PROGRAMMABLE SAFETY IN THE AUTOMOBILE INDUSTRY

Fabio H. Chaves

Siemens Canada Limited, 1550 Appleby Line, Burlington – Ontario - Canada

Abstract: This paper discusses the application of state-of-the-art failsafe technologies implemented in controllers, fieldbuses and sensors/actuators specially in the automotive industry. It summarizes the results of a one-year study on practical and theoretical aspects of Safety Engineering. The discussion of multi-vendor features in hardware and software implementing fault diagnosis/failure detection and the appreciation of each one under the economical and legal point of view are supported by the experience gained during two real projects developed to automakers. Engineers and plant managers can take advantage of this study when choosing failsafe technologies to new and retrofit projects.

Keywords: Safety; Automobile Industry; Failure detection; System Reliability; Fieldbuses.

1. INTRODUCTION

Safety should be the prime objective of each and every installation that may pose risk to human beings and the environment. Any kind of industrial activity has an intrinsic risk, which can be quantified and then used to determine the safety measures to be adopted to lower this risk to an acceptable level. The major challenge has always been the determination of this "acceptable" level. Although safety should have the highest priority, the financial side is still dominant and, unfortunately, in some countries the legislation that is supposed to protect workers and the environment is milder as they should be. Indeed, there is a trade-off between the costs involved in making an installation safe enough to avoid hazardous situations or injuries and the costs that one must accrue paying fines due to injuries to workers, the environment or even downtimes due to damage to equipments. In developed countries, stricter legislations force companies to consider safety as part of new as well as retrofit projects in order to avoid being prosecuted. Many standards, for instance IEC61508, EN954, EN61131-2, CSA Z434-03 and CSA Z142-2, are available nowadays dictating how the system behaviour shall be in the presence of hazards to avoid injuries. However, it is not said how one can achieve this desired safe operation (i.e., what technology or measure shall be applied). The homepage of the Canadian Ministry of labour has many examples of fines imposed to companies whose installations were not compliant with the applicable standards, what led to accidents to operators and/or damage to the environment. Figure 1 shows a generic curve of the resulting costs due to accidents and the costs of making the operations complaint with the standards. Determining the 'cost-effective balance' is the aforementioned challenge.

Many manufacturers worldwide offer products with different technologies and the choice of the right one is not straightforward. Of course, one can choose a

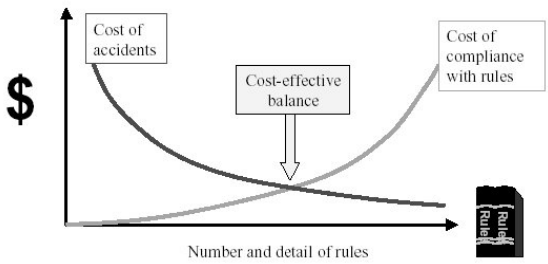

Fig. 1. The cost of compliance with rules vs. the costs resulting of accidents

fancy highly redundant control solution to a single press, what is going to guarantee a safe operation (let's say, the ram stops if the operator presses the emergency-stop button). However, one may ask a justification for choosing such extremely expensive solution (definitely an overkill to the final objective to be reached: avoid injuries). The use of fault-tolerant systems is normally not necessary if the target is not the continuous operation of a process even in the presence of faults. It seems to be obvious, but it is not. The solution required for the safe operation of an oil refinery (example of process industry) is different from the one for a press-shop in an automobile industry. Both are distinct in some points, for instance:

- An oil refinery (chemical plant) can cause catastrophic effects to the environment if the process fails, what requires a failsafe control system to keep the process operating safely, and a fault-tolerant solution to avoid downtimes, once its interruption can lead to big economic losses. Moreover, a failure could also lead the process to undesired or unpredictable states, posing danger to operators and environment. Taking as example a batch process: if the reaction in a given production step is interrupted before completion, it may be rejected, justifying the implementation of a redundant control system.
- Power press is a discrete process and rarely poses danger to the environment. Basically, the process shall be driven to a safe state (controlled stop) if the system detects any failure in hardware/software to protect the operators. It demands no redundant solution, although effective diagnostics are of utmost importance to minimize downtimes after a fault has been detected.

