HIGH RELIABILITY COMPUTING FOR CONTROL AND SAFETY*

E. Marszal, W. Goble, exida.com, Sellersville, PA USA

Abstract

Safety Programmable Logic Controllers (PLCs) are special purpose computers that are used to provide critical control and safety applications for automation users. There are serious questions though about the use of programmable systems for critical control and safety automation. How can the use of these machines be justified? This paper covers the essential attributes of safety PLCs including high strength design, excellent self-diagnostics, redundancy, and high common cause strength. When these attributes are combined with third party functional safety certification, a reliable and safe machine is the result.

1 MISSION CRITICAL CONTROL

In many industries there exists a need for mission critical control and safety systems. These systems are used where failure of the control system will cause serious problems including expensive downtime and possible hazards. Many users are looking for a control system that is reliable and safe. A system is reliable if it fails very infrequently. A system is 'safe" if it fails in a predictable way when it fails – fail-safe. Figure 1 shows a Venn diagram of system operation that includes successful operation and the two primary failure modes of a control system, fail-safe (PFS) and fail-danger (PFD).

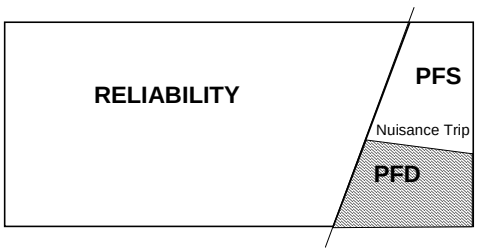

Figure 1: Control system operation/failure modes.

There are three important issues to consider when looking for a control system that is safe and reliable. These are: 1) a low failure rate – high strength, 2) predictable failure modes and 3) redundancy that is designed correctly considering high self diagnostic capability and high common cause strength.

2 LOW FAILURE RATE – HIGH STRENGTH

A fundamental concept in the field of reliability engineering is that all failures occur when some 'stress' exceeds an associated strength. The stress can be physical like humidity and temperature. The stress can be mechanical like shock and vibration. The stress can be electrical like electric surge, radio frequency interference or electro-static discharge. The stress can even be human like incorrect calibration, setup or maintenance. Usually some combination of these stresses actually causes a failure.

Following this concept further, it is theoretically possible and even practical to build equipment with very low failure rates. While it could be argued that ideal reliability is not possible, it is surprising how much strength can be designed into a product when a small cost premium is allowed by the market.

The overall effect of high strength is to increase system reliability as shown in Figure 2.

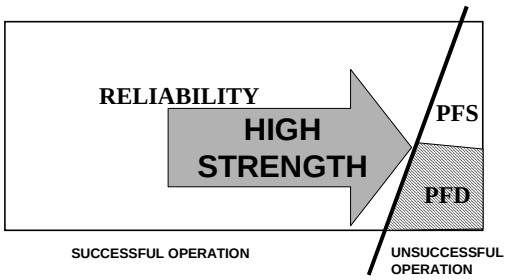

Figure 2: Effect of high strength.

2.1 Adding strength – Physical/Chemical

A number of things can be done to resist the stress of humidity and temperature. Heat sinks can be added to the significant heat producing electronic components. When junction temperatures of semiconductors are lowered, the failure rates will be lower. Circuit boards may be coated with new plastic sealants or completely encased in silicon. These techniques can be especially effective in reducing failures due to humidity, corrosive atmospheres or conductive dust.

2.2 Adding Strength - Mechanical

Failures in control systems are also caused by mechanical stress including shock and vibration. Mechanical strength is added by bracing printed circuit boards. Careful testing must be done for resonance in the frequency band of the industrial environment (rotating equipment primarily). Two piece electrical pin and socket connectors with positive latching will also be more robust against this stress.

2.3 Adding Strength - Electrical

Many consider electrical stress to be the greatest source of control system failure. Electrical stresses including

electrical surge, radio frequency interference and electro-static discharge are the main issues. Control system strength is obtained via shielded metal enclosures, surge protection components on power and I/O lines, RF bypassing and filtering. Testing must be done to insure high strength especially for electro-static discharge as protection techniques involve a proper combination of insulation and shielding against ground currents.

3 PREDICTABLE FAILURE MODES

Reliability is not enough. In many applications it is also important that the controller fail in a predictable manner. This is especially true in automatic protection applications where a fail-safe output state for the controller can be defined. These applications are called Safety Instrumented Systems (SIS).

For SIS, two primary failure modes are important. These are called fail-safe and failure-on-demand (fail-danger). For a normally energized system (de-energize to trip) a fail-safe failure is one where the controller output de-energizes and a fail-danger output is one where the controller output has failed energized. Of the two modes, the fail-danger is far more serious as the SIS protection function cannot provide its protection capability and worse yet, these failures are not revealed by a process trip.

