International Journal of Occupational Safety and Ergonomics
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/tose20

Certification of Highly Complex Safety-Related Systems

Dietmar Reinert[a] & Michael Schaefer[a]
[a] Berufsgenossenschaftliches Institut für Arbeitssicherheit, Sankt Augustin, Germany
Published online: 08 Jan 2015.

To cite this article: Dietmar Reinert & Michael Schaefer (1999) Certification of Highly Complex Safety-Related Systems, International Journal of Occupational Safety and Ergonomics, 5:4, 537-552

To link to this article: http://dx.doi.org/10.1080/10803548.1999.11076437

INTERNATIONAL JOURNAL OF
OCCUPATIONAL SAFETY AND ERGONOMICS 1999, VOL. 5, NO. 4, 537–552

Certification of Highly Complex Safety-Related Systems

Dietmar Reinert
Michael Schaefer

Berufsgenossenschaftliches Institut für Arbeitssicherheit, Sankt Augustin, Germany

The BIA has now 15 years of experience with the certification of complex electronic systems for safety-related applications in the machinery sector. Using the example of machining centres, this presentation will show the systematic procedure for verifying and validating control systems using Application Specific Integrated Circuits (ASICs) and microcomputers for safety functions.

One section will describe the control structure of machining centres with control systems using "integrated safety." A diverse redundant architecture combined with crossmonitoring and forced dynamisation is explained. In the main section the steps of the systematic certification procedure are explained showing some results of the certification of drilling machines. Specification reviews, design reviews with test case specification, statistical analysis, and walk-throughs are the analytical measures in the testing process. Systematic tests based on the test case specification, Electro Magnetic Interference (EMI) and environmental testing, and site acceptance tests on the machines are the testing measures for validation.

A complex software driven system is always undergoing modification. Most of the changes are not safety-relevant but this has to be proven. A systematic procedure for certifying software modifications is presented in the last section of the paper.

certification complex electronic systems numerical controller power drive machining centres validation verification microcomputer metrics software

1. INTRODUCTION

Today just-in-time-manufacturing requires highly flexible machinery working in a complex network. Flexibility is guaranteed by software

Correspondence and requests for reprints should be sent to Dietmar Reinert, Berufsgenossenschaftliches Institut für Arbeitssicherheit, 53754 Sankt Augustin, Germany. E-mail: <Dietmar.Reinert@hvbg.de>.

driven manufacturing cells whose functionality can be changed easily by varying the input parameters. A new production cycle is introduced via bus systems without mechanical or electrical changes of the equipment. In consequence safety-related equipment also becomes more flexible and complex.

Whereas some standards still do not allow software driven systems for specific safety functions, things have recognizably changed for safety devices during the last 5 years:

- Light curtains, which are used for high integrity applications in machinery today, mostly use programmable electronics.
- Laser scanners or safety Programmable Logic Controllers (PLCs) are increasingly used for area guarding, safe muting, or processing of the emergency stop.

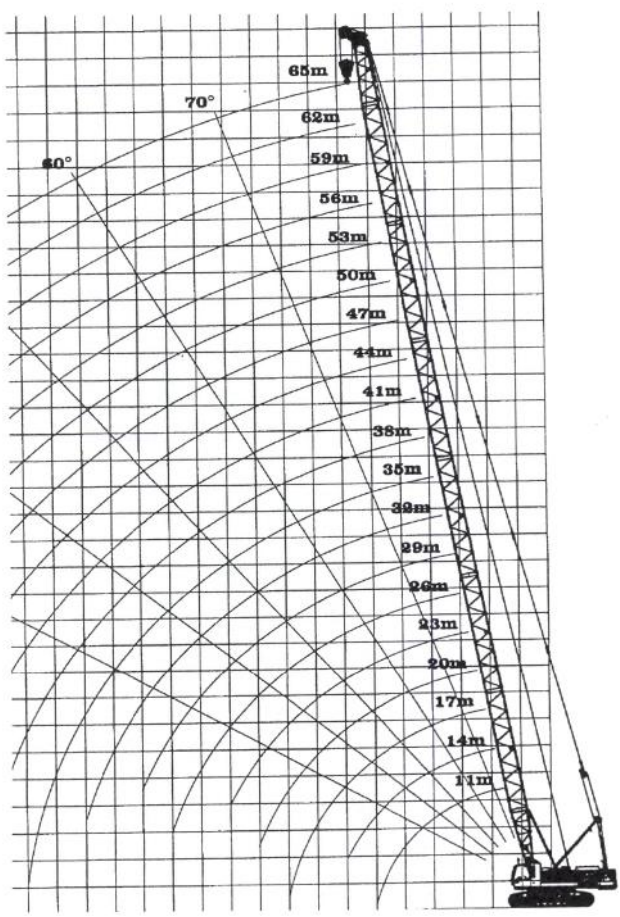


Figure 1. A 65-m high cable excavator.

