Maschinensteuerungen. SISTEMA nutzt dabei ein verfeinertes Verfahren zur Bestimmung von genaueren Kenngrößen der Ausfallwahrscheinlichkeit.

Funktionale Sicherheit, Steuerungssysteme, Maschinen, Software Werkzeug

1 Background

For well over a decade, safety-related parts of machine controls have been designed and assessed in accordance with the EN 954-1 safety standard. The need for greater consideration to be given to new technologies such as electronics and software necessitated a thorough revision of this standard. In the revised standard, EN ISO 13849-1:2006 [1], proven deterministic characteristics of the categories and new requirements concerning the probability of failure (service life of the parts, quality of testing) are combined in a practicable manner [2 - 4]. As early as the mid-1990s, the BGIA was successful in acquiring knowledge and experience of quantification and in applying it in the testing of safety components, for example by its involvement in the European STSARCES project (Standards for Safety Related Complex Electronic Systems) [5]. This expertise has resulted in crucial input and ground-breaking work for the simplified analysis methods employed in the revised version of the standard.

These analysis methods and the handling of reliability data are still relatively unknown in machine construction. Despite simple approaches, they remain complex in practice. Owing to its prevention mandate and with the background knowledge gained during the revision, the BGIA is therefore supporting the introduction and application of this new standard by developing tools and making them available free of charge. One such tool is the SISTEMA PC program for the safe control of

machines, which will be presented here. SISTEMA is the German acronym for "safety of controls on machines". Essentially, the purpose of SISTEMA is to enable the probability of failure of control systems, whether planned or already implemented, to be analyzed quickly and easily. Besides enhancing acceptance of the new methods, structured user guidance is to assure complete, error-free application of the EN ISO 13849-1 standard. With plausibility and consistency checks and a three-level indicator system, SISTEMA contributes to the avoidance of user errors. The tool assists machine manufacturers, control system manufacturers and test bodies in designing, integrating and assessing the safety-related parts of machine controls. It addresses all relevant control technologies. SISTEMA was funded by the German Fachausschuss “Druck und Papierverarbeitung".

The requirements for the program were defined following systematic examination of the standard in its final form, and with the incorporation of experience gained with a software prototype developed beforehand. The various methods set out in the standard were to be modelled in the software such that users need only enter their data in manageable input dialogs, and the result would be calculated continuously. A further important requirement was the separation of the user interface from the database for projects, safety functions and components. Besides robust computing functions, user-friendly functionality was implemented, such as the results prognosis and a database for standard components and control systems which have already been analyzed. The serviceability of the software is enhanced by documentation of the results in a report and by the use of a "wizard" by which users are instructed in the software's use.

SISTEMA is currently available in German and in English; further language versions are in preparation. This will enable the software to be used internationally. Testers at the BGIA trialled the program by analyzing real-case control systems. In addition, many example circuits have already been analyzed and have been published in a BGIA Report 2/2008.

2 How SISTEMA works

The SISTEMA software tool provides developers and testers of safety-related machine controls with comprehensive support in the analysis of safety in accordance with EN ISO 13849-1. The tool, which runs on Windows, enables its user to model the structure of the safety-related control components based upon the designated architectures, and ultimately permits automated analysis of the reliability values at different levels of detail, including that of the attained performance level (PL) and the average probability of a dangerous failure per hour (PFH).

Input dialogs are used for the step-by-step input of relevant parameters such as the risk parameters for definition of the required performance level (PL_r), the control system category, the measures against common-cause faults (CCF) on multi-channel systems, the average component quality (mean time to dangerous failure, $MTTF_d$) and the average test quality (average diagnostic coverage, DC_{avg}) of components/blocks. Once the necessary data have been entered into SISTEMA, the results are computed and displayed instantly. A practical advantage for the user is that the effects of each parameter change upon the system as a whole appear immediately in the user interface. Users are spared virtually all the time-consuming searching in 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.). This enables them to "experiment" with parameter values in order to assess the global effect of modifications at no great effort. The final results are summarized in an overview ready for printout.

Even with analysis by means of a tool such as SISTEMA, however, the user still faces certain challenges which can be overcome only with practice and experience. Before SISTEMA can be used, the safety functions must first be specified and the actual structure of a safety-related control system must be modelled. This model is described as a safety-related block diagram. In practice, the actual structures cannot always be modelled by the architectures employed in the standards. Following modelling, a second challenge is that of obtaining all the necessary data relating to the probability of failure of parts. A reasonable diagnostic coverage (DC) of discrete measures must also be estimated properly, particularly with wide variation in effectiveness (fault detection by the process: DC = 0–99%).