Those examples show how different kind of processes demand different solutions, leading to incredible cost issues during their life-cycle if a non-optimal solution for a given scenario has been chosen. There are many great documents based on research and studies of safety systems specifically to the process industry, but rarely formally devoted to the unique needs of the automobile industry. This paper intends to fill out this gap bringing only the most important results of a study, which is a comprehensive research of the many techniques that has been used so far to achieve safety in the automobile and also in the process industry. The target of this study aimed at state-of-the-art technologies and techniques available in current products of many market-leading manufacturers and at the selection of the most suitable ones specifically to the automobile industry, ranging from sensors to failsafe controllers going through safety fieldbuses. This paper intends to be a reference to anyone who needs to choose amongst the technologies available or to recycle his/her knowledge on the current trends in the safety field focusing the automobile industry.

2. SHORT HISTORICAL BACKGROUND

The automobile industry heard about PLCs (Programmable Logic Controller) for the first time in 1969, when introduced by GM to replace the relays in the control logic implementation in assembly lines. Although the PLC brought about many advances compared to the conventional relays (logic implemented in software, better diagnostic capabilities, self-documentation, etc.), the PLC was ill suited for safety (Gruhn, 1998), mostly due to the unpredictable behaviour of their outputs in the presence of failure. The PLC was the first great advance in the control technologies available to the automobile industry. However, the use of PLCs had still to remain associated with safety relays, which implemented simple interlocking functions at that time. Figure 2 shows an overview of the evolution of automation technologies throughout the time.

The main motivation to get rid of relays was the lack of flexibility on changing the logic implementation every time new vehicle models rolled out on production. The time and efforts needed to do a complete rearrange of the electrical connections specially in a largely automated assembly line was getting prohibitively high. The programmable logic has eliminated this problem. At that time safety implementations were simple and the use of safety relays was not a big deal. However, the more the safety regulations got stricter and the plants got more automated and bigger, the more the complexity of safety implementations with safety-relays increased, mostly with the necessity to change them with every new vehicle model to be produced. It was the main motivation to release the safety PLCs by the middle of 80's, known as the "second generation" of PLCs. Indeed, it was a great step towards more flexibility, shorter time-to-production and less downtimes, but another drawback was created: the necessity of specialized skills to deal with two different PLCs. They were normally from different manufacturers, with different hardware/software, fieldbuses and therefore with different ways to solve problems and deal with them. Moreover, the necessity of keeping inventory parts for both PLCs was expensive and undesirable. The third generation of PLCs is already available in the market: standard and failsafe control logics implemented in one PLC. It reduces inventory of spare parts and reduce the knowledge necessary to maintain and operate it, when compared to the traditional use of two different PLCs (standard and failsafe). Moreover, the parallel hardwired connection of field devices to the PLC I/O modules can be replaced with the direct connection of it to

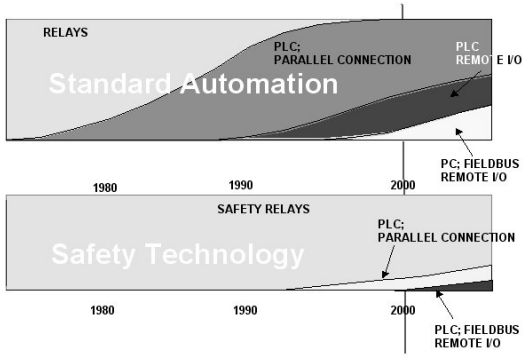

Fig. 2. The waves of automation technologies throughout the time

the safety fieldbus, what reduces wiring and problems originated thereof (short-circuit, wire-brake, etc). The use of such system offer new possibilities to the automotive industry, in terms of savings, quicker start of production, higher flexibility and better diagnostic coverage, common to safety PLCs, but now combined in one system.