Printing machines use a complex network of PLCs, which can be compared with a small chemical plant. The safety functions of reduced velocity, protection against unintended movements, or muting of fences are realized using redundant PLC architectures.

Automatically guided vehicles are used as cleaning machines in department stores. The multiprocessor control systems process safety functions for collision protection and navigation. Cable excavators use 32-bit controllers for lifting 20 tons up to 60 m (see Figure 1). The safety function of the load moment limitation is realized by a redundant processor configuration.

Robots and modern machining centres are equipped with fast numeric controllers, several processors for power drives (PD), and PLCs to fulfil their tasks. In new controls several safety functions (see Table 1) are executed using diverse redundant programmable electronic systems.

TABLE 1. Safety-Related Machine Functions for Machining Centres

Safety Function	Description
Safe stopping process	Fastest stopping process of the Power Drive (PD) under monitoring of the Numerical Control (NC).
Safe standstill	No unexpected movements are possible.
Safe operational stop	The motor is under position control of the PD. The monitoring of unexpected movements is active in PD and NC. Fastest reaction in case of unexpected restart.
Safely reduced speed	PD and NC supervise that the speed does not exceed certain risk dependent limits.
Safely limited distance	PD and NC supervise that a certain defined relative distance is not violated by one of the axes.
Safely limited absolute position	PD and NC supervise that a certain defined absolute position is not violated by one of the axes.

All these examples cannot be fully tested and the failure modes are not completely defined. For the described safety functions a standard EN 954-1:1997 (European Committee for Standardization [CEN], 1997) requirement like "If the detection of a fault is not possible, then an accumulation of faults shall not lead to a loss of the safety function" is not totally achievable.

This introduction shows that software-driven highly complex systems are becoming more and more state-of-the-art in the machinery sector. The BG Institute for Occupational Safety (Berufsgenossenschaftliches

Institut für Arbeitssicherheit [BIA], in German) has been certifying such systems for more than 15 years; during the last 8 years on the basis of the German prestandard DIN V VDE 0801:1990 (Deutsches Institut für Normung [DIN], 1990). This paper will describe the certification procedure using as an example the testing and certification of a control system of machining centres. The following section will first illustrate the safety functions for machining centres, whereas section 3 describes in eight steps the systematic approach used by the BIA.

2. SAFETY FUNCTIONS FOR MACHINING CENTRES

2.1. Machining Centres: Concept and Scope

Machining centres are used for cutting cold metal work material. A machining centre is a numerically controlled machine tool where the spindle orientation is usually either horizontal or vertical; it is capable of carrying out two or more machining processes (e.g., milling, drilling, boring), and it has facilities to enable tools to be changed automatically from a tool magazine or similar storage unit in accordance with the machining programme (Draft Standard No. prEN 12417:1997; CEN, 1997).

Machining centres are operated in different modes. One mode is the automatic production of workpieces where normally all safety guards are closed. Another mode is the setting mode of the machine where all or some protection guards are open. In this mode the user has to work close to the movements of the machine axes. For the setting mode the machine control has to prevent or to guide these motions so that they can be estimated by the worker. A ground plan of a machine tool (Figure 2) shows two safety-related areas: tool magazine and operational area. Several times a day the user has to enter the operational area. The magazine is only important for the setup.

In the last 2 years, several German manufacturers have been interested in the certification of these Control Systems. The main reason is that the state-of-the-art monitoring of dangerous machine movements does not achieve high availability and fast fault reaction (Umbreit & Zinken, 1995). The German authorities, therefore, require the restricted use of safety guards on the basis of the European Machinery Directive (Council Directive 89/392/EEC). The measures to achieve machinery safety are responsible for lower productivity. The example of an important German manufacturer of turning machines shows the extent of the problem:

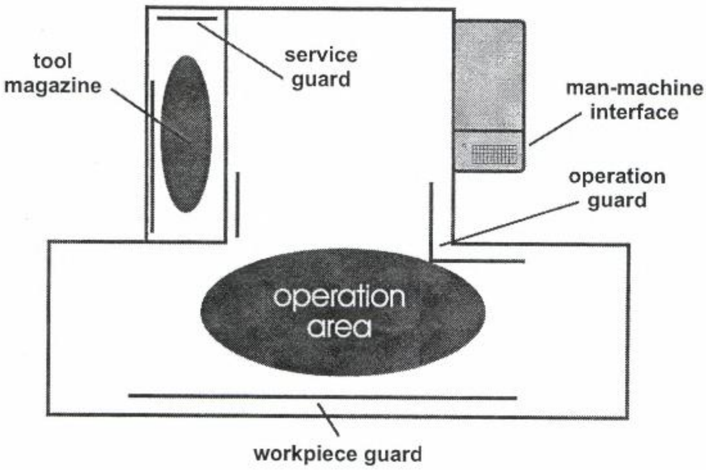


Figure 2. Ground plan of a machining centre, safety areas.

