

Functional Safety of a Theatre Stage Machinery Control System

Michael J. Bauer

Bytecraft Automation Pty Ltd
23-27 Fonceca Street, Mordialloc, VIC 3195
Melbourne Australia

mbauer@bytecraft.com.au

Abstract

Computer technology has the potential to significantly reduce the risks associated with scenery motion in live theatre, as well as enhancing the spectacle of performance. The industry is becoming more concerned about safety standards compliance. IEC 61508 is emerging as the universally favoured standard for functional safety of stage machinery control systems.

Acknowledgments

The author gratefully acknowledges the contributions of Ted Fregon (CEO, Bytecraft Automation) and Kevin Anderson (Director, Risk & Reliability Associates) to the preparation of this paper.

1 Introduction

The application of new technology to the "performance space" not only creates the opportunity to produce greater novelty and spectacle but also the opportunity to increase safety & reliability and ultimately reduce the levels of risk in the theatre environment.

Control system safety deficiencies in other industries have led to new International Standards such as IEC61508 for "Functional Safety" and this standard appears to be generically applicable to theatre technology.

Faced with this reality and the clear vision that the professional entertainment industry was ready for a viable International Standards regime, Bytecraft elected in 1995 to embrace IEC 61508.

Bytecraft has recently embarked on a new stage machinery control system development project. The aim is to address safety-related aspects in just one of the many new-technology systems that operate in the theatre performance space, the Scenery Handling System (SHS). This undertaking required a rigorous Hazard and Risk Analysis.

To perform the Hazard and Risk Analysis, it was necessary to develop a level of understanding of the Equipment Under Control (EUC) and its environment (physical, legislative etc.) sufficient to enable the other safety lifecycle activities associated with development of the SHS to be satisfactorily carried out.

2 What is "Functional Safety"?

Functional Safety is defined (by IEC 61508) as "part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk-reduction facilities". The keywords here are "correct functioning".

Explosives manufacture, nuclear reactor and aerospace flight-control applications are characterised by the need for "continuous" control, because there is no "fail-safe" state. Thus reliability and availability (together) become effectively synonymous with safety integrity.

Conversely, stage machinery control systems have a clearly defined safe state, i.e. "motion stopped". Fail-safe systems are a lot simpler to design and implement than continuous control systems. As a minimum requirement, the safety functions built into a fail-safe SHS Control System need to ensure that motion is prevented in the event of a "loss of control" condition, i.e. a dangerous failure.

Functional safety is realised by attaining an acceptably low "dangerous failure rate" and/or by implementing fault-detection mechanisms that ensure the system fails to a safe state.

3 Applicable standards

Several non-sector-specific standards other than IEC 61508 are relevant to stage machinery control systems. For example, European and German standards:

EN 954-1 [2] (which covers electronic and software controls, but not as comprehensively as IEC 61508.), EN 1050 [3], EN 1037 [4], EN 60204-1 [5], DIN V 19250 [6], DIN VDE 0801 [7], etc.

The following sector-specific German safety standards relating to safety of theatre stage machinery were identified as being relevant to the project:

DIN 56925 [8] "Theatre engineering: Stage machinery - Point hoist - Safety requirements and testing" (June 1997)

DIN 56921-11 [9] "Theatre engineering: Stage machinery - Batten hoist - Safety requirements and testing" (July 1997)

DIN 56940 [10] "Theatre engineering: Stage machinery - Stage Elevators - Safety requirements and testing" (Draft, 2001)

4 Why Bytecrafft chose IEC 61508

Increasingly, clients and theatre technology consultants are specifying compliance to safety standards. The sector-specific DIN standards are often quoted, but the general consensus within the industry is that these will be superseded by 61508.

IEC 61508 is a single unified work which subsumes the scope of multiple separate entities from the EN and DIN regimes. Further, 61508 offers a choice of methods for risk assessment, both qualitative and quantitative, whereas the EN and DIN methods are just qualitative (i.e. "Risk Graph"). Although generic, 61508 when properly applied, leads to a determination of specific design measures and techniques to be applied to safety functions at each safety integrity level (SIL).

As 61508 is a truly International standard, it is likely to be specified in more countries than the DIN standards. Where necessary, equivalence between DIN "Risk Class" (AK) and IEC "Safety Integrity Level" (SIL) can be inferred.