3 SISTEMA in use

SISTEMA processes basic elements from a total of six different hierarchical levels: the project (PR), the safety function (SF), the sub-system (SB), the channel (CH)/test channel (TE), the block (BL) and the element (EL). Their interrelationship between these levels is summarized below (Fig. 1).

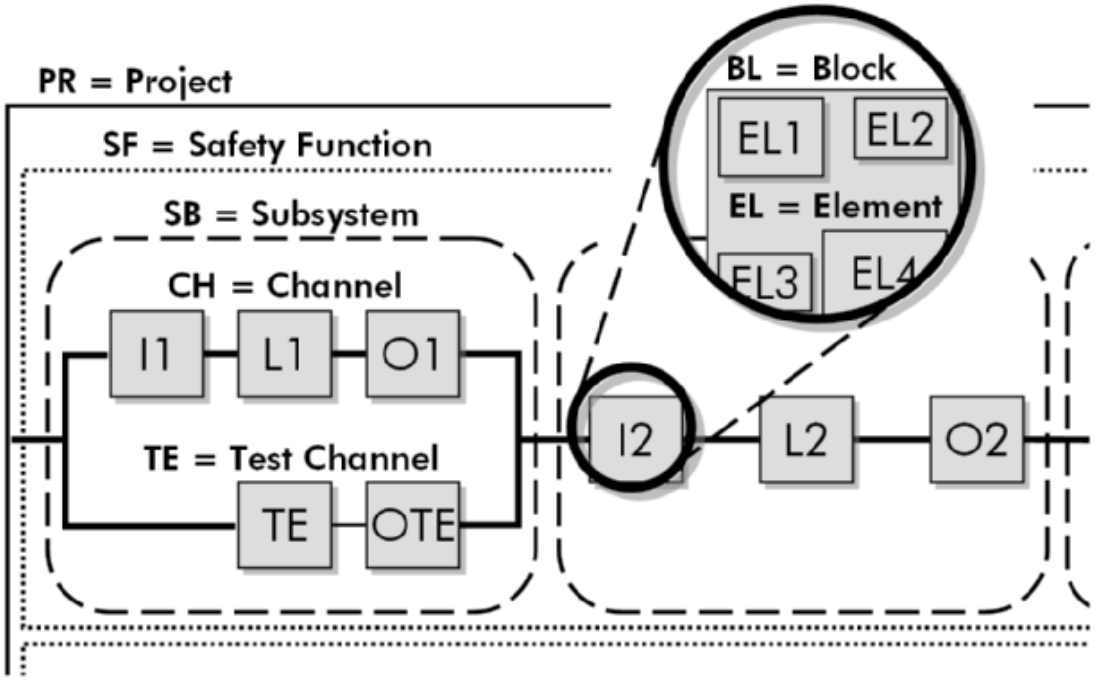

Fig. 1: The hierarchical levels considered in SISTEMA

The user first opens a project, in which he is able to define the machine or hazard point which is to be considered in greater detail. All necessary safety functions are then assigned to the project. These can be defined and documented by the user, and a PL_r assigned to them. The performance level (PL) of the parameterized SRP/CS (safety-related part of the control system) which is actually attained is determined automatically from the sub-systems which, connected in series, execute the safety function. The sub-systems are in turn based upon a "designated architecture" from the standard, as a function of the selected category. Among other things, the architecture determines whether the control system is of single-channel, single-channel tested or redundant design, and whether a special test channel must be

considered during analysis. Each channel can in turn be divided 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 hierarchical level, the values for the individual components from which the block is compiled.

4 The SISTEMA user interface

The user interface of SISTEMA is divided into four areas (Fig. 2). The greater part of the area is occupied by the workspace on the right-hand side. Depending upon which view is active, the workspace contains an editable input dialog, or a partial view of the overview document.

