www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 11 November, 2013 Page No. 3133-3135

“Review on Redundancy in Electronics”

Mr. Gurudatt Kulkarni[1], Prof. Mrs. Lalita Wani[2],
1 Student in Siddhant College of Engineering, Pune
2Professor in Siddhant College of Engineering Pune

Abstract-The dependence of numerous systems on electronic devices is causing rapidly increasing concern over fault tolerance. At the system level. Redundancy is a technique that has been used to improve space electronic systems reliability. The traditional implementation has been to incorporate redundancy by having the passive or active availability of two separate boxes that perform the same function. This paper argues that redundancy in engineering, should be understood as a ‘design paradigm’ that frames regulatory assessments and interpretations of all complex technical systems, profoundly shaping decisions and judgments about modern technologies. The purpose of this paper is to provide a brief overview of redundancy

Keywords- fault detection, fault tolerance, safety, soft-errors, automotive.

I. INTRODUCTION

In the last quarter of the 20th century, the word ‘computer’ became synonymous with unreliability. Whenever a system failed it was always the computer that had made the mistake. This was often unjustified and became a convenient mechanism for covering up human errors perpetrated either by the programmer or the operator. The computer became a scapegoat for our own failings and everybody was happy to put up with this situation as long as so-called ‘computer errors’ didn’t lead to injuries or death. But technology moved on, and computers became mobile in cars and then airborne, controlling non-safety-critical functions such as windscreen wipers and navigation. All that changed when flight control systems became computerised: first with military aircraft and then with civilian types such as the Airbus A320. Nowadays even cars are packed with microcontrollers and they too are taking over safety critical functions like emergency braking and airbag operation. Recently, Google has demonstrated that truly driverless cars are a practical proposition. Reliability is always of concern for protective relay systems and redundancy plays an important role for reliability. Reliability is a compromise between security and dependability. Security is the ability to properly restrain from tripping when not called for. Dependability is the ability to trip when required. While security is not improved by increased redundancy, dependability is. Clearly, the impact on the power system when a protection device is not functioning when required is much less severe when there is a redundant device that takes over the job. If the two redundant devices are of equal performance, there should be no detrimental effect at all on power system In general, the hardware redundancy system, which is to add an extra hardware with the same functions implemented in the original hardware, can be classified into static redundancy, dynamic redundancy, and hybrid redundancy system according to its architecture and function. The static redundancy system requires a voter that determines the final output of the system. The voter can use majority or average rule as its fault masking algorithm to isolate any faulty input. However, the static redundancy system tends to cost more because it requires at least three parallel modules for majority vote, and it is difficult to detect faults when two or more modules are faulty. The dynamic redundancy system achieves fault tolerance by having fault detection and reconfiguration functions instead of a voter. In general, the dynamic redundancy system can be classified into hot and cold standby dynamic redundancy system according to whether all modules are always operating or not. In the hot standby dynamic redundancy system, two modules are constantly sending their outputs, and the output switch is connected either of two modules. On the other hand, the cold standby dynamic redundancy system uses only one module at a time, and two switches are controlled by the reconfiguration module to block the signal from the faulty module. Here, the cold standby has a longer module life and better energy efficiency than hot standby because a single module is working at a time. But, the cold standby needs complex fault detection algorithm because it uses only one input value. Operations and a non-functioning device would just need to be repaired or replaced. Redundancy is one of the key requirements placed on power systems, it is particularly important for critical protection and substation automation applications. Redundant systems eliminate single points of failure and improve overall system availability, security and dependability. In order to arrive at a mathematical function for reliability, two main assumptions are made. These are that device failures are random in occurrence and are thus statistically independent, and the failure rate, expressed as so many failures per hour, is a constant over the equipment lifetime. Both these assumptions are shaky but providing certain conditions are met, they have been found to be reasonably valid for system analysis purposes. Statistical independence assumes that the failure of one component does not impose increased stress on its neighbor thus increasing their likely failure rate.

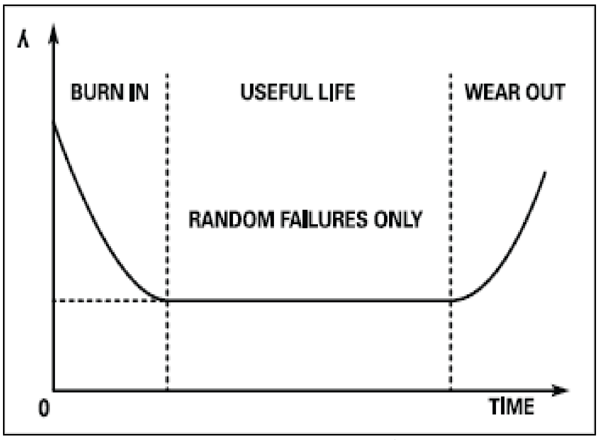

Figure1.0 Component life Failure

When computers were constructed from discrete transistors, resistors, etc, then failure short circuit failure of a capacitor, say, could cause overload of a transistor and lead to cascaded failures. Integrated circuit logic elements are less susceptible to cascading damage and should conform more closely to the reliability model.