5 Hazards in live theatre

There are areas of the theatre environment where both people and the scenery handling system (SHS) and attached scenery co-exist. Within the stage area there is the risk of collision between the SHS or attached scenery and people, thus potentially causing harm. The likely sources of hazards fall into three areas:

- An operator makes an error or fails to notice a dangerous situation;
- There is a dangerous failure in the equipment under control, or in the SHS Control System itself;
- A performer, crew member or maintenance worker is in the wrong position and hence exposed to danger.

Machinery parts in a winch room, on the grid and below-stage areas will often be commanded to move from arbitrary operator control panel (OCP) locations within the stage tower. Operators would not normally monitor these areas and thus machine parts may move without warning at any time, putting at risk people working in close proximity.

In the current development project, risk assessment is concerned primarily with SHS Control System hazards and does not consider hazards of the SHS itself (mechanical, electrical, structural) beyond potential failures that could place demands on the SHS.

Many of the identified hazards were found to be attributable to human error, e.g. failing to look out for dangerous situations before starting a machine, pressing the wrong buttons, overloading a machine, etc.

Other hazards are inherent in the equipment under control, e.g. mechanical failures in gearboxes, couplings, holding brakes, motors and drives, etc.

Examples of hazards attributable to the SHS Control System itself are:

- Spurious brake release, due to random hardware failure (e.g. micro-controller output logic, relay driver, relay), or due to systematic error (software bug);
- Axis position or velocity measurement error, or position sensor calibration error;
- Database corruption in server or system controller ;
- Data communications error (data loss, data corruption, packet timing, packet sequence);
- Human-machine interface (HMI) error, e.g. wrong command generated (due to systematic error or random hardware failure);
- System controller processing error;
- Axis controller module (ACM) processing error;
- Group synchronisation error, including failure to start & stop concurrently.

6 Risk-mitigating measures

IEC 61508 identifies three categories of risk-reduction measures: "ERRFs", "Other Technology" and safety functions within the safety-related system.

Examples of "external risk-reduction facilities" (ERRFs), primarily aimed at minimising human error are:

- Operator supervision;
- Operator training;
- Operation & maintenance procedures.

Examples of "Other Technology", risk-reduction measures largely outside the scope of the SHS Control System (although interfaces to it may be required), are:

- Emergency Stop;
- Safe-edge sensors (stage wagons, doors, etc);
- Safety gates (stage elevators);
- "Look-ahead" sensor (stage wagon);
- Limit available output power of machine to safe level;
- Motor over-temperature sensor;
- Secondary brake.

Examples from the many safety functions incorporated into Bytecrafft's "State™" SHS Control Systems (some of which require external sensors) are:

- DMB ("Dead-man button") function;
- Automatic cue sequencing;
- Comm's network data integrity and timing checks, (CRC, preset time-out, packet sequence field);
- Command & data "sensitivity checks" by system controller and axis controller module (ACM);
- Static load measurement, overload sensing, load/speed de-rating;
- Dynamic load monitoring ("snag" detection);
- Supervision of ACMs in synchronous group motion;
- Axis controller "Safety Processor" (smart watchdog);
- Actuator state feedback to ACM;
- Dual redundant position measurement sensors;

- Software travel limits (ACM parameters);
- Hardware travel limits (inputs to ACM);
- Safety sensors, e.g. belt/chain break, crossed-groove, slack cable (inputs to ACM);
- Redundant axis speed and acceleration monitoring;
- Redundant axis position profile tracking.

7 The risk-prediction model

A tool or model of some sort is required to assess or quantify the risk attributable to the identified hazards, with and without risk mitigation measures, and hence to assess the portion of risk attributable to the SHS Control System.

Bytecraft opted to apply both the Risk Graph and Cause-Consequence Model (CCM) methods and to compare the results. A German sector-specific standard, DIN 56921-11 [9], contains examples of the application of the Risk Graph method to various safety-related functions. Hence, a benchmark has been established.

The outputs of the CCM were shown as probability of hazardous event, i.e. probability of “no harm”, “person struck by moving object”, “injury”, “fatality”, etc. This gave a measure of residual risk for each hazard.

Hazards relating to synchronous group movements were considered far more likely to result in harm than others. Further, the ratio of “fatality” to “injury”, as a consequence of a dangerous failure, was estimated to be higher in the case of synchronised group motion. This takes into account the possibility of groups of machines being used to suspend large heavy objects above the performance space.