Probably one may ask: "Why should a standard PLC not be considered failsafe?" Looking from outside, a failsafe PLC and a standard one can barely be distinguished from each other, because the mechanisms that make a PLC failsafe are the firmware implementation and a more robust hardware structure. Standard PLCs are built using ordinary semiconductors and electronic components (transistors for instance), which have an unpredictable behaviour in terms of which state they are going to fail in (conducting or opened). Because a standard PLC has a poorer diagnostic capability (let's say around 60%), it may not be used for safety purposes. Safety relays are known for their predictable behaviour on failing opened (over 95% of probability for good safety-relays). That weakness inherent of a standard PLC was eliminated improving the diagnostic capabilities of it (some failsafe PLCs have over 99% of coverage) and depending of their architecture (discussed on section 3) they can be safer and more or less complex hardware- and/or software-wise. Firmware is playing a decisive role in the implementation of newer architecture, permitting the construction of intelligent field devices and safer, intelligent I/O modules.
There are other classes of solutions used to implement control and failsafe logic, but they were often used in the process industry. For instance, pneumatic- and semiconductor-based systems, which are being replaced nowadays with newer redundant failsafe PLC-based systems. Please refer to (Chaves, 2004) for a detailed description about them.

3. FAILSAFE CONTROLLER ARCHITECTURES

There are many different controller architectures implemented in failsafe systems, for instance 1oo1D, 1oo2, 1oo2D, TMR, hot-backup, calculate/verify or quad redundancy – please refer to (Chaves, 2004) for a complete explanation about those concepts. However, the most cost-effective ones to be used in the automobile industry, supposing the production may stop in case of a fault (i.e., no fault-tolerant systems), are the 1oo1D and the 1oo2D architectures. Figure 3 shows the 1oo1D architecture and figure 4 the 1oo2D. The 1oo1 means "one out of one" – if one channel fails, the controller fails to operate - and "D" stands for diagnostics, because this architecture has a second layer of independently operating circuitry that checks the consistency of the signals flowing from the input up to the outputs going through the signal processing in the CPU. If the diagnostic circuitry notice that the information processed in the CPU disagrees with the one received by the output module (i.e., the CPU sent "open" to the output module, but it failed closed), this circuitry

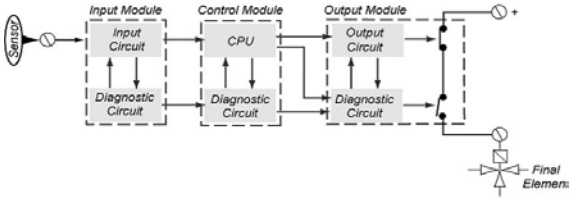

Fig. 3. 1oo1D architecture

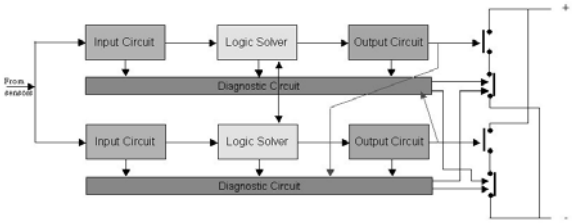

Fig. 4. 1oo2D architecture

has a relay-based output which can open the output circuit, forcing it to fail safely. The relay output ensures the circuit remains open even if it fails because on its known behaviour.