A special turning machine works with 60 tools on a revolver tool device. The tool exchange is made manually by the user. The revolver is driven by a highly dynamic Alternating Current (AC) drive. In case of a fault the revolver accelerates very fast (within some 10 ms) to an angle-velocity of 1500 rpm (rotations per minute). To change all tools the user has to open the safety guard, install a new tool, close the guard, rotate the revolver to the next tool-position, and so on, 60 times for all tools! This procedure results in a high unacceptance of safety requirements: The user will try to manipulate the guard-locking device for the sake of more ergonomic working conditions, but with risk of losing hands in case of a fault in the control system.

In a new approach safe monitoring was integrated in numerical controllers to fulfil the market requirements of flexible productivity: The user's claim is to work close to the machine motions to watch, for example, the process for a highly expensive workpiece (Reinert & Schaefer, 1998). In totally manually controlled machines (e.g., small milling machines) such observation is possible because all movements are directly controlled by the user. If the automatic motion is controlled in a safe way, the user can also move inside defined areas. All these areas in space and also in velocity space can be observed by an integrated monitoring, realised by safe software only. In a highly flexible way the machine can be adapted to the work of the user and not vice versa. The safety functions realized by the integrated monitoring are listed in Table 1.

2.2. Hazards in Machining Centres

Machining centres present a wide range of hazards, not least because of their wide application as a rotating tool and "stationary" workpiece machine tools, for the general purpose of cutting cold metal work material. Protection of operators and other persons from contact with moving cutting tools, especially when being rapidly rotated in the spindle, or being swung from a tool magazine to the spindle during power-operated tool changing, or from contact with fast-moving workpieces, is of great importance. When power-operated mechanisms are provided for workpiece transfer, they can also create hazardous situations during loading/unloading and workpiece alignment or clamping (Draft Standard No. prEN 12417:1997; CEN, 1997).

Based on the methodology and the catalogue given in standard EN 1050 (CEN, 1996), the draft standard prEN 12417:1997 (CEN, 1997) for machining centres lists 19 groups of hazards with 30 individual hazardous situations. This C standard gives a detailed description of the hazardous situations, the operating modes, and associated activities where these situations may occur and the hazardous zones related to each hazard.

In chapter 5 of draft standard prEN 12417:1997 (CEN, 1997) requirements and measures that are necessary to prevent the individual hazards are discussed. Besides, three operating modes are referred to. These are

- automatic cycle (mode 1) for the automatic production with closed guards,
- setting (mode 2) for programming the system with open guards,
- optional mode for manual intervention under restricted operating conditions (mode 3) with programme execution in real-time for test purposes with open guards.

Additionally mentioned is the movement of machine axes for emergency purposes (e.g., release of trapped persons), which could be understood as a fourth operating mode.

2.3. Safety Functions

The safety functions listed in Table 1 can be defined especially for the modes "setting" and "manual intervention under restricted operating conditions." For the different safety functions different categories according to standard EN 954-1:1997 (CEN, 1997) are required by draft standard prEN 12417:1997 (CEN, 1997; see Table 2).

TABLE 2. Safety Functions and Control Systems

Safety Function Initiated or Maintained by	Category (CAT) for Access > 1/hr	Category (CAT) for Seldom Access
Interlocking device associated with a movable guard applied to:		
work zone	3	3
transmissions, drive mechanisms	3	1
tool changer, tool magazine	3	3
work loading/unloading device	3	3
pallet changer	3	3
swarf conveyor	3	1
access to pits, gates in perimeter fencing	3	1
Hold-to run control	3	3
Enabling device	3	3
Speed limit control	3	3
Control of tool clamping	1	1
Electrosensitive protective equipment	3	3
Pressure sensitive protective devices	3	3
Emergency stop	3	3

2.4. New Architectures for Safety

Table 2 attributes category (CAT) 3 to all of the safety functions of Table 1. According to standard EN 954-1:1997 (CEN, 1997) "Safety-related parts of control systems according to category 3 shall be designed so that a single fault in any of these parts does not lead to the loss of the safety function. Whenever reasonably practicable the single fault shall be detected at or before the next demand upon the safety function." The requirement of fault tolerance towards a single failure will be achieved by the following architecture.