II. REDUNDANCY IMPLEMENTATION PARAMETERS

A. Fault Avoidance

Of course, some method of determining when the system failure rate has flattened out must be found. In practice this is achieved at high cost by ‘soak’ testing the system until the burn-in phase is left. Generally manufacturers of military and some life-critical equipment are the only people who do this. With commercial and domestic systems, new products are likely to be tried out on the customer and reliability calculation adjustments based on complaints received. The Mean Time between Failures (MTBF) is often used as a reliability parameter and is simply the reciprocal of the failure rate l.

- Purpose of redundancy
  Redundancy is required for several reasons including governmental and regulatory requirements, ensure reliability, maintain customer satisfaction, increase system stability, and for maintenance purposes.
- Redundancy versus backup
  Older documents, such as The Transmission and Distribution Electrical Reference Book do not make a distinction between backup and redundancy: ―The measures employed in practice vary all the way from complete duplication of relays at one extreme to no backup at all at the other extreme.‖ However, common convention today is to define a redundant system as a second (or third) system that has essentially equal performance to the primary system applied. A backup system, while covering the zone protected by the primary equipment, will provide a lower degree of performance, e.g. less speed or less selectivity.
- Redundancy’s influence on reliability
  Reliability of a protection system is a combination of dependability and security. For protective relays, dependability is the ability to trip for a fault within its protective zone while security is the ability to refrain from tripping when there is no fault in the protective zone. Redundancy will increase dependability since the required operation can be carried out by the redundant system. A failure of a single system will not affect operation. Typically, redundancy will decrease security as the added device(s) will increase the risk for an unwanted operation. A failure (causing over tripping) of either system will produce a false trip. However, combining redundancy and duplicated devices, as in the voting scheme described in Section 4.5, will result in increased dependability and increased security. Redundancy does not influence dependability and security to the same degree. The optimal degree of dependability and security, and consequently redundancy, has to be determined based on the impact of a false trip versus the impact of lack of trip for a fault.

B. Economic considerations

Cost is an important factor in determining the level of redundancy to design into a relay scheme. The cost of the relay scheme is weighed in light of its impact on dependability, security, and reliability of the power system. The goal is to achieve optimal results at an acceptable cost. Generally, the appropriate amount of money to be allocated increases with the level of load impacted by the relay scheme, or the criticality of the load. The level of load considered increases with the system voltage of the facilities in question. Therefore, it is safe to expect that the higher the voltage class of the protection system, the greater its impact, which results in the need for increased levels of protection redundancy. It is worthwhile to allocate more money to achieve this requirement. There are of course exceptions to this ―rule-of-thumb.‖ For example, a large customer receiving power at a lower voltage distribution substation may apply funding to install a level of redundancy in order to achieve greater reliability of service. Aside from such special cases, the redundancy requirements may result in the accumulation of costs beyond those required for simply meeting the relay protection needs.

C. Asset management

Asset management can be described as ―a systematic process of maintaining, upgrading, and operating physical assets cost-effectively‖. It combines Engineering principles with sound business practices and economic theory, and it provides tools to facilitate a more organized, logical approach to decision-making. Thus, asset management provides a framework for handling both short-and long-range planning.‖ It is also considered ―a business process allowing a utility to make the right decisions on the acquisition, maintenance, operation, rehabilitation, and disposal of assets used for customer service.

D. Physical separation

One facet of hardware redundancy is the consideration of the physical location of each piece of equipment with the goal of minimizing the effects of any single physical event. Some limitations to this are obvious. All of the equipment under consideration is most likely to be located within the same substation. All of the CTs may have to be on the same breaker and maybe even be around the same bushings. Even with this in mind, some physical separation may be achieved. The goal of providing physical separation is to eliminate, as much as is practical, any single point of failure that could cause the simultaneous failure of two or more complementary relay systems. A few examples may serve to illustrate this concept. If redundant relay schemes are placed on separate panels, one scheme may survive damage from a leaking roof, mice chewing on wiring, or a worker lifting the wrong wire that disables a system.

E. Multi-Processor Modular Redundancy

Traditionally, redundancy in computer control systems has referred to the duplication (DMR or 2oo2), triplication (TMR or 2oo3) or even quadruplexing (QMR or 2oo4) of the processor units with the same program running on each in 'lock-step'. Separate comparison or voting logic only allows an output through to an actuator if a majority of processors agree. This means DMR is not fault tolerant because the voting logic cannot tell which output is incorrect, so both processors must be shut down in a Fail-Safe manner. However DMR with an SFF > 99% could still meet the SIL3 criteria. TMR allows one processor to fail with continued operation as long as the remaining two agree. (Figure.1) A QMR system should be able to handle two failures with no reduction in performance. TMR and QMR based systems should meet the criteria for SIL4 if they can achieve an SFF > 99% because they are also fault tolerant.

