The Relative Impact of Control Reliability on Machinery Risk

Douglas S. G. Nix, A.Sc.T., *Member, IEEE*

***Abstract*—Control of risks related to machinery is central to current product and occupational health and safety legislation in North America and the European Union. Understanding these risks requires risk assessment, and this process is represented in all leading standards in these jurisdictions. Standards provide machine designers with a hierarchy of controls that can effectively control these risks when appropriately applied, including the application of engineering controls as the second stage in the hierarchy. In the second stage, safeguarding systems that involve the control system of the machinery to alter the characteristics of the hazard or the probability of exposure to the hazard have become central in the large majority of machinery designs. Reliability of these control systems is one critical element in the application of these systems.**

This paper explores the impact of control reliability on overall risk control for machinery, and shows the cost of analysis and design of safety-related control systems may be greater than the benefits of the risk reduction achieved.

***Index Terms*—machinery, reliability, risk, safety, SRP/CS, control system**

I. Definitions

safety–related part of a control system (SRP/CS)

Part of a control system that responds to safety-related input signals and generates safety-related output signals. [8, 3.1.1]

SME

Small to medium-sized enterprise, a company with no more than 500 employees.

The New Oxford American Dictionary, THIRD EDITION.

II. Introduction

When electrical control systems first began to be developed in the 1880's with the advent of early electrical machinery, it was soon evident that safety-related aspects of the machinery could and should be addressed by features in the design of the control systems.

Electric trolleys installed in Richmond, VA in 1887/88 by F. J. Sprague [1] included some of the first safety-related electrical controls, later included in the design for the electric elevators.

These elevators included one of the earliest instances of the 'dead man control', a device intended to ensure that the elevator remained under control. These devices became what we now call 'enabling devices' in machinery control system designs. Variations are still part of the streetcar and rail locomotive design today. Sprague's work on train control systems at Grand Central Station in New York City resulted in the development of the earliest track side controls, used to ensure that trains obeyed signals in yards. Sprague also developed the first Multiple Unit Train Controls, demonstrated in Chicago in 1892.

The advent of safety-related controls systems showed the large potential for electrical control systems to provide safety functions and reduce risk. Reliability of these systems was not initially a major consideration since there was virtually no data on failures, and the reliability discipline was not yet developed. Formal risk assessment methods were also undeveloped, and no formal methods for assessing risk and implementing risk controls existed. Much emphasis was placed on the operators of the systems to ensure safety, often with disastrous results. System reliability began it's early development in aircraft design during World War II, but the operator-centric approach continued to predominate until the NASA space program started in the late 1950's.

Development of nuclear power started after World War II, and electrical and electronic controls were integral to reactor design. Safety-related control design gained increasing focus as these systems were developed, in large part due to the introduction of formal risk assessment methods developed to try to gain insight into the risks posed to the general population by this new technology. Failures in these systems could lead to the deaths of thousands in the general population, and the loss of use of large areas of land contaminated by radioactive debris [2].

Only rarely were control reliability techniques used in the design of machine-tool controls until the 1980's, with the introduction of PLC controls and robotics. Slowly, risk assessment methods developed for aviation and nuclear power design were being adapted to the design of increasingly sophisticated manufacturing systems. The potential for injuries and fatalities from these machines was becoming reality in many workplaces, but even with the advancement of this understanding, most machine-tools were still being built with very simple safety-related controls. Most commonly this was an emergency stop control, with some machinery including simple electro-mechanical or purely mechanical interlocks.

During the 1980's the earliest machinery safety standards were being developed. Risk related to early robotic systems had resulted in the deaths of workers in the USA, and the users

Manuscript received Aug. 31, 2012. This work was entirely supported by Compliance InSight Consulting Inc.

D. S. G. Nix is with Compliance InSight Consulting Inc. phone: 519-650-4753; fax: 519-653-1318; e-mail: dnix@ieee.org.

of these systems in the automotive sector were demanding improved safety. OSHA's earliest standards for machine guarding were introduced in 1974, but these early standards did not adequately address the hazards presented by these new technologies.

