PERIODICA POLYTECHNICA SER. EL. ENG. VOL. 34, NO. 4, PP. 245-255 (1990)

STRUCTURAL DESIGN OF SAFETY-RELATED MICROPROCESSOR BASED PROCESS CONTROL SYSTEMS

M. WAGNER

Institute for Quality and Safety in Electronics
TÜV Bavaria, Munich, FRG

Received July 2, 1990; Revised Nov. 30, 1990.

Abstract

This paper first describes the latest progress in national and international standardization efforts concerning the use of microprocessor based safety-related systems.

General design considerations applying to the German standards (TÜV Handbook, DIN 801) are then presented in the second part, where a commonly used failure model and certain process-related time constraints will be discussed.

The third part of this paper deals with two possible examples of commonly used system structures and describes basic technical solutions to provide the necessary safety features.

Keywords: safety-related systems, safety standards.

Standards Concerning Safety-related Applications

In the common European market primarily European Standards will be used and therefore it is a goal of national standardisation efforts to work on European standards. The national standards should only be used in areas where no international or European standards. The national standards should only be used in areas where no international or European standards are available.

The standards described in the following chapters are original German standards used in the fields of safety related applications. It is intended to faise the standard DIN VDE 0116 to a European level. The DIN V VDE 19250 influences the work of some CEN standardisation groups as a working document. DIN V VDE 801 is seen in some correletion to the IEC working groups 9 and 10 and at the moment it is not predictable if this standard will lead to a European Standard.

DIN VDE 0116: Electrical equipment of furnaces

DIN VDE 0116 concerns the electrical equipment used in furnaces and is one of the first German standards to use failure models with the help of data flow diagrams. The following cases are distinguished:

- Failure consideration on the permanently wired part of the safety equipment
- Evidenced safety against failures and faults for the stored program part of the safety equipment
- Evidenced safety of software

Beside the details of furnace techniques, the explanatory part of this standard provides several basic statements on:

- specification
- checking the specification
- program diversity
- program analysis and software tools

What is special about this standard is its historical aspect, as it is one of the first specific standards to deal with the basic problems of software development.

TÜV Handbook: Microcomputers in Safety Technique

The handbook 'Microcomputers in Safety Technique' (HÖLSCHER and RADER, 1986), is a guide for developers and manufacturers who are designing and developing safety-related systems. It contains a catalogue of system structures and safety measures for microcomputer control systems, distinguishing various safety classes and providing different sets of measures those classes.

Five safety classes are defined here. Beginning with the existing equipment-specific individual standards, these classes are assigned to applications. The following list shows the original assignments of safety-related equipment to the classes:

Class 1:
- Press control systems to ZIII/456 or 457
- Train signalling systems to DIN 57831 / VDE 0831
- Tracking systems

Class 2:
- Elevator control systems to TRA 200/101
- Escalator control systems (unless covered by EN 115)

Class 3:
- Road traffic signalling equipment to DIN 57831 / VDE 0832
- Electrical furnace equipment to DIN 57116 / VDE 0116

— Remote control systems for gas and oil pipelines to TRGL 181
— Mobile sales units (current equipment)
— Aerial cableway control systems

Class 4:
— Electrical medical equipment to DIN IEC 601 / VDE 0750
— Radio remote control systems for cranes to ZH1/547
— Platform lifts to VBG 14

Class 5:
— Household appliances
— Ski fixtures and adjustment equipment
— Paper shredders
— Control systems for power-driven gates

Sets of technical measures are assigned to each of these safety classes, while distinguishing between two alternative implementations:

— single-channel structure with monitoring
— twin-channel structure

The individual measures are then described, along with their efficiency in dealing with the various fault causes and the testing necessary to demonstrate safety.

DIN V VDE 19 250: Measurement and control: Fundamental safety aspects to be considered for measurement and control equipment

This standard provides a systematic way of setting up technical safety requirements. Some important terminology is defined and the significance of process control protection and protection equipment is explained. The risk of equipment without protection is reduced by process control protective measures,often in combination with non-process control protection, to a residual risk, which should be smaller than the acceptable risk limit. The acceptable risk limit is defined by the acceptance of the threats by the society and by the needs for protection.

The risk of the overall system being reduced is divided into partial risks of the subsystems. Requirements graded into eight requirement classes are determined for each partial risk, which is described by its risk parameters.

These eight requirement classes represent an extension of the previous five-class scheme from the TÜV Handbook and, in addition , they are independent of applications, i.e. not assigned per definition to fixed areas, for example an elevator control system.