Many control system designs use special circuitry in combination with self-diagnostic capability to convert dangerous failures into safe failures. When an internal component failure is detected, the special circuitry may disable controller outputs. This converts a potentially dangerous failure into a safe one. The overall effect of diagnostics along with special circuit design is shown in Figure 3.

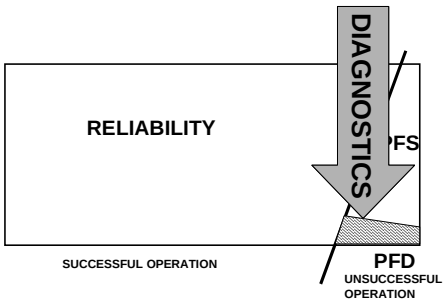

Figure 3: Diagnostic effect on controller operation.

4 REDUNDANCY

The use of redundant components has long been the solution of choice when attempting to build high reliability systems. The concepts are simple. You put in two or three controllers to do the job of one. When one controller fails, another takes over. The system remains successfully operating. When repairs can be done on the failed controller, the system can be especially effective – theoretically. But reality can be quite different. Redundancy is effective in control system designs only when the controllers have highly effective internal diagnostics and high common cause strength. The effect of redundancy under those circumstances is shown in Figure 4, an increase in system reliability.

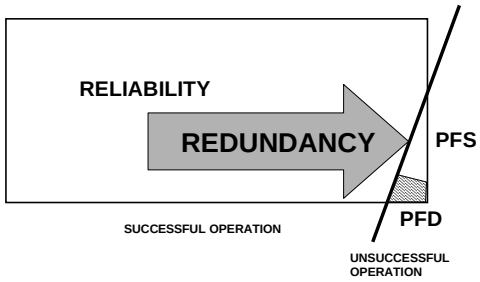

Figure 4: Effect of redundancy on system operation.

2.4 Adding Strength – Human Stress

In spite of the attempts of many good designers, "foolproofing" can be quite elusive as control system designers have sometimes wondered how smart a fool can be. Techniques such as module keying to prevent modules from being inserted into the wrong slot are effective. Other techniques include hot insert connection capability and automatic calibration.

4.1 Diagnostics and redundancy

Most implementations of redundancy in control systems involve some form of switching mechanism to select the output of a successfully operating controller to the final elements (valves). Often this switch depends on diagnostic information from the controllers to determine which output to select. What happens when the diagnostics do not detect a failure? Often that fails the system.

Consider a block controller model shown in Figure 5. Two controllers feed an output to a switch that selects an output for the system. The selection is based on two diagnostic signals that come from the controllers. If both signals indicate successful operation, the switch is free to select either output. If one output is bad, the other is selected. If both are bad, the output is programmed to either fail-safe or maintain last output whichever is appropriate to the application.

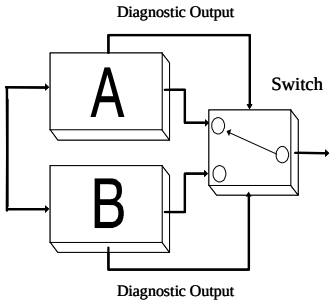

Figure 5: Redundant controller block diagram.

A Markov model of this system is shown in Figure 6. The system fails if both controllers fail, the switch fails or there is an undetected failure in the controller selected by the switch.

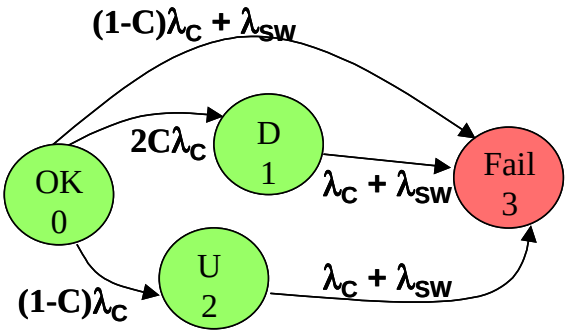

Figure 6: Markov model of redundant controller.

When this Markov model is solved as a function of C, a measure of diagnostic coverage, the results are plotted in Figure 7. That figure shows that the MTTF of the redundant system make strong gains only when the diagnostic coverage goes into the 95% plus range. A diagnostic coverage of 95% or greater takes careful design and analysis.