Figure 3 shows a typical architecture of a machine tool Control System. In these systems several computers are implemented for functional reasons. The Numerical Control (NC) is responsible for powerful calculation processes (e.g., complex interpolations in space); the digital Power Drives (PDs) have to control the motions of the axes. Numerical Control and Power Drive System form a natural diverse redundant computer-based system. Normally the process interfaces are not redundant. To achieve a totally redundant control the only hardware changes are extensions to the input and output interfaces for sensors (e.g., rotational sensors, guard switches, control switches) and actuators (e.g., guard locking, relays, and final switching devices). All safety-related functions can be implemented within these two channels by software. Figure 3 shows that the combination of NC and PDs of each machine axis forms a diverse redundant control system. The redundancy fulfils the requirement that no single fault leads to a danger.

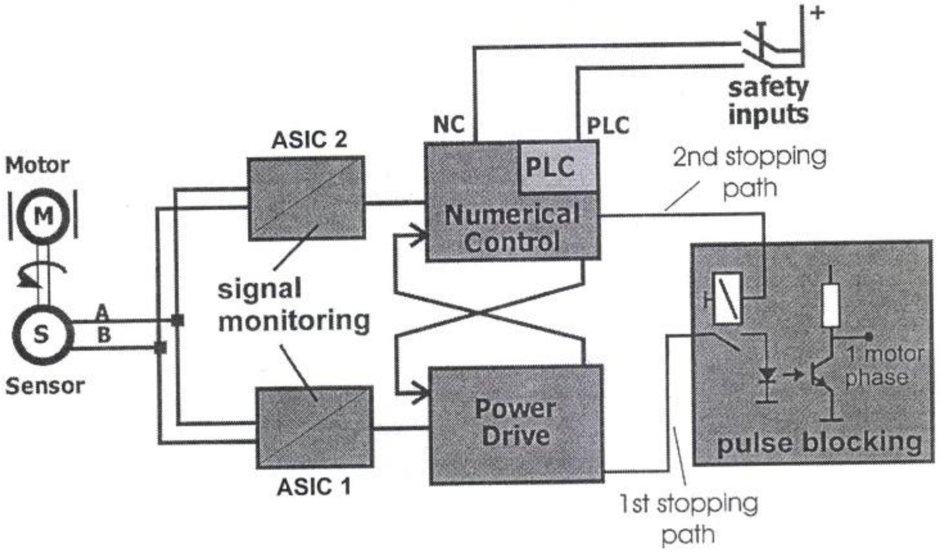


Figure 3. Architecture of a fault-tolerant Numerical Control system. *Notes.* ASIC—Application Specific Integrated Circuit, PLC—Programmable Logic Controllers.

This architecture does not fulfil the requirement of fault detection whenever reasonably practicable. This requirement was covered by cross monitoring and forced dynamisation.

PD and NC simultaneously calculate the safety-related values. All safety-related parameters of the control system have to be monitored in both channels. Cross monitoring happens not only in the NC but also in the PD. To achieve a good diagnostic coverage, cross monitoring is not only restricted to comparing output signals but it has to compare a lot of intermediate results inside the controllers. These results are, for example, position values, speed values, input and output values, safety-related machine parameters. For all these monitoring functions special tests were conducted to validate their presence and correct function. All tests are carried out manually at a real simulation station to guarantee that the conditions are close to the practice. More than 100 test cases were constructed during the careful analysis of the design documents to prove the system reaction under real-time conditions. For every test case, the system reaction was monitored and documented.

To detect failures in the signal processing of static inputs by cross monitoring, the signal must change for a test within the so-called fault recognition time. For example, the input signal of the emergency stop, which is connected to NC and PD, changes only on demand. If these two channelled input signals change at every standstill of the machine for a short time, PD and NC could monitor (cross monitoring) this test and react in case of differences. This mechanism is called "forced dynamisation."

The main important motion sensors are the rotational sensors of each axis. Normally all electronic parts of the safety related Control System have to be redundant. For high dynamic signal change it is possible to reduce the number of rotational sensors to only one. Therefore, fault-detection has to be made in a highly dynamical way by two channels, NC and PD (see Figure 3).

Figure 3 also shows an example for safe pulse blocking. The main features are the two channelled stopping paths and the stopping via switch-off of the opto-couplers, which transmit the pulses to the end stage of the PD. Both channels are able to stop the movement of the axes simultaneously.