The risk element of a technical system is assigned to one of the eight requirement classes using a risk chart which applies the parameters: extent

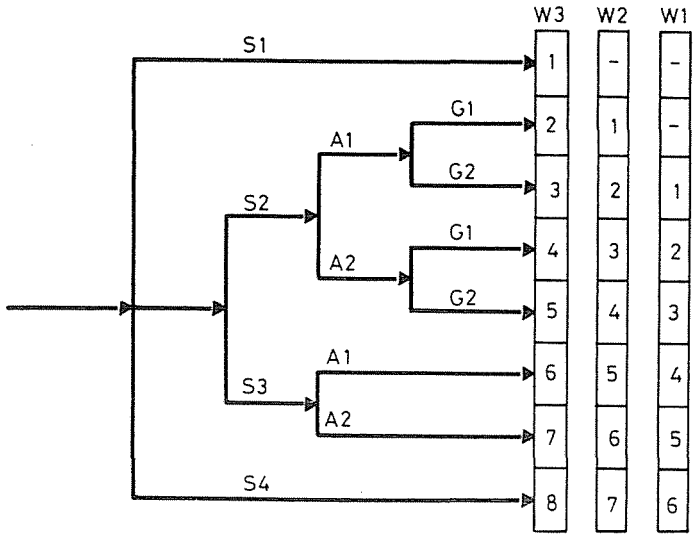

Fig. 1. Risk chart and requirement classes

of damage, abode time, hazard prevention and occurrence probability to determine the assignment.
The risk parameters have the following meanings:

S Extent of damage
- S1: slight injury
- S2: severe irreversible injury to one or more persons or death of one person
- S3: Death of several persons
- S4: catastrophic consequences, several deaths

A Abode time
- A1: seldom to relatively frequent
- A2: frequent to continuous

G Hazard prevention
- G1: possible under certain conditions
- G2: hardly possible

W Occurrence probability of the undesired event
- W1: very low
- W2: low
- W3: relatively high

The essential new basic idea here is that these parameters can be used to assign the various applications (from the nuclear power station to the household iron) to one of the eight classes independently of the application

and the technology used, making the different application areas comparable in terms of their safety-related classification.

DIN V VDE 0801: Principles for computers in safety-related systems

This standard is an extension to the TÜV Handbook by HÖLSCHER and RADER. It also deals with measures for avoiding and controlling faults, whereby the measures for avoiding faults take into account the different phases of the product life cycle. The individual measures are then explained in detail and illustrated by examples in a very exhaustive normative appendix. The discussion includes hardware and software development as well as structural considerations on redundant and diversified systems.

The subject is rounded off by a number of examples of measures in different requirement classes.

5SC65A WG 10: Draft: Functional safety of programmable electronic systems: Generic aspects

This draft is concerned on an international level with the functional safety of programmable electronic systems. It is currently under thorough revision but finally aims at forming a 'basis for future application-specific in ternational standards for all areas of application.' Revisions are also intended to make the standard independent of the technology of the protection system.

Ideas on system structure and on the classification of systems form one of the essential aspects of this paper. In the chapter entitled 'Phase plan of the safety system,' fundamental knowledge is imparted on:

- Hazard analysis and risk assessment
- Specification of safety requirements
- Description of safety-related systems
- Design and execution
- Validation of safety
- Operation and maintenance
- Modification of the system (in preparation)
- Shutting down (in preparation)
- Retrofitting (in preparation)

The elaboration of the subjects covers the entire service life of the programmable electronic system.

The further key points of this paper are ideas on the quality requirements and ways of assessing the system.

SC65A WG 9: Draft: Software for computers in the application of industrial safety-related systems

This paper (IEC 1989b) deals specifically with issues of software safety. Beside general considerations on software architecture, design strategies (top-down design etc.), the entire software life-cycle is examined. The following topics are discussed:

- Software requirements specification
- Development
- Verification
- Integration
- Validation
- Documentation
- Assessment
- Quality assurance
- Maintenance

The appendix introduces and discusses methods of design, design verification, documentation and development rules.

System Design Considerations

This chapter collects some ideas on the designing of safety-relevant systems. The basic idea is to distinguish between all functional parts of the process and all safety related parts. The safety related parts should handle all safety features, e.g. failure detection, shut down operation, self tests ect. Most of all safety related applications are time critical and therefore a failure model commonly employed in safety engineering techniques will be explained and basic timing considerations presented.

Failure Model

Safety engineering usually assumes the following basic premise:
A simple first error must not lead to a critical system state. This means that when a fault of this type occurs, the protection system must immediately bring the process into a safe state, at least within a maximum fault detection and fault response time specified by the process.

It is not assumed that two independent faults occur exactly at the same time, but consecutive faults are regarded as a single fault.