In 1986, the Robotics Industry Association in the US published the first edition of RIA R15.06, but it was not until the 1992 edition of this standard [4] that control reliability was introduced. In Europe work had started on the first edition of CEN EN 954-1, published in 1995 [5]. In Canada, the first edition of CSA Z434 [6] took a similar approach to RIA R15.06-1992 and was published 1994. Many other standards have since been published that include control reliability requirements for safeguarding systems, or that reference current standards such as ISO 13849-1 [7], and IEC 62061 [8].

The advent of the EU Machinery Directive in 1992 [9] placed specific legal obligations on machine builders to produce and sell safe machinery. These legal requirements are supported by technical standards harmonized for use in all EU member states. EN 954-1 was the first standard on control reliability harmonized under this directive and therefore broadly applicable to all forms of machinery sold in the EU. Clearly, the need for reliable safety-related controls was recognized by the engineering and safety communities. It was believed that control system failures were making some contribution to the risk to which machine operators were exposed, but quantifiable data was needed to advance understanding.

In Canada and the USA, workplace injury statistics are kept by the workplace insurance organizations in each Province, and by OSHA in the USA [10], [11]. Unfortunately, research using these databases showed that statistics relating workplace injuries and fatalities connected to machinery control system failures are not being collected. Some European countries, most notably Germany, are collecting data on these points, and publication of this data will begin to show the effects these failures on injuries and fatalities, but as yet, the impact remains unclear.

Current emphasis on control system design for reliability has caused designers to lose sight of the small effect that the reliability of the safety-related parts of the control system (SRP/CS) often play in overall risk reduction. While International standards focus on increasingly flexible but complex methods for analyzing and assessing control reliability, there is very little statistical data to back up assumptions about the contribution of SRP/CS failures to injuries from machinery. This emphasis on SRP/CS design is leading machine builders to invest increasingly large amounts of design time in analysis of the SRP/CS, without considering the small effect this aspect of the machine design has on the overall risk posed by the machinery. Additionally, small and medium-size enterprises (SME) may not be able to afford the engineering expertise necessary, leaving them in a position where they feel justified in continuing to build designs that seem 'safe enough' based on their experience.

III. CONTROL SYSTEM CONTRIBUTION TO RISK REDUCTION

Standards such as ISO 12100 [12], CSA Z432 [13] and ANSI B11.19 [14] have formalized the use of the 'hierarchy of controls' for reducing risk created by machinery. At the most basic level, the hierarchy includes hazard elimination, hazard substitution, engineering or design control methods, information for use, administrative controls and personal protective equipment. The majority of users perceive engineering controls as the safety part of machine design, and most of the measures used to reduce risks fall into this part of the hierarchy.

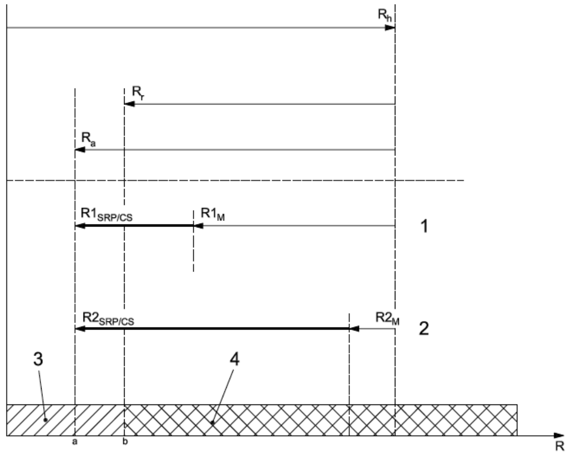
The engineering control portion of the hierarchy includes:

1) Barriers (e.g. perimeter fences, guard rails);
2) Guards:
   a) Fixed guards;
   b) Adjustable guards;
   c) Movable guards (see 3 below):
      - Interlocked guards;
      - Interlocked guards with guard locking;
   d) Mechanical restraint devices (e.g. active pull-back devices used on power presses);
3) Safeguarding Devices:
   a) Interlocks;
   b) Guard locking systems associated with interlocks;
   c) Presence-sensing safeguarding devices (e.g. optical beams, light fences, light curtains, area scanners, two-hand controls, mats, etc.)
4) Complementary Protective Measures (e.g. emergency stop systems, etc.)