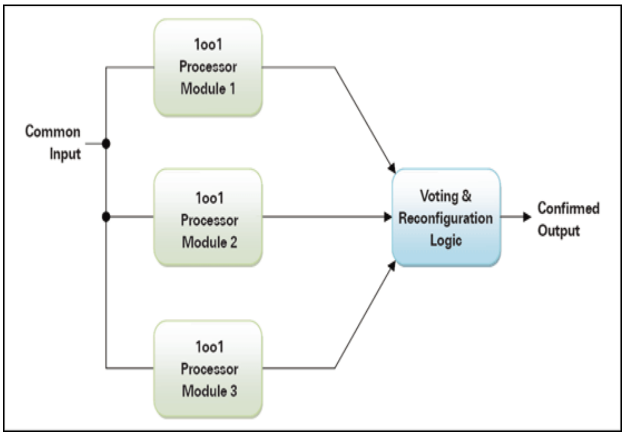

Figure 2.0 Triple Modular Redundancy

F. Static & Dynamic Redundancy

Basic modular redundancy with voting circuits is normally classified as Static, where all modules are 'hot' and running. A processor module may be ignored or powered-down when it develops a hard fault. Dynamic redundancy involves hot or cold standby spare units which are switched in and out as required by fault detection logic and/or software. Dynamic redundancy has been used extensively on the Space Shuttle [4] and Airbus aircraft [5]. In the latter example, a further precaution was taken against common-mode faults by introducing Diversity whereby processor modules are based on different microcontroller platforms with software written by independent teams. These systems feature dual processor 1oo1D modules which could now be replaced with single chips such as the Hercules dual-core devices. For example two chips could be combined to form a fault tolerant 1oo2D system compliant with SIL4. In this case both processors are 'hot' and both receive the same inputs including a common Reset. When a switch is commanded, the outputs of the standby unit replace those of the failed module. Although processor clocks are not synchronized, there should be no more than a minor glitch at switchover.

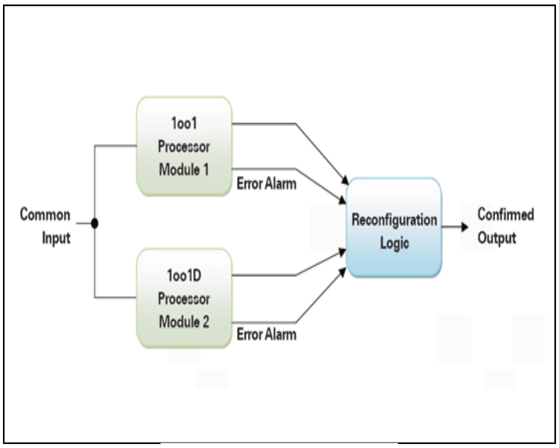

Figure 3.0 Hot Redundancy

III. CONCLUSION

By providing an active redundancy protocol and therefore a zero delay re-configuration in case of a switch or link failure, HSR and PRP are especially of interest for protection applications based on digital communication such as IEC 61850-9-2 and IEC 61850-8-1. Changing standards and expectations from new technologies are the continuing challenge for designers and users of metering instrumentation The intent of this article was to present some common redundancy implementations and to illustrate the importance of considering related failures when determining component or system reliability. The motivation for this is the fact that increasingly compact designs, based on technologies which have reduced interconnect densities, have increased the likelihood that designers will unwittingly incorporate related failure mechanisms. Related failures can have a large effect on system reliability. The standard approach of considering prime and redundant functions to be independent needs to be reevaluated in light of increasingly compact designs.

IV. REFERENCES

1. TedW. Yellman. Redundancy in designs. Risk Analysis, 26(1):277-286, 2006.IEEE 100-2000 seventh edition International Electrotechnical Vocabulary (IEC 60050)
2. David Costello, ―Fly Safe and Level: Customer Examples in Implementing Dual Primary Protection Systems‖ SEL White Paper 2007
3. NERC System Protection and Control Subcommittee of the NERC Planning Committee Technical Paper ―Protection System Reliability - Redundancy of Protection System Elements
4. IEEE Committee Report, Local Backup Relaying Protection‖, IEEE Transactions on Power Apparatus and Systems, Vol. PAS-89, No. 6, July/August 1970, pp, 1061-1068.
5. N. Oh, P. P. Shirvani, and E. J. McCluskey, "Control-Flow Checking by Software Signatures", IEEE Transactions on Reliability, vol. 51, no. 1, pp. 111-122, March 2002.
6. Sagan, S. (2004) 'The problem of redundancy problem: why more nuclear security forces may produce less nuclear security, *Risk Analysis* 24 (4): 935-46.