3. SYSTEMATIC CERTIFICATION PROCEDURE

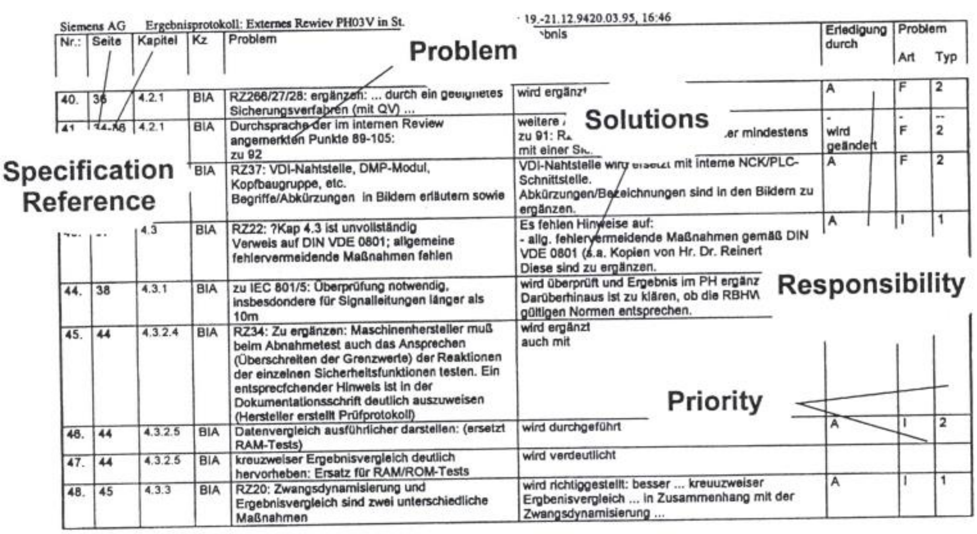
3.1. Review of the Specification

Special effort was put into the validation of the specification. Especially the following points were investigated:

- Does the requirement specification deal in a correct, clear, unequivocal, and consistent way with every safety-relevant function, which will be implemented, the external interfaces, the man-machine interface, the internal interfaces, the initialisation procedure, the reaction in case of power failure and restart, the presupposed operational conditions, the internal self-tests and reactions to detected faults, the border conditions for software due to hardware restrictions, and the software codex to be fulfilled?
- Are the documentation rules adequate for the application?

- Is the specification of a form that it can be understood by developers and programmers?
- Is there an adequate process to control changes in the specification?
- Are development tools used by the manufacturer?

These formal aspects were approved by two safety experts simultaneously. All recognised problems were discussed in about 20 review sessions with an average duration of 2 days. Figure 4 shows an example of the documentation of the review sessions. This documentation was made by the manufacturer and checked by the BIA. It was the basis for changes in the specification. The changes in the specification were checked by the BIA, too.


Siemens AG Ergebnisprotokoll: Externes Rewiev PH03V in St. · 19.-21.12.9420.03.95, 16:46

Nr.:	Seite	Kapitel	Kz	Problem	·bnis	Erledigung durch	Problem Art	Problem Typ
40.	36	4.2.1	BIA	RZ266/27/28: ergänzen: ... durch ein geeignetes Sicherungsverfahren (mit QV) ...	wird ergänzt	A	F	2
41	34-36	4.2.1	BIA	Durchsprache der im internen Review angemerkten Punkte 89-105: zu 92	weitere ... zu 91: R... ...er mindestens mit einer S...	- wird geändert	- F	-- 2
			BIA	RZ37: VDI-Nahtstelle, DMP-Modul, Kopfbaugruppe, etc. Begriffe/Abkürzungen in Bildern erläutern sowie	VDI-Nahtstelle wird ersetzt mit interne NCK/PLC-Schnittstelle. Abkürzungen/Bezeichnungen sind in den Bildern zu ergänzen.	A	F	2
		4.3	BIA	RZ22: ?Kap 4.3 ist unvollständig Verweis auf DIN VDE 0801; allgemeine fehlervermeidende Maßnahmen fehlen	Es fehlen Hinweise auf: - allg. fehlervermeidende Maßnahmen gemäß DIN VDE 0801 (s.a. Kopien von Hr. Dr. Reinert Diese sind zu ergänzen.	A	I	1
44.	38	4.3.1	BIA	zu IEC 801/5: Überprüfung notwendig, insbesdondere für Signalleitungen länger als 10m	wird überprüft und Ergebnis im PH ergänz Darüberhinaus ist zu klären, ob die RBHW gültigen Normen entsprechen.			
45.	44	4.3.2.4	BIA	RZ34: Zu ergänzen: Maschinenhersteller muß beim Abnahmetest auch das Ansprechen (Überschreiten der Grenzwerte) der Reaktionen der einzelnen Sicherheitsfunktionen testen. Ein entsprecfchender Hinweis ist in der Dokumentationsschrift deutlich auszuweisen (Hersteller erstellt Prüfprotokoll)	wird ergänzt auch mit			
46.	44	4.3.2.5	BIA	Datenvergleich ausführlicher darstellen: (ersetzt RAM-Tests)	wird durchgeführt	A	I	2
47.	44	4.3.2.5	BIA	kreuzweiser Ergebnisvergleich deutlich hervorheben: Ersatz für RAM/ROM-Tests	wird verdeutlicht			
48.	45	4.3.3	BIA	RZ20: Zwangsdynamisierung und Ergebnisvergleich sind zwei unterschiedliche Maßnahmen	wird richtiggestellt: besser ... kreuuzweiser Ergbenisvergleich ... in Zusammenhang mit der Zwangsdynamisierung ...	A	I	1

Figure 4. Documentation of reviews.