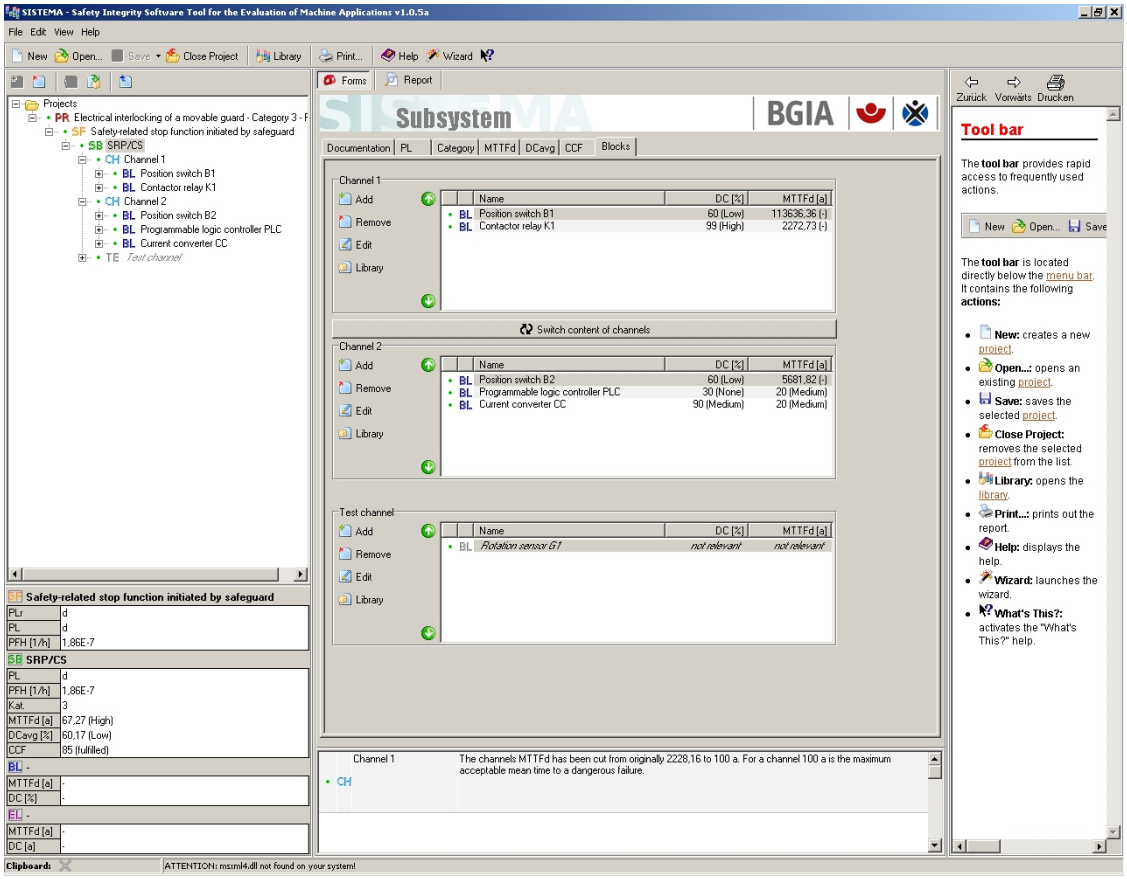

Fig. 2: The SISTEMA user interface

The content of the active view is determined by the basic element selected from the hierarchy described above (Fig. 1), 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 sub-divided further 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. Yellow indicates a non-critical message (e.g. a basic element has not yet been named). All other basic elements are marked green. 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 sub-system, and the PL_r, PL and PFH of the higher-level safety function (this applies, of course, only to basic elements which are on lower hierarchical levels). The consequences of changes in the displayed parameters are thus displayed continually to the user.

In addition to its flexibility, the SISTEMA user interface is notable for its ease of use and intuitiveness. Context help facilitates familiarization. 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.

5 Interfaces to users' and manufacturers' databases

User-friendly library functions complete SISTEMA's range of features. The libraries supplied with the software contain a number of standard elements, blocks and complete sub-systems. They can however be extended as desired by the user, for example to form a database for parts which are frequently used. If desired, further library modules can be installed retrospectively; these include project-specific and machine-specific libraries from machine manufacturers, containing re-usable objects. SISTEMA enables the user to toggle between different libraries. The user can exchange library files with other SISTEMA users and incorporate them. Component manufacturers can also support their customers by creating write-protected libraries containing the reliability data of their products.