The 1oo2D is a redundant way to implement the 1oo1D architecture: if one channel fails, the other one takes over the control, although it has a time restriction (calculated based on probability) during which it can work on a one-channel structure without posing risk to anyone. Newer 1oo1D systems have a more sophisticated firmware and processor implementation that guarantee an operation even safer then the 1oo2D, but without redundancy. It means less hardware, what reduces the costs and the risk of failing. Such mechanism is called *instruction-diverse processing with time redundancy*, as shown on figure 5. This mechanism is supported by the compiler, which is specially designed to generate the failsafe PLC code twice: in bit and in word instructions, both processed with diverse boolean operators. Both instructions are executed in different parts of the CPU, each one appropriate to the kind of instructions handled (bit or word), and the results of both operations are compared number- and time-wise. If they don't match or the execution of an instruction took longer than expected (monitored by a watchdog), the CPU drives the system to a safe state. This feature along with the 1oo1D architecture is approved to the highest safety level according to IEC61508 (Safety Integrity Level 4), higher than the 1oo2D without this feature. The only drawback of this mechanism is the time spent executing the same program twice, what demands the use of a more powerful microprocessor to guarantee the response time remains within the expected range for a safe operation of the process. The non-failsafe program is executed only once as in a standard PLC. Besides these features, some other resources are used to improve the system reliability and safe operation. The safety legislation requires a complete self-test of hardware and software during operation to detect any problem. It is done at the start-up and during the normal operation in the background, testing CPU, memory, watchdogs, clocks, etc and checking the CRC signature of the failsafe software blocks.

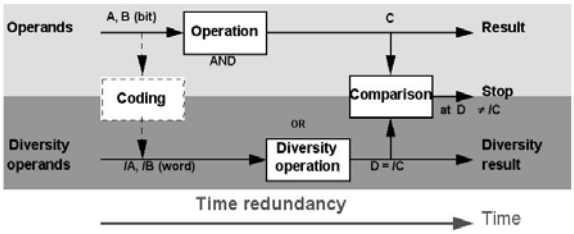

Fig. 5. Instruction-diverse processing with time redundancy

Flow monitoring is used to detect inconsistency within the program execution. During its compilation, safety-certified software blocks are inserted automatically in the code to monitor time- and logic-wise the program execution.
The 1oo1D and 1oo2D architectures are not limited to the main processing unit. The I/O modules can also have those architectures implemented aiming at the self-diagnostics, reducing the load over the main CPU and being able to operate safely (driving the outputs to a safe state, for instance) even if the communication to the CPU is unavailable. Advanced diagnostic capabilities, like short-circuit and wire-break detection, are implemented in the input and output modules to guarantee a correct behaviour. Normally, input modules have source/sinking sensor voltage supply to detect short-circuit and output modules have the "dark and light periods" feature to detect possible wire-break.

4. SAFETY FIELDBUSES

Ordinary fieldbuses are around for over 10 years connecting distributed stations with local I/O capabilities to a master station with processing capability. It made possible the elimination of the messy parallel wiring going from field devices to central stations. Despite of their versatility, ordinary fieldbuses are not suitable to carry safety-related signals, demanding the connection to safety-relays through parallel wiring. Standard fieldbuses normally lack determinism, short and known response times and also mechanisms to detect and correct the transmission of disturbed data. There are mainly four safety fieldbuses in the market: PROFIsafe, Actuator-Sensor Interface (ASI) "Safety at Work", SafetyBUS p and SafeEthernet. The aforementioned fieldbuses have a common characteristic: the availability of approved measures to ensure an error-free safety-related communication, detecting and correcting problems like: repetition, loss, insertion or incorrect sequence of packages, data corruption and transmission delay. In (Chaves, 2004) there is a detailed description of the above cited measures.

One of the first failsafe fieldbus released was the SafetyBUS p, developed on the existing CAN bus through the implementation of measures to handle communication errors. The SafetyBUS p takes advantage of the proven-in-use CAN chips applied since 1981 in embedded automotive applications, the real-time communications capabilities inherent of its event-driven behaviour, short reaction times and its noise-resistant characteristic. Despite the advantages, the drawbacks of SafetyBUS p are:
- the lack of determinism, which becomes critical when the number of bus participants grows to near its limit, turning collisions on accessing the bus into a real problem;
- short distances and low transfer rates available (3500m @ 50Kbits/s and 100m @ 500Kbits/s);
- accepts only linear topology;
- lack of gateways to other fieldbuses;
- non-failsafe bus members can listen to the bus (read-only access) but no write access is allowed;
- small size of data telegrams (8Bytes compared to 244Bytes of Profibus) causes lower data throughput;
- the use of fibre-optics does not imply in an increase in length or transfer-rate, as it occurs in other buses.