In cases of hazards arising from operator error, differing estimates of Human Reliability were used, depending on the task. These estimates were based on published statistics on HEP, for example Shelton (1995).

There is a scarcity of reliable statistics on injury and/or fatality due to the use of powered stage machinery, with or without computer-based controls. Without such statistics, it is not possible to validate the absolute accuracy of the risk-prediction model. Consequently, Bytecraft elected to establish relative risk targets rather than absolute.

A relative risk target could be expressed as the fraction of risk attributable to the SHS Control System, compared with the overall risk attributable to the use of powered stage machinery (including risks due to human error). For example, a “tolerable risk” target for the SHS Control System could be set at 10% of the overall residual risk, on the assumption that the overall risk is not significantly higher than the average occupational risk in our civilisation.

The CCM method determined that the risk attributable to the computer-based SHS Control System could be less than 5% of the overall residual risk associated with the use of stage machinery, without incurring costs grossly disproportionate to the safety benefit.

A variant of the model further revealed that the use of computerised controls would actually reduce the overall risk compared to using manually-operated (open loop) controls, by a factor of about five.

If this result seems counter-intuitive, based on the complexities of programmable electronic equipment, consider that in general a computer-based system can provide:

- Higher diagnostic coverage (monitoring of itself and EUC functions);
- Precision, predictable and repeatable actions ;
- Lower dependence on human reliability (by means of command “sensitivity checks” etc).

The results of Bytecraft’s quantitative risk assessment model are consistent with the sector-specific German safety standards, DIN 56925, DIN 56921-11 and DIN 56940, which use the qualitative “Risk Graph” model.

8 Safety Requirements Determination

The risk-prediction model (CCM) was implemented as a spreadsheet calculator, facilitating the task of determining a suitable safety integrity (i.e. acceptable failure rate) for each of the 39 safety functions defined. This determination was made consistent with the “ALARP” principle, i.e. that the residual risk should be kept “as low as reasonably practicable”.

In practice, it is likely that the realisation of most of these safety functions will result in a higher safety integrity than the determined minimum. This happens because, in many cases, safety functions of varying safety integrity requirement cannot easily be made independent, so the highest determined integrity level must be allocated to all.

9 SIL allocation

A Safety Integrity Level (SIL) was allocated to each safety function based on its maximum allowable probability of failure. The correlation between these quantities is defined in IEC 61508, Part 1, clause 7.6.2.9, Table 2, for “low demand mode of operation”. For example, SIL2 corresponds to a probability of failure on demand in the range 0.001 to 0.01.

In our application, the safety function SILs vary from “none” to SIL2. Note that SILs derived in this manner apply purely to safety functions, as opposed to “operational functions”. It is important to make the distinction, because an operational function may embody more than one safety function acting in parallel, yielding a higher SIL than that of any single safety function.

For example, movement of a synchronised group of machines is a “safety-critical operational function”, the associated hazards of which are mitigated by several safety functions acting together.

It is common practice, although not very meaningful, to specify a Safety Integrity Level (or DIN “Risk Class”) to the EUC control system as a whole. It is more meaningful to specify a SIL for a particular safety-related operational function, e.g. that assigned the highest SIL.

The IEC 61508 method for allocating a SIL to an overall system, or a particular safety-related function, is to express the residual risk in terms of “dangerous failures per hour” and then applying Table 3 (IEC 61508-1) to obtain an equivalent SIL.

When applied to the Bytecraft SHS Control System under development, this method yields a high SIL2 for the system as a whole and SIL3 for the highest integrity functions, e.g. movement of a synchronised group of axes.

10 Realisation of the Safety Functions

The practical implementation of each safety function must be designed and analysed to ensure that its specified Safety Integrity Requirement is achieved.

The preferred method is to break down the function into elementary hardware and software components, assigning to each a failure rate. These failure rates may be design targets (e.g. for software modules), or may be obtained from known data (e.g. for hardware components).

Graphical tools such as “Fault Tree analysis” can be used to calculate the composite failure rate and to identify “weak spots” in the design. Weak spots may need fortification, e.g. by means of (further) redundancy. Conversely, the analysis may well reveal elements which are non-critical, i.e. having negligible effect on the composite safety integrity, and hence may be exempt from the application of formal design methods and techniques.

Having determined SIL requirements for every safety function, the IEC 61508 standard “recommends” various design methods and techniques at each SIL, for “control of random hardware failures” and “avoidance of systematic errors...” A few examples from the Bytecraft development project follow.