In addition, SISTEMA provides a number of libraries containing the technical and organizational measures necessary for analysis of a control system. These libraries primarily contain the typical and most frequently applied measures, such as those contained in EN ISO 13849-1. SISTEMA manages the following libraries for this purpose:

- The library of CCF measures: this library contains a list of measures against common-cause faults, including their point values for quantification of the CCF in accordance with Annex F of EN ISO 13849-1. This list can be extended as desired by the user.

- Library of DC measures: this library contains a list of diagnostic measures, including their DC values, in accordance with Annex E of the standard. This list can likewise be extended by the user as desired.

- Library of good engineering practice methods: this library provides $MTTF_d$ and $B10_d$ values, based upon good engineering practice, for various element types in accordance with Annex C of the standard. In this case, changes, deletions or additions to the list entries are not possible.

6 Refined analysis methods for performance levels

The DC_{avg} values obtained for a system are sometimes only slightly below one of the thresholds, i.e. "low" (60%), "medium" (90%) or "high" (99%). If the simplified quantification method from EN ISO 13849-1 is then applied, analysis must continue with the next-lower DC_{avg} level, i.e. "none", "low" or "medium", as a purely formal requirement. This procedure results in estimation of the system erring on the side of safety. Owing to the low number of levels on the DC_{avg} scale, however, a minor system modification which causes the DC_{avg} value to fall just below one of the thresholds may on occasion result in a substantially inferior analysis result for the system. This may occur even when high-quality tested components (high DC) in a channel are replaced by better components (with a higher $MTTF_d$). The minor improvement in the channel $MTTF_d$ is over-compensated for in this case by the reduction of the DC_{avg} to the next lower value for formal reasons, as a result of which the measured PFH becomes poorer (greater). This effect, which appears paradoxical, is a consequence of the coarseness of the DC_{avg} scale: in other words, it is ultimately attributable to the crudeness of Fig. 5 and Table K.1 of EN ISO 13849-1.

The described effect can be prevented or alleviated by the use of an alternative diagram employing a finer gradation of the DC_{avg} values than that shown in Fig. 5 of the standard. The superior gradation is shown at the bottom of Fig. 3. With consideration for the limited precision of DC_{avg} values, the minimum possible DC_{avg} values were also considered for all categories. SISTEMA uses this refined method to determine the PFH value, interpolating further values between the columns shown in Fig. 3 in the process. In general, this enables major downgrading of the DC_{avg} value to be avoided, and often a PFH value to be determined which is both more precise and superior.