In the automobile industry, where standard as well as failsafe signals are expected to be handled in many systems, the use of two separate fieldbuses (one safety and one standard) creates extra costs as discussed in the introduction of this paper. That is one reason why SafetyBUS p is not widely used.

The Actuator-Sensor interface (ASI) was created to be a more cost-effective solution to replace the parallel wiring generated by the direct connection of sensors and actuators to the PLC I/O modules. The transmission of power and data is accomplished over the same duplex unshielded wire. In the sensor-actuator level, the quantity of data is very small, mostly binary information, but requiring deterministic behaviour, short reaction times and high transfer rates, with simplicity whilst rugged for such a harsh environment. The ASI "Safety at Work" is an extra profile added on the standard ASI bus to turn it into failsafe. It means one cable to transfer both standard and safety-related data, with standard and failsafe devices taking part of the same network. The installation of a safety monitor (a hardware device) to monitor the status of safety-related devices and ensure the correctness of the transferred data is mandatory. The unique features of the standard ASI bus implemented to transport signals, detect and correct transmission errors are so efficient that it needs just the safety monitor (and failsafe slaves) to operate safely. Devices are connected to the cable through the insulation displacement technology or "vampire" pins, making the installation of devices easy and quickly. The ASI bus has some limitations, resulting from the use it is intended to: maximum length of 300m, 31 or 62 devices per network (depending on the version) and maximum of 4 data bits per device channel. ASI is one of the best solutions to the shop-floor, due to the savings in commissioning hours, less troubleshooting efforts and less wires. Thus, representing a great solution for paint-shops, press-shops, weld-shops and others.

Profibus is one of most successful fieldbuses ever, with over 10 millions of nodes installed worldwide. Profibus has 3 variants:
- DP (Decentralized Periphery): used in the shop-floor to connect decentralized stations and field devices to a master (central) station;

- PA (Process Automation): specially designed to use in intrinsically safe areas, where explosive atmosphere is present, for instance paint-shops, refineries, some kinds of chemical processes, etc. with a transfer-rate of 31,25Kbits/s;
- FMS (Field Message Specification): not so commonly used, it was designed to connect control stations in the shop-floor to the administrative layer (office). It is being replaced with Industrial Ethernet.

Profibus has interesting characteristics, what turns it into a great choice to many applications. Transfer rates up to 12Mbits/s and length up to 23Km can be reached using fibre-optics. Copper cable allows 12MBits/s as well and the mix with optical network, what guarantee flexibility to develop customized solutions. Because virtually every manufacturer of automation solutions has field devices, sensors, actuators, PLCs and other products ready for Profibus and also gateways to make the transition to other networks, the concurrence among them makes Profibus products technologically better, cheaper and more available than products to any other network. The Profibus association decided to develop a safety profile based on the established Profibus and the result is the PROFIsafe. PROFIsafe is a profile integrally built on the existing Profibus protocol. On the top of the 7-layers OSI model used in the Profibus, a new layer has been added to implement the extra-measures necessary to make Profibus able to handle safety-related signals as a failsafe bus. Therefore, PROFIsafe works along with Profibus on the same cable. Failsafe and standard devices work connected to the same bus. It has a big impact on costs, once it protects previous investments in standard Profibus devices and cable. Moreover, the maintenance team just needs to learn about the extra features in hardware and software to deal with the new failsafe products (keeping the previous investments on Profibus training) and adding only new products to the inventory.