3.2. Design Review and Test Case Specification

Besides the validation of the specification, project organisation (proof of the formal mechanisms in the manufacturer's organisation), documentation (approval of design documents and manuals, reviews with machine manufacturers as users of the NC and PD), and functional tests (test of all safety-related machine functions with different combinations) were subjects of the approval.

Several reviews of the design documents led to more than 100 test cases for systematic testing and some minor changes in the design.

3.3. Statical Analysis

In several recursive steps soft- and hardware of the NC and the PD, which are both diverse redundant, were analysed by safety experts. Because of the diverse redundant architecture only minor changes were found in the hardware. The safety software of NC and PD were statically analysed by a static analyser. Both source codes have the typical extent of about 1000–2000 instructions. In Table 3, the main results of the statical analysis are represented for two versions of the PD software and one version of the NC software by listing the main metrics (Dumke, 1992). The third version of the PD software shows some dramatic changes in the average number of statements, average programme length and cyclomatic number (McCabe, 1976). These changes are the results of the first software verifications. Every weak point of the software, as pointed out by the metrics, was investigated in greater detail.

TABLE 3. Example Results of Statical Software Analyses

Iteration Step	Metric Type	Value
PD, before validation	average number of statements	225
	average programme length	1946
	cyclomatic number $v(G)$	28
	undefined jumps	0
	unconditional jumps	0
	average number of I/O points	4
PD, after first validation	average number of statements	55
	average programme length	440
	cyclomatic number $v(G)$	7
	unconditional jumps	0
	average number of I/O points	4
NC	average number of statements	33
	average programme length	174
	cyclomatic number $v(G)$	6
	undefined jumps	0
	unconditional jumps	0
	average number of I/O point	3

Notes. NC—Numerical Control, PD—Power Drive, I/O—Input/Output.

3.4. Walk-Throughs

The analyses were accompanied by several walk-through sessions of the software.

The correct and complete realisation of the requirement specifications and the software codex of the manufacturer in the software was checked during the walk-throughs. Figure 5 shows the standardized documentation of the walk-through sessions. These walk-through minutes have been drawn up by the BIA. The walk-throughs showed several failures in the PD software. The structure of this software was changed also due to the statical analysis. Today the software of PD and NC is written in a structured way.

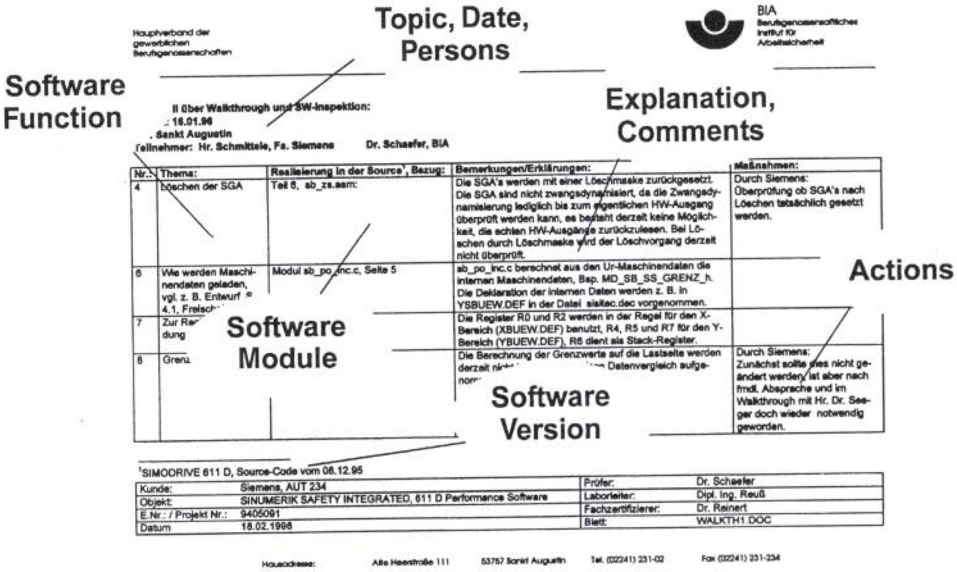


Figure 5. Documentation of walk-throughs.

3.5. Systematic Tests

During the reviews of the specification and the design documentation, the statical analysis, and the walk-throughs, several test cases were generated. Figure 6 shows the BIA's standardized test case documentation. During the generation of the test cases the upper four points were edited into files. These files were then sent to the manufacturer, who prepared the test cases according to the requirements. During several 3-day sessions all test cases were executed in the presence of the BIA experts. The documentation of the tests was directly made during the tests by the BIA.