11 Design measures & techniques

Example 1: Processor Redundancy.

Many of the safety-related functions of the axis controller are realised in software. A random hardware failure in a sole micro-controller, or for that matter a systematic error (e.g. software bug), could conceivably result in loss of control.

The hazard is mitigated by the introduction of an independent “Safety Processor”, i.e. a second (redundant) micro-controller, having the responsibility to supervise all safety-related functions of the axis controller. The safety processor has the ability, via a single logic output, to inhibit all control outputs of the main processor, thereby placing the machine into a safe state, i.e. a processor-initiated emergency stop.

Example 2: Signal Monitoring.

The axis controller has inputs dedicated to monitoring the states of external actuators by means of feedback signals, including drive main contactor(s), brake actuator(s) and a velocity reference signal from a variable-speed drive.

This provision will not only detect faulty operation of the module’s control outputs, but also external equipment.

For purposes of Functional Safety Assessment (FSA), the realisation of safety-related functions must be traceable from Safety Requirements Specifications through to design Verification and Validation testing. This process can be formalised by means of CASE tools. Bytecraft has chosen several tools from the “Rational Unified Process” suite, e.g. “Requisite Pro” for requirements capture, traceability, etc.

A comprehensive study of software design measures and techniques aimed at avoidance of systematic errors is beyond the scope of this paper. The reader is referred to the standard, IEC 61508, Part 7.

12 Conclusion

The paper presented a brief account of the actual process followed toward achieving compliance with Part 1 of the standard, up to Safety Requirements Definition and SIL Allocation. A more detailed account of the realisation of safety functions, including semi-formal software design measures and techniques employed in the project, may well provide material for a future paper.

Term	Meaning
ACM	Axis Controller Module (“Wincon” = winch controller). One ACM is interfaced to each variable speed machine in a typical SHS. The ACMs are networked to a system controller CPU, via Ethernet, from which the ACMs are commanded to execute precise movements of their axes.
ALARP	“As Low As Reasonably Practical” – Legal term used in reference to risk minimisation.
CCM	Cause-consequence model, as used for risk prediction and safety integrity determination.
CRC	Cyclic Redundancy Check – A form of checksum.
DIN	Deutsches Institut für Normung (German Institute for Standards)
DMB	Dead-Man’s Button: A mechanism to ensure that motion will be stopped if an operator’s attention is diverted from the task at hand. In order for a machine to continue its motion, the operator must keep a DMB push-button depressed.
EN	European Norm (European Standard)
E/E/PE	Electrical / Electronic / Programmable Electronic (system)
EUC	Equipment Under Control
FSA	Functional Safety Assessment / Assessor
HEP	Human Error Probability
HMI	Human-Machine Interface
IEC	International Electro-technical Commission
OCP	Operator Control Panel (generic)
SHCS	Scenery Handling Control System
SHS	Scenery Handling System, comprising stage machinery (EUC) and the SHS Control System; in some contexts also the attachments (scenery).
SRS	Safety-Related System (also Safety Requirements Specification)
SIL	Safety Integrity Level

Table 1: Terms and Acronyms

References

1. IEC 61508 (1998, 2000): Functional safety of electrical/ electronic/ programmable electronic safety-related systems. <http://www.iec.ch>
2. EN 954-1 (1997) Safety of machinery. Safety-related parts of control systems. General principles for design.
3. EN 1050 (1996) Safety of machinery. Principles for risk assessment.
4. EN 1037 (1996) Safety of machinery. Prevention of unexpected start-up.
5. EN 60204-1 (1998) Safety of machinery. Electrical equipment of machines.
6. DIN V 19250 (1994) "Control Technology: Fundamental Safety Aspects..."
7. DIN VDE 0801 (1994) "Principles for computers in safety-related systems"
8. DIN 56925 (1997) "Theatre engineering: Stage machinery - Point hoist - Safety requirements and testing" (June 1997)
9. DIN 56921-11 (1997) "Theatre engineering: Stage machinery - Batten hoist - Safety requirements and testing" (July 1997)
10. DIN 56940 (2001) "Theatre engineering: Stage machinery - Stage Elevators - Safety requirements and testing" (Draft)
11. SHELTON, Charles P (1995): Human Interface/ Human Error, *Dependable Embedded Systems* 18-849b, Carnegie Mellon Univ.