The PROFIsafe implementation on the existing Profibus is possible because of its inherent determinism and short reaction times. The determinism of Profibus is due to its master-slave polling procedure, which takes always the same amount of time for a given number of bus members. The size of the message can be variable to better suit the kind of transferred data: 16 bytes to simple safety-related bus members or 128 bytes to complex field devices, what improves the bus performance. Both Profibus DP and PA support PROFIsafe, so that the entire shop-floor can have a failsafe operation using gateways to connect portions of both networks. Figure 6 shows failsafe and standard devices connected to the same network (Profibus with PROFIsafe profile).
One of the most remarkable advantages of using Profibus-based solutions is the possibility of a seamless and gradual migration to newer technologies, whilst saving the previous investments.
It is fact that (Industrial) Ethernet will be the next generation of fieldbus, being extended from the office up to the shop-floor, due to its low-cost, well-

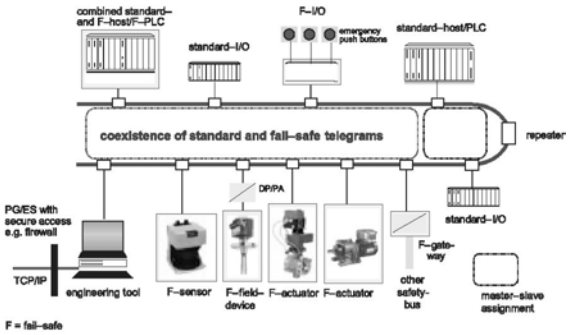

Fig. 6. The coexistence of failsafe and standard devices in a Profibus/PROFIsafe network

known simplicity and high transfer rates (10/100/1000Mbits/s). But much more has to be done to bring it to the shop-floor. First of all, Ethernet is proven-in-use in the mild office environment and has to be improved to resist to dirty, electromagnetic interference and noise present in the shop-floor. Moreover, there are rarely field devices (sensors, actuators) available to this bus. The Profibus Organization is working on a new concept called PROFInet. PROFInet is a new engineering concept that has emerged as a result of the trend in automation technology towards modular, reusable machines and equipments with distributed intelligence. It proposes the use of Profibus along with Ethernet while field devices are not ready to Ethernet. IT standards are used and mirrored to the Profibus network portion through the concept of proxies. While new Ethernet-ready devices are made available, the transition can go forward until the total elimination of the Profibus network. This scenario will take a long time to happen, but the investments are protected and the Engineering is made easier with this new approach. Instead of programming during commissioning, one needs just to configure the system using a single software tool and the PROFInet technological module containing the machine functions and properties delivered by the machine builder. One just needs to load the module in the configuration software and connect to other modules to compose the operations-flow of the entire plant. Figure 7 shows this engineering concept.

In the middle of 2005 the PROFIsafe profile will be available to PROFInet, extending the safety-related data transfer capabilities to Ethernet.

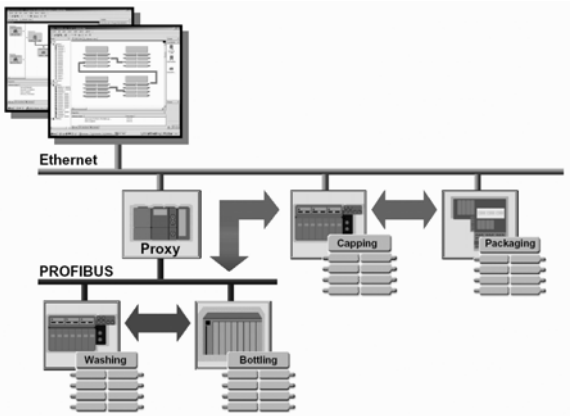

Fig. 7. The PROFInet plant engineering concept

Ethernet lacks determinism, what is a hurdle to the transfer of safety-related data. PROFInet will solve this problem dividing the data transmission in 3 channels (as per figure 8) over the same cable:
- An open channel for TCP/IP: used to transfer data without need of determinism, for example, values to be displayed in a panel;
- A soft realtime channel: deterministic to transfer safety-related data (used by PROFIsafe);
- A realtime channel: ideal for synchronous data transfer, for instance in motion control.

The PROFIdrive concept will merge into PROFInet to take care of the realtime channel, using it to promote synchronization of many axes with minimal overhead, essential to precisely control drives in position and velocities, for instance in the pulp and paper industry.