The majority of the risk control measures in the hierarchy are mechanical (1 and 2 above), with no connection to the SRP/CS; these measures are often more effective and more reliable than the use of safeguarding devices. The SRP/CS affects only the measures listed in 3), having no impact on the effectiveness of the other levels. Complementary protective measures are generally excluded completely from this discussion [7, Table 8], although in many cases the same methods are applied by designers. Without the involvement of the control system, either electrically, pneumatically or hydraulically, control reliability cannot affect the effectiveness of the risk reduction.

Presence-sensing safeguarding devices are among the most noticeable control measures (3 above), since they are used at the point of interaction between operator and machine. This visual prevalence can, however, lead people to believe that these are the primary means of safeguarding operators. In many cases, the primary safeguard is the structure of a barrier fence that supports the presence-sensing device.

Figure 1 illustrates the small component of risk reduction typically achieved using the SRP/CS. Both R1 and R2 in the figure represent partial contributions to the overall risk reduction, with the initial risk reduction accomplished through mechanical means following the Hierarchy of Control. While full risk reduction is possible in many cases using exclusively mechanical measures or exclusively SRP/CS measures, these cases are rare, and most machinery is equipped with a hybrid system that incorporates both measures.



Key

R_h for a specific hazardous situation, the risk before protective measures are applied

R_r risk reduction required from protective measures

R_a actual risk reduction achieved with protective measures

1 solution 1 — important part of risk reduction due to protective measures other than SRP/CS (e.g. mechanical measures), small part of risk reduction due to SRP/CS

2 solution 2 — important part of risk reduction due to the SRP/CS (e.g. light curtain), small part of risk reduction due to protective measures other than SRP/CS (e.g. mechanical measures)

3 adequately reduced risk

4 inadequately reduced risk

R risk

a residual risk obtained by solutions 1 and 2

b adequately reduced risk

$R1_{SRP/CS}$ $R2_{SRP/CS}$ risk reduction from the safety function carried out by the SRP/CS

$R1_M$, $R2_M$ risk reduction from protective measures other than SRP/CS (e.g. mechanical measures)

NOTE See ISO 12100 for further information on risk reduction.

Fig. 1 - Overview of the risk reduction process for each hazardous situation [8, Fig. 2]

The overall effect of an undetected failure in the SRP/CS is often significant-to-catastrophic for the people exposed to the hazard. For Example, an undetected failure in a light curtain system used to protect a worker from the point of operation of a power press can lead to amputation or more catastrophic injuries for the exposed person. However, a control system failure in a nuclear power plant, or a process plant, may result in the inadvertent exposure of hundreds or thousands of people to the hazards with catastrophic results.

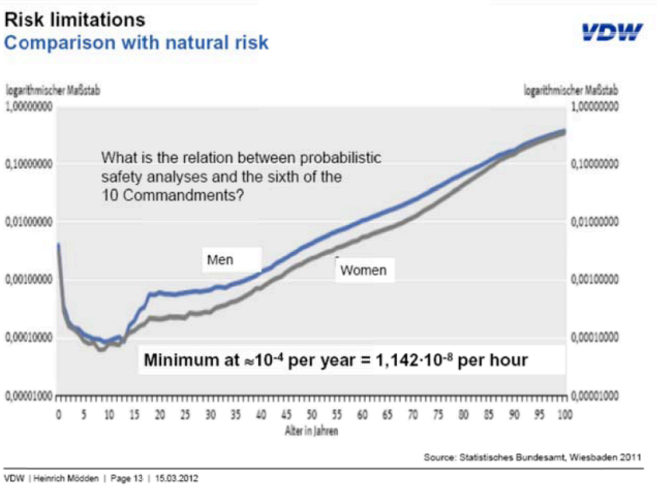
IV. Understanding the Real Contribution of SRP/CS Failures to Injuries

Considering the significant effect that a single undetected control system failure can have on risk to an exposed person, the opportunity for failure should be minimized, especially where the technology necessary to reduce the failure modes is readily available and comparatively inexpensive.

In a presentation made to ISO TC 199-JWG1 in March of 2012, H. Mödden reported on a study done by VDW in Germany [15]. In the report, Mödden showed that the number of machine-tool related injuries had fallen from more than 45,000 in 1993 to less than 25,000 in 2009, the last year for which data was available. No conclusions were given regarding the cause of this reduction or the contribution that improved SRP/CS reliability may have made to this reduction.