In the event of an undetected and inherently non-critical first fault the additional occurrence of a second fault must be expected after a period of time specified.

The fault detection and fault response times of the protection system should always be clearly shorter than the second fault occurrence time. Values of 1/10 of the second fault occurrence time or better would be recommendable here.

Timing Considerations

In the following section different configurations of single-channel and twin-channel systems will be examined with regard to their timing, based on the failure model above. We distinguish between the actual process guidance (operational process control system) and a process control protection system in conjunction with various process-conditioned timing requirements.

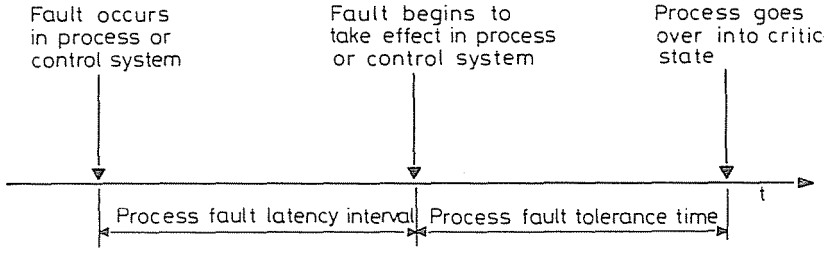

Fig. 2. Timing considerations for control system and process

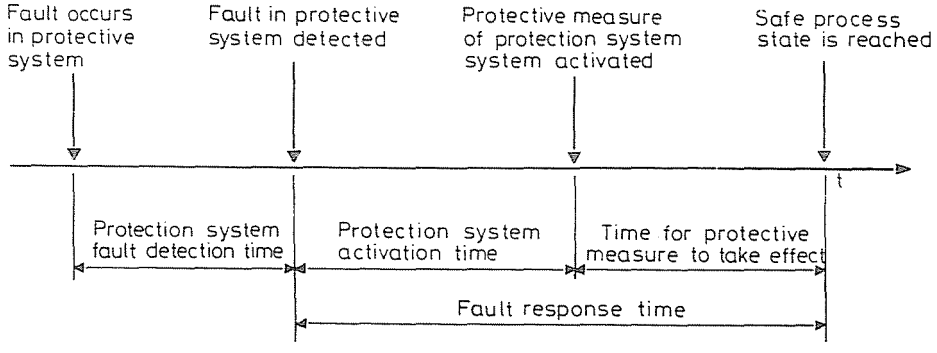

Fig. 3. Timing considerations for the protection system of the process

a) Process control system containing control and protection functions
In a combined control and protection system — without additional measures — no fault must occur which will lead to a critical process state and at the same time prevent the protection system from taking effect.

This leads to the need for a functional separation of the closed-loop control system and the protection system.

b) The control and protection system are functionally separate, the protection system is simple

b1) Fault in control system, protection system intact

The requirement for the protection system here is that the fault detection and response times required to detect and respond to the faulty process state always be smaller than the process-conditioned fault tolerance time.

b2) Faults in the protection system, control system intact

Here, the fault detection and response times required to detect and respond to the protection system fault should always be clearly smaller than the second fault occurrence time.

The second fault occurrence time is a period of time independent of the reliability of the overall system (process, operational and protective systems) following which, on average, the occurrence of a further independent fault can be expected. This second fault may by, for wxample, a fault in the closed-loop control system, necessitating the availability of a functioning protection system. Depending on the type of process control safety requirement, this can mean that different measures are taken when a fault is detected in the protection system, e.g:

- safe process state reached, emergency shut down systems
- pure message, alarm systems
- reconfiguration with standby systems etc.

The fault can also be detected in different ways, e.g. by

- technical measures, self-testing etc.
- organisational measures, repeated tests etc.

The selection of measures, however, is always dependent on the process-conditioned timing requirements and on the feasibility of the organisational measures.

c) Closed-loop control system, parallel protection system, multiple protection systems to increase safety

c1) Fault in closed-loop control system, protection system intact

The same requirement applies here as in case b1)

c2) Fault in a protection system, closed-loop control system intact

As the protection system here is a twin version, there will still be a functioning protection system available at this moment. Lower requirements can be specified here with regard to the fault detection and response times required to detect and respond to the faulty protection system.

Examples of Technical Solutions

Single-channel Solution

We speak of a single-channel structure when there is one single processing unit (e.g. a microprocessor) responsible both for operational functions and protection functions of the systems.