The execution of the test cases revealed a serious fault in the redundant architecture: Some Input/Output (I/O) information could be blocked by a high priority interrupt of the NC channel so that the machine could move with full speed with opened guards. The fault was corrected using additional software algorithms in both channels.

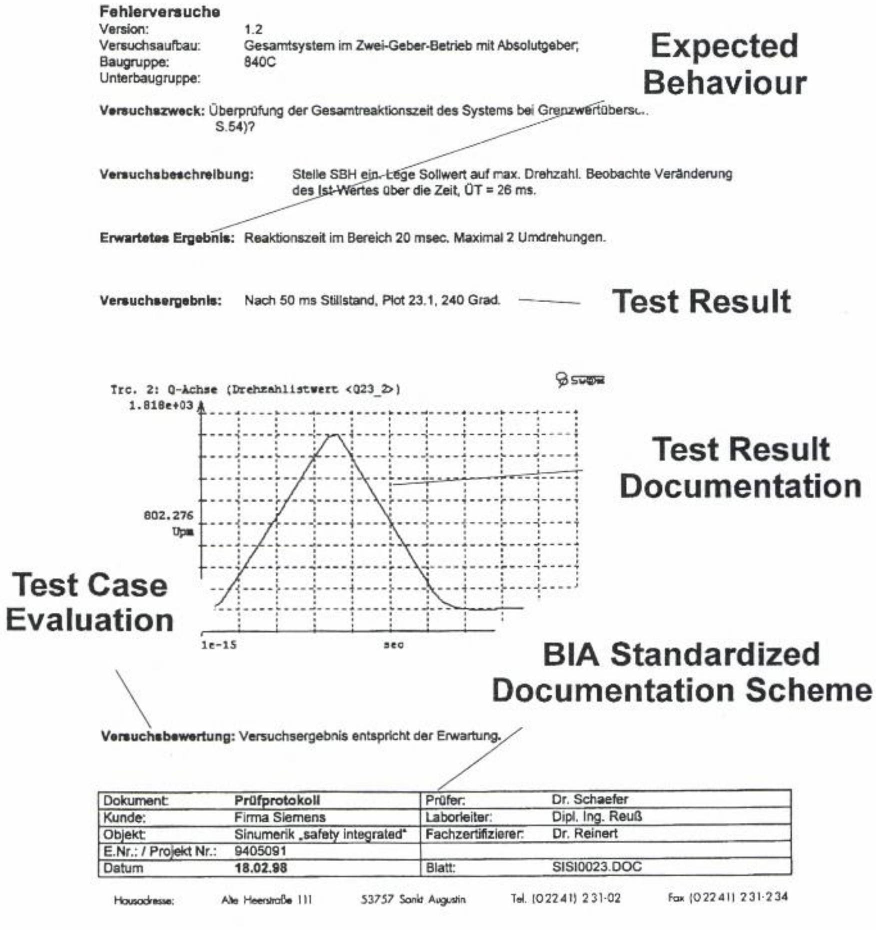


Figure 6. The BIA's standardized test case documentation.

3.6. EMI and Environmental Testing

The robustness of the safety-related system towards expected operating stresses and external influences was checked by means of Electro Magnetic Compatibility (EMC) tests, mechanical shock and vibration testing, Isolation Protection (IP) rate testing, and climatic tests. These tests were conducted by accredited laboratories of the manufacturer and the complete test documentation was checked by safety experts of the BIA.

3.7. Site-Acceptance Tests

An installation manual, which described in detail the installation process, was checked. A complete test was required after installation of the safety-related system. A more than 100-page document describes the operating conditions using the software driven safety functions (see Table 1). During a site acceptance test (see Figure 7) the safety experts checked the use of the installation manual by the machine manufacturer.

Necessary changes were implemented after the first meetings together with the machine manufacturer.

Figure 7. Site acceptance tests on a real machining centre.

3.8. Modification Procedures

After the first certification both controls were changed several times because of user requests. All modifications were documented according to the BIA's requirements. Figure 8 shows an example of a modification in the NC software.

The old and new version numbers were clearly documented. The affected programmes were listed and a verbal description of the modification was made. The origin of the modification request was documented. In several enclosures the listings of the modified code are given together with the code walk-throughs after the modification. Each modification was signed by the software engineer and certified after testing by the BIA.