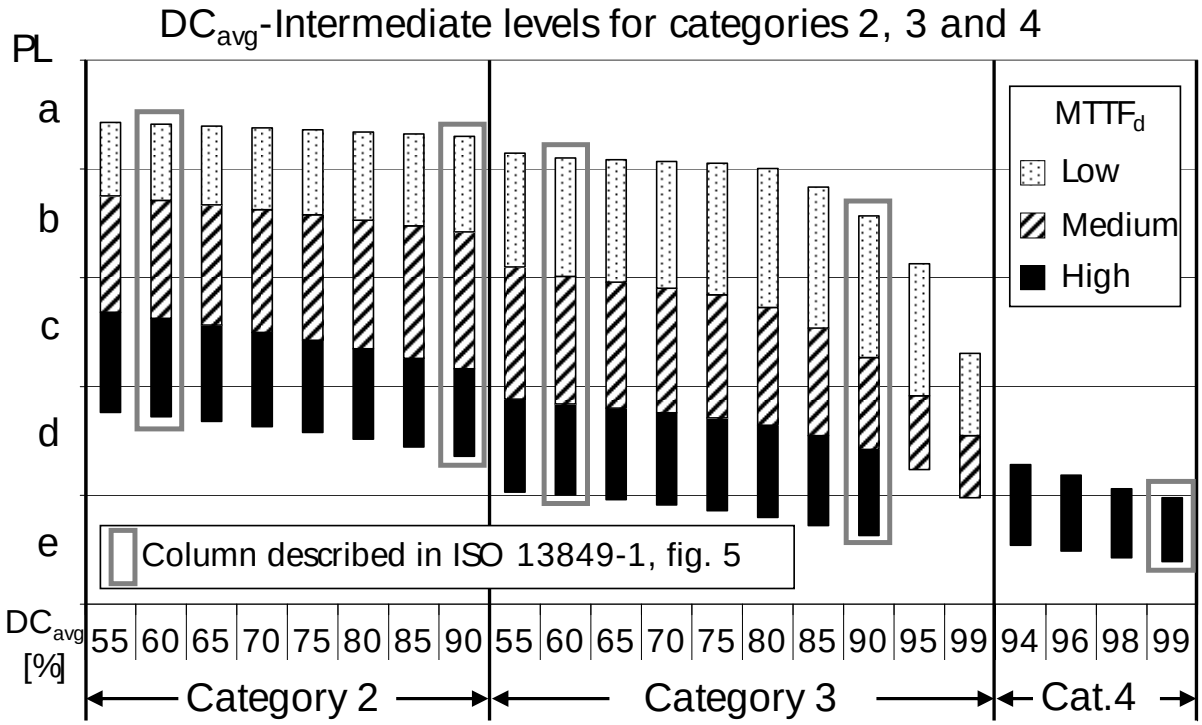

Fig. 3: Refined analysis method for the performance level

7 Conclusion and prospects

Major aims of the harmonized standard EN ISO 13849-1:2006 are ease of use, transparency and reproducibility. The standard primarily employs quantification of component reliabilities, the quality of fault detection, and also requires the inclusion of common-cause faults in the analysis. In principle, EN ISO 13849-1 represents a carefully designed superstructure, placed over the proven core of EN 954-1, which equips the revised standard for all technologies of relevance today. Existing users of the EN 954 standard can therefore quickly become familiar with the new standard. In addition, EN ISO 13849-1 requires no particular mathematical knowledge, unlike IEC 61508. It is generically suitable for mechanical, electrical, electronic, microprocessor, pneumatic and hydraulic control technologies.

The SISTEMA software tool provides developers and testers of safety-related machine controls with comprehensive support in the analysis of safety in accordance with EN ISO 13849-1. The tool, which runs on Windows, enables its user to model the structure of the safety-related control components based upon the designated architectures, and ultimately permits automated analysis of the reliability values at different levels of detail, including that of the attained performance level (PL).

The BGIA supports the introduction and use of these new methods. This support includes the provision free of charge of further tools and publications. The PLC (performance level calculator) disc is available for straightforward calculation of the PL of safety-related machine controls, at http://www.dguv.de/bgia under Webcode e20892. The methods in the standard are illustrated by two discs of card which can be rotated against each other. The disc was developed with the aid of the ZVEI (Zentralverband Elektrotechnik- und Elektronikindustrie)/Fachverband Automation and the German Engineering Federation (VDMA). Many safety engineering companies use this disc, with their own corporate design, in order to support their customers.

The BGIA Report 6/97 concerning control systems was fully revised in 2007, in order to describe the application of EN ISO 13849-1 and the new hardware and software requirements. It once again describes numerous examples of controls, which are analyzed by means of the tool SISTEMA and are available in the form of project files. This new BGIA Report 2/2008 appeared in German under the title "Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13849“, (Webcode d18471). An English version of this report is in preparation for the beginning of 2009.

SISTEMA is available in German and in English; versions for other languages are to follow. All language versions are distributed by only one setup file. The tool may be downloaded on the BGIA's website and distributed to third parties free of charge. The modification of SISTEMA is not permitted. Up-to-date information and the link for the download can be found at http://www.dguv.de/bgia under Webcode d11223 (in German) or e34183 (in English). Information on the standard and all available tools can be found at http://www.dguv.de/bgia/13849.

8 Literature

[1] EN ISO 13849-1:2006 "Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design"

[2] Plüddemann, G.; Schaefer, M.; Hauke, M.: Im Wandel – Vergleich und Verkettung unterschiedlicher Sicherheitsnormen, Elektrotechnik 89 (2007) No. 2, pp. 26-28

[3] Hauke, M.; Schaefer, M.: Sicherheitsnorm mit neuem Konzept, O + P Ölhydraulik und Pneumatik 50 (2006) No. 3, pp. 142-147

[4] Plüddemann, G.: Sicherheitsgerichtete Funktionen im Maschinenbau – Neue Norm bietet Lichtblicke, article in IEE (2005) No. 8, pp. 74-79

[5] Dorra, M.; Reinert, D.: Quantitative Analysis of Complex Electronic Systems using Fault Tree Analysis and Markov Modelling European Project STSARCES (Standards for Safety Related Complex Electronic Systems). Contract SMT 4CT97-2191, Final report of Work Package 2.1, annex 6, published by: European Commission – DG XII, Brussels 2000