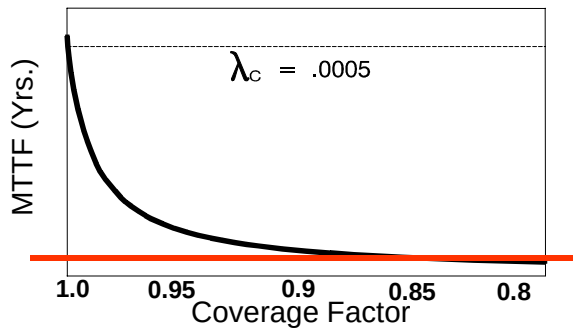

Figure 7: MTTF versus diagnostic coverage for the redundant system.

4.2 Common cause and redundancy

In many industries, especially nuclear, it is well known that stress can fail multiple components in a redundant system. This is called a 'common cause" failure. While many different models have been created to understand this limitation in redundant systems, all show clearly that if only a small percentage of the failure rate results in multiple failures, gains achievable via redundancy are limited.

A number of techniques have been recognized for reduction of common cause failures. These techniques can be grouped into categories that result in three basic rules [1]: reduce the common stress between units, increase the diversity of the design, or raise the design's strength.

RULE 1 – Reduce the Probability of Common Stress

One way to reduce the common cause failure rate is to reduce the chance of two units being exposed to the same stress. When redundant units are physically separated, there is less coupling between units and less likelihood of a common stress. Most physical stress factors vary non-linearly as a function of physical distance. Redundant units should not be physically mounted side by side. In such situations, coupling is maximized because the physical and electrical stress is nearly identical for each unit.

Programmable Electronic Systems that have redundant equipment physically separated will be less susceptible to environmental common-cause failures simply because the common environment has been reduced. This can best be accomplished by mounting redundant equipment in different cabinets.

RULE 2 – Design Redundant Units to Respond Differently to a Common Stress (Diversity)

A second common cause defense technique is "diversity." Diversity is a concept in which different units are used together in a redundant configuration. The intent is that different units should not respond the same way to a common stress. The coupling is lowered because units designed and manufactured differently will have different strengths against a common stress.

The technique has been tested and has had some success in both hardware and software. But testing has shown that design diversity does not eliminate all common-cause failures [2]. In addition, many new problems having to do with synchronization, calibration, and data mismatch due to digital round-off have appeared in examples of software diversity [3].

In terms of environmental stressors, redundant components using different technologies may increase common cause strength if the designs respond differently to a common stress. For example, a mechanical unit backing up an electrical unit (a relay wired in series with a

transistor) would be a good use of diversity. The use of "different manufacturers" of a common component may provide some benefit since this reduces the possibility of a common manufacturing defect, but significant benefits may not be achieved if both units respond to the same stress.

RULE 3 – Make the Design More Rugged (High Strength)

Equipment design attributes that lower the single unit failure rate will also lower the common cause failure rate. Design techniques that provide greater resistance to stress, such as good heat sinking, coated circuit boards, rugged module covers, and secure mechanical connectors, will lower the component failure rate because these features increase strength. If a module is less likely to fail due to a certain stress level, it is less likely to have a common cause failure. All the things that increase strength decrease common cause susceptibility. The higher the design margin, the less likely is a common cause failure.

The operation and maintenance of a system can generate common cause failures. Incorrect commands sent to synchronously operating controllers will cause both to fail. Complex operations should be automated whenever possible. Foolproofing techniques can be used for both operations and maintenance. Repairable assemblies should be keyed so that modules and connectors cannot be installed improperly. Manual calibration should be eliminated if possible.

5 CONCLUSIONS

High reliability and safety in computing systems used for control can be achieved using a combination of high strength, diagnostics and high common cause strength in redundant architectures. The best of these systems are certified per international standards such as IEC 61508 [4].

The design certification process including detailed failure, modes, effects and diagnostic analysis [5] often finds obscure design problems and helps manufacturers build even better control systems equipment.

6 REFERENCES

[1] W. M. Goble, J. V. Bukowski, and A. C. Brombacher, "How Common Cause Ruins the Safety Rating of a Fault Tolerant PES," Proceedings of the 1996 International Conference of the ISA, Cleveland, OH, June 1996.

[2] Knight, J. C. and Leveson, N. G., "An Experimental Evaluation of the Assumption of Independence in Multi-Version Programming", IEEE Transactions on Software Engineering, Vol. SE-12, No. 1, NY: New York, IEEE Computer Society, 1986.

[3] Brilliant, S. S.; Knight, J. C.; and Leveson, N. G., "The Consistent Comparison Problem in N-Version Software," IEEE Transactions on Software Engineering, Vol.15., No.11, IEEE Computer Society, 1989.

[4] IEC 61508, Functional Safety of electrical / electronic / programmable electronic safety-related systems, International Electrotechnical Commission, Geneva, Switzerland, 2000.

[5] Goble, W.M., Control Systems Safety Evaluation and Reliability, second edition, NC: Research Triangle Park: ISA, 1998.