Defining 'tolerable risk' and 'acceptable risk' with regard to product safety is controversial at best. Current standards like [7] and [12], use figures developed in Europe as the basis for risk reduction. As a path to understanding what 'acceptable risk' might mean, Germany started by examining the death rate in the population, that is the death rate from all causes.

Mödden's report indicated that that the lowest risk of death in the general population occurs among teenagers, at approximately 1 x 10^{-4} fatalities per year, or 1,142 x 10^{-8} per hour. This death rate is shown in Figure 2. This rate is used as underlying criteria for 'acceptable risk' in existing safety standards like [7] and [8], the conclusion being that this rate is suitable as an overall target for risk reduction.


Risk limitations

Comparison with natural risk

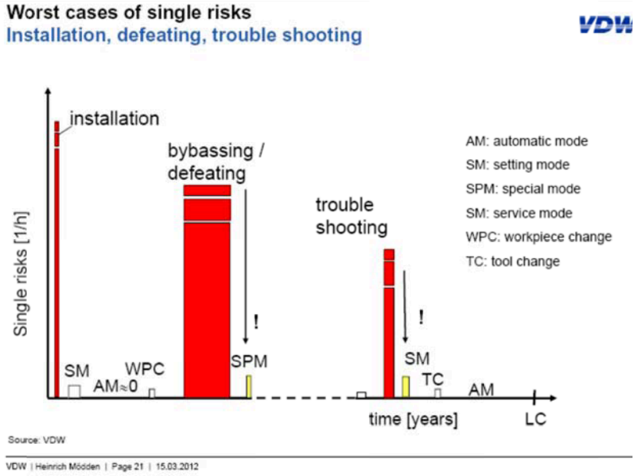
Source: Statistisches Bundesamt, Wiesbaden 2011

VDW | Heinrich Mödden | Page 13 | 15.03.2012

Fig. 2 - Comparison with Natural Risk [15]

However, using the VDW data to set the upper boundary for acceptable risk is controversial. In a 1992 report on the risks related to nuclear power stations [16], the UK HSE suggested that the lower boundary for acceptable risk to the general population was 1 x 10^{-6} 'dangerous doses' per year, and that 1 x 10^{-5} 'dangerous doses' per year represented the upper boundary. The report goes on to suggest that the upper boundary of risk tolerability for plant workers lies between 1 x 10^{-3} and 3 x 10^{-3} fatalities per year. It may be that the German data shows a higher level of 'natural risk' than that in other countries.

Mödden also showed that the most dangerous periods in the life of the equipment occurred when the the SRP/CS was intentionally bypassed for maintenance or service activities as shown in Figure 3.


Worst cases of single risks

Installation, defeating, trouble shooting

Source: VDW

VDW | Heinrich Mödden | Page 21 | 15.03.2012

Fig. 3 - Installation, defeating, troubleshooting [7].

Considering these points, the value attached to developing more reliable SRP/CS for machinery begs the question: Are we adding value, or just cost? Understanding the cost-benefit relationship is necessary to making any judgement about the need to apply these techniques. Data on many types of injuries is publicly available through OSHA databases [10] in the USA, and from Association of Workers' Compensation Boards of Canada [11]. These databases do not code SRP/CS failures as a cause of injuries or fatalities. This creates a significant problem, as it is not possible to determine the extent of the problem created by control system failures. How then can industry determine the cost or the benefit of controlling these types of failure?

The argument given in Mödden's report is a reasonable one: Reducing the risk from the use of machine tools, or any machinery, to a level similar to the natural risk of death in the overall population implies that working with these tools would then be no more dangerous than day-to-day life, but the question remains: At what cost?

To develop an analysis that would answer this important question, data is required on three fronts: The contribution of SRP/CS failures to workplace injuries and fatalities, the labour hours required to complete the design analysis and validation tasks under current standards, and the labour hours that were required for the same tasks before 1992 when the first control reliability requirements were made in machinery standards. This data is not currently available.

Anecdotally, we know that many machine tool manufacturers are spending more time now on the development, analysis, design and validation of the safety systems on their machinery than ever before. Estimates run from 15% to 30% additional hours are required for these tasks, and these numbers grow if the control system relies on in-house software as part of the SRP/CS. Not included in these estimates are the additional hours required to train engineering and design staff in the application of the standards, purchase of software tools to facilitate the analysis, additional component costs, training of manufacturing and service personnel in the use and fault-finding of the resulting complex systems, and many other factors.