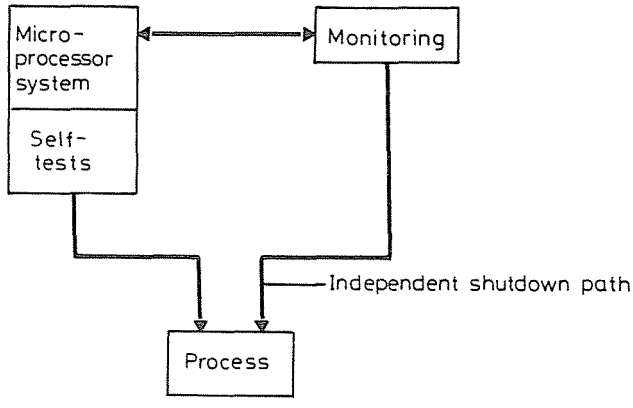

Fig. 4. Single channel system with monitoring

As explained in the previous chapter, processor failure here could lead to dangerous system states, as the protection function is also provided by the processor. This makes single-channel solutions suitable only for low safety requirements, and only when a system state can be clearly defined and additional monitoring functions are incorporated. This means:

— implementation of timing monitoring (watch-dog)
— implementation of a second independent time base
— two shutdown paths independent of each other
— implementation of extensive self-testing

The processor and the monitoring system must test each other and each must be capable of bringing the process into a safe state independently of each other in the event of a fault. This shutdown option must be tested at certain intervals to ensure that when an undetected and non-critical first fault occurrs, which would prevent protective action from being taken, the first fault is detected by the self-test, an alarm message is generated and the process can be taken into safe state (shut down).

The cyclic self-tests contain:

— microprocessor self-test (instruction set, registers etc.)

— RAM test
— EPROM (memory) test
— test of peripheral components (timers, DMA etc.)
— test of I/O paths
— watchdog test
— shut-down path test

Further methods of providing robust program and software configuration are:

— logical and temporal program execution monitoring
— assertions
— area checks (index range etc.)
— functional diversity by means of control and protective software separation

Twin-channel Solution

In the twin-channel solution two independent processing units (microprocessors) each perform the same tasks, while the results are continuously and cyclically cross-checked (complementary testing). This can mean that the output signals from the processors are each put through a fail-safe comporator which shuts down the process when a mismatch is found.

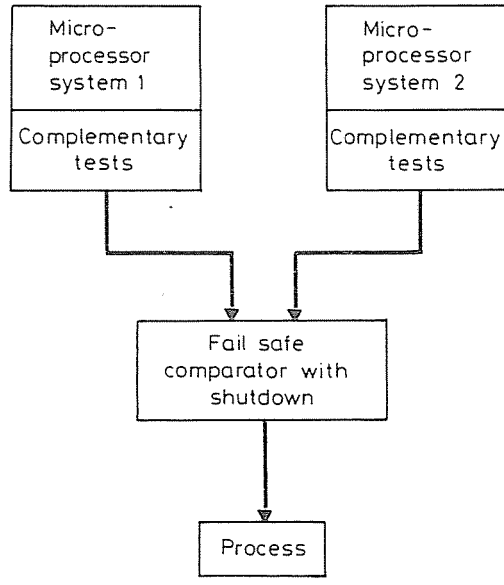

Fig. 5. Twin channel system

Self-tests should be incorporated here too, but they need not be performed to the full extent. All dynamically changing signals fed through the comparator are supervised. Static signals however need to be tested, because passive br eakdown (no signal change) will not be detected by the comparator. In this case the same failure could occur in the second channel after a certain time and the protective system would not be able to operate correctly.

Conclusion

In the first chapter we introduced various national and international standards and guide-lines reflecting the current state of standardization activity in the field of safety-related systems and equipment.

This was followed by some basic system and timing considerations for a failure model commonly used in safety engineering.
Finally, examples of single-channel and twin-channel solutions completed our brief safety discussion.

References

DIN (1989a): DIN VDE 0116: Electrical equipment of furnaces, 1989

DIN (1989b): DIN V VDE 19 250: Measurement and control: Fundamental safety aspects to be considered for measurement and control equipment, January 1989

DIN (1989c): DIN V VDE 0801: Principles for computers in safety-related systems, preliminary standard.

HÖLSCHER, H. — RADER, J. (1986): Microcomputers in Safety Technique. Verlag TÜV Bayern, Verlag TÜV Rheinland, Munich 1986

IEC (1989a): IEC SC65A WG 10: Draft: Functional safety of programmable electronic systems: Generic aspects. October 1989

IEC (1989b): IEC SC65A WG 9: Draft: Software for computers in the application of industrial safety related systems. August 1989

Address:

Dr.-Ing. Markus WAGNER
TÜV Bayern
Westendstr. 199
D-8000 München 21,
BRD