Some manufacturers are supporting the introduction of the SafeEthernet network in the market. It is based on the standard Ethernet hardware (routers, switches and cable) adding the implementation of measures to detect and control possible transmission errors of safety-related data. Although the implemented measures are very similar to the ones available in the PROFIsafe, they seem not to be open-source. This possible proprietary approach is not interesting, once it avoids other manufacturers to develop devices ready to this technology or even to improve the technology itself. The use of numerous routers and switches in parts of the network is sometimes necessary to make it deterministic depending of the number of bus members. Ethernet is non deterministic by nature because of its bus-access arbitration method, and determinism is a requirement to be fulfilled by a bus if used in safety-related applications. In the same case of PROFInet, the inexistence of field devices ready to this network makes the use of Profibus necessary. Some manufactures are pushing hard towards the development of Ethernet-ready field devices, but it going to take long to replace all the Profibus devices available with the same quality and price level. Despite the difficulties to be overcome, SafeEthernet has special characteristics, like the transmission of data in long distance, even using satellite to link two plants within the same country or in different continents. Experiments have shown that the determinism is lost transmitting over in very long distances, although the safety-related data is transmitted without errors. The transmission of safety-related and standard data is also supported over the same media. The transmission of large amount of data in high transfer rates makes Ethernet-based networks very attractive to the current growing amount of information to be transferred back and forth between shop-floor and the business (office) layer, both supported by the Manufacturing Execution System in between.

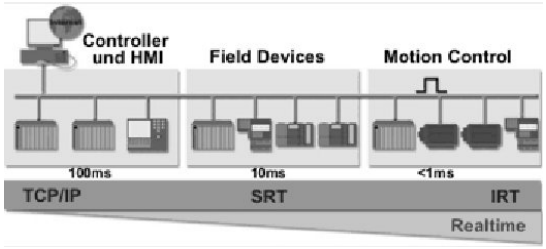

Fig. 8. The different integrated profiles of Industrial Ethernet according to PROFInet

5. FAILSAFE SENSORS AND ACTUATORS

Intelligent sensors and actuators are implemented with microprocessor, making them able to execute self-diagnostics (self-test routines) and to handle safety-related data. Two special safety devices often used in the automobile industry are laser scanner and light curtains. Both are opt-electronic devices with failsafe capabilities, used to guard hazardous areas from access of personal when the protected equipment is in operation, for instance a press or a robotic cell. Current versions are available with interfaces to many fieldbuses, like Profibus, ASI etc.

6. CONCLUSIONS

The huge amount of technologies, products and manufacturers make the choice difficult. The automobile industry has special needs and a careful analysis of the technologies available in the market before projecting a new installation or to retrofit one can be the key to the success regarding maintenance, upgradeability and operation costs of an installation. As per the discussion in this paper and the results shown in the study presented on (Chaves, 2004), the tendency to the automobile industry points towards the use of open standards that can handle both standard and safety-related data using the same hardware and can be seamlessly migrated to Ethernet-based solutions in the future: Profibus-based technologies (PROFInet, PROFIsafe) along with simpler, more cost-effective failsafe architectures (for instance, 1oo1D with instruction-diverse processing with time redundancy).

REFERENCES

Chaves, Fabio H. (2003). *PROFInet: The Totally Integrated Automation concept of the future – An introduction about the theme with a practical approach.* Document developed for Siemens Canada Limited, Burlington, ON, Canada.

Chaves, Fabio H., (2004). *The Application of Flexible, Modular 'Control Reliable' PLC Solutions in the Automotive Industry: A Theoretical Approach with Case Study*. Chapters 3 and 4. Graduation Thesis developed at Siemens Canada Limited, Burlington, ON Canada. Presented and evaluated at Federal University of Santa Catarina, Brazil.

Gruhn, Paul (1998). *A Salesman's Guide to Quadlog*. Moore Products Co. Sumneytown Pike Spring House, PA, USA.