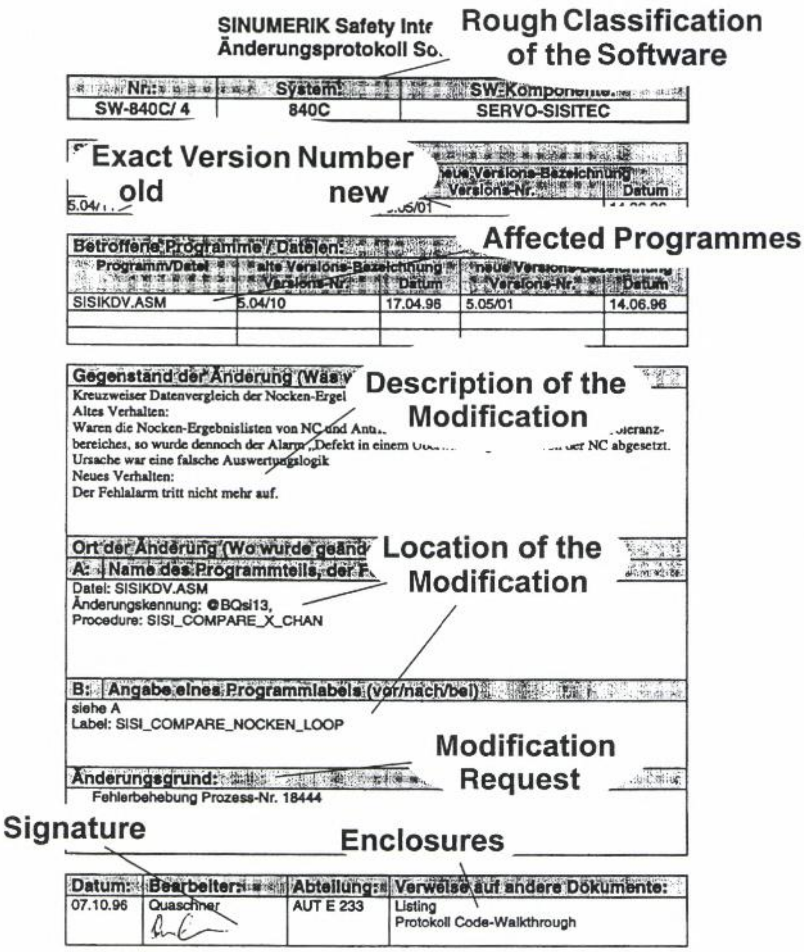


Figure 8. Standardized modification procedure.

4. CONCLUSIONS

This paper shows that machinery safety can be achieved using C standards, which are application-specific, and the requirements of standard

EN 954-1:1997 (CEN, 1997). It could be demonstrated that the use of the German prestandard DIN V VDE 0801 (Standard No. DIN V VDE 0801:1990; DIN, 1990) is necessary for the certification of computerized safety-related systems. In future, the international standard IEC 61508 (Standards No. IEC 61508-1–61508-8:1998; International Electrotechnical Commission [IEC], 1998) will be used instead of the German prestandard. Most of the procedures are identical if a link between requirement classes and safety integrity levels can be established. Per definition, a link between category 2, 3, and 4 and safety integrity level 1, 2, and 3 can be established at least for measures against systematic failures.

REFERENCES

Council Directive 89/392/EEC of June 14, 1989 on the approximation of the laws of the Member States relating to machinery. *Official Journal of the European Community*, No. L 183, June 29, 1989, p. 9.

Deutsches Institut für Normung (DIN). (1990). Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben, mit Anhang A1 [Principles for computers in safety-related systems with annex A] (Standard No. DIN V VDE 0801:1990). Berlin, Germany: Beuth-Verlag.

Dumke, R. (1992). Softwareentwicklung nach Maß. Schätzen—Messen—Bewerten [Adapted software development. Estimation—Measurements—Assessment]. Braunschweig, Germany: Vieweg.

European Committee for Standardization (CEN). (1996). *Safety of machinery—Principles for risk assessment* (Standard No. EN 1050:1996). Brussels, Belgium: Author.

European Committee for Standardization (CEN). (1997). *Machine tools—Safety—Machining centres* (Draft Standard No. prEN 12417:1997). Author: Brussels, Belgium.

European Committee for Standardization (CEN). (1997). *Safety of machinery—Safety-related parts of control systems. Part 1: General principles for design* (Standard No. EN 954-1:1997). Brussels, Belgium: Author.

International Electrotechnical Commission (IEC). (1998). *Functional safety of electrical/electronic/programmable electronic safety-related systems. Parts 1–7* (Standards No. IEC 61508-1–61508-8:1998). Geneva, Switzerland: Author.

McCabe, T.J. (1976). A complexity measure. *IEEE Transactions on Software Engineering, 2*, 308–320.

Reinert, D., & Schaefer, M. (1998). Integrated safety in flexible manufacturing systems. In R.D. Schraft, G. Brandenburg, & W. Leidig, (Eds.), *Tagungsband SPS/IPC/DRIVES* (pp. 305–314). Heidelberg, Germany: Hüthig-Verlag.

Umbreit, M., & Zinken, E. (1995). Drehzahl und Betriebshalt bei Werkzeugmaschinen sicher beherrschen [Speed and operational stop of machine tools safely controlled]. *Antriebstechnik, 5*, 34–38.