For SMEs, these additional costs may be more than can be borne and still remain competitive. In these cases, many SME's will simply use a design taken from a catalog or a competitor's machine, without any clear understanding of why the system is designed a certain way or what needs to be done to ensure that it achieves the level of reliability needed in the application, resulting in misapplication of these systems.

V. Conclusion

Improving the reliability of the SRP/CS in machinery is a worthwhile target, as long as the benefits gained are not disproportionate to the cost. Without supporting data on the benefits and costs of improving SRP/CS reliability, industry currently has no way to determine if the time and money spent on this work is achieving the desired outcome. Standards are driving designer to develop increasingly reliable SRP/CS without any apparent attention given to the costs added to the machine designs. Manufacturers have difficulty finding engineers and designers with the necessary background to design these systems because this field is new, and not generally part of the engineering curriculum in post-secondary schools. The result is that costs are increased while selling prices must remain at current levels, decreasing the profitability of the machine building companies while yielding uncertain effects on risk reduction from machinery.

Until governments and other responsible bodies begin to gather data on SRP/CS failures linked to injury, this situation cannot be resolved, and manufacturers will continue to be required to implement these standards in their designs to avoid potential liability. Clearly, further study is required to determine the effects of increased SRP?CS reliability on occupational injury.

Acknowledgment

Kimberly Nix is gratefully acknowledged for her ongoing support in the creation and editing of this work, and for her continuous encouragement, without which this paper would not have been written.

Mr. Thomas J. Doyle, Industrial Safety Integration is acknowledged for the many hours spent discussing this topic.

Heinrich Mödden and VDW are acknowledged for permission to use images from his report to ISO TC 199-JWG1.

Barry Warrack of the Worker's Compensation Board of Manitoba is acknowledged for his contribution of workplace injury statistics in that Province.

Réal Boubonnière and Yuvin Chinniah are acknowledged for their previous work in this area, and their support in the early stages of the research for this paper.

References

[1] (2012, March, 23). Frank J. Sprague. [web]. Available: http://en.wikipedia.org/wiki/Frank_J._Sprague

[2] (2012, March, 24). Chernobyl Disaster. [web]. Available: http://en.wikipedia.org/wiki/Chernobyl_Disaster

[3] (2012, April, 5). Timeline of OSHA's 40 Year History. [web]. Available: http://www.osha.gov/osha40/timeline.html

[4] *American National Standard for Industrial Robots and Robot Systems —Safety Requirements*, ANSI/RIA R15.06, 1992.

[5] *Safety of Machinery—Safety Related Parts of Control Systems—Part 1: General Principles for Design*, CEN EN 954-1, 1996

[6] *Industrial Robots and Robot Systems—General Safety Requirements*, CSA Z434, 1994.

[7] *Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design,* ISO 13849-1, 2006.

[8] *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems,* IEC 62061, 2005.

[9] European Commission. *Council Directive 89/392/EEC of 14 June 1989 on the approximation of the laws of the Member States relating to machinery,* 31989L0392, [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31989L0392:EN:HTML.

[10] US Occupational Health and Safety Administration. Workplace Injury, Illness and Fatality Statistics,. [Online]. Available: http://www.osha.gov/oshstats/work.html.

[11] Association of Workers' Compensation Boards of Canada. National Work Injury Statistics Program (NWISP). [Online]. Available: http://www.awcbc.org/en/nationalworkinjuriesstatisticsprogramnwisp.asp.

[12] *Safety of machinery—General principles for design—Risk assessment and risk reduction,* ISO 12100, 2010.

[13] *Safeguarding of Machinery,* CSA Z432, 2004.

[14] *American National Standard for Machines—Performance Criteria for Safeguarding,* ANSI B11.19, 2010.

[15] H. Mödden. "VDW Research. Probabilistic safety analysis for the safety related Proven-in-Use argument.", unpublished.

[16] G. Ballard, D. Broadbent, R. Clarke, et al. Tolerability of Risk from Nuclear Power Stations. UK Health and Safety Executive. [PDF] Available: http://www.hse.gov.uk/nuclear/tolerability.pdf