

A High Functional Safety Performance Level Machine Controller for a Medium Size Agricultural Tractor

Massimiliano Ruggeri, Carlo Ferraresi, Luca Dariz, and Giorgio Malaguti
IMAMOTER

ABSTRACT

Functional safety requirements and solutions are more expensive when it comes to lower cost machines with less power but same functionalities with respect to big machines. The paper will show a real Electronic Control Unit (ECU) design of a machine controller, controlling both engine working point, transmission, and other utilities like PTO, 4WD, brakes and Differential Lock; the ECU was designed in accordance to ISO 25119 regulation, to meet AgPL = C or even D for some functionalities. The unit is a fully redundant electronic control unit with two CAN networks and some special safe state oriented mechanism, that allow the Performance Level C with less software analysis requirements compared with traditional solutions. All safety critical sensors are redounded and singularly diagnosable, all command effects are directly observable and most of commands are directly diagnosable. With a minimum extra-cost the hardware category for the most critical controls was brought to the category 4, thus theoretically allowing the Performance Level D achievement. But the most unseen solution was to include this unit in the dashboard, thus creating a smart dashboard and machine controller, with an important machine cost reduction. The paper will explain all technical solution, analyzing functionalities and showing the most interesting problem solutions. The hazard analysis and the functional assessment results will be briefly exposed.

CITATION: Ruggeri, M., Ferraresi, C., Dariz, L., and Malaguti, G., "A High Functional Safety Performance Level Machine Controller for a Medium Size Agricultural Tractor," *SAE Int. J. Commer. Veh.* 7(2):2014, doi:10.4271/2014-01-2421.

INTRODUCTION

The growing importance of electronics control systems for Agricultural Machines and Construction Equipment demands new architectural approaches in the design, that must be oriented to the functional safety considering the highly dynamic operational environment of these vehicles, where many different types of users are involved, causes even small failures in their systems to probably result in accidents with fatal consequences. Different international directives have changed during the years and since the 2014 all the agricultural machines, with the exception of the tractors, must follow the new ISO4254 [5] that recalls [3], but is necessary to make an effort for what concerns the functional-safety in the design of the newer machines, in order to be compliant with [3], that is going to be officially implemented in the 2016.

Both process and design needs are covered by the functional safety standards, starting from a preliminary analysis of the possible hazards in order to identify the related Performance Level (PL) of each hazard, based on the probability, controllability and severity. This risk analysis is actively used for the product development to design architectures that can prevent fault conditions or reduce the risks due to malfunctioning behavior of electronic systems. This classification of hazards, described in [1,3], makes difficult to

realize a general purpose approach that can be reused, therefore, for what concerns the Agricultural and Constructions machines, it can lead to an high expenses increase because the costs are usually distributed on small series. Moreover these machines operate in many different environments so the hazards analysis is rather time consuming and a big part of the development project.

This paper deals with the architecture and the design of electronic control for agricultural machines that integrates the management of a wide range of safety-related functionalities, such as engine working point, the transmission control, brakes and HDL system, Cruise Control, PTO and hitch quick raise/lowering. All these functionalities was designed in accordance to [3] whose key principles will be later introduced in this paper, and some mechanisms have been implemented to allow various recovery levels in order to reduce the software overhead at the price of a minimum hardware extra cost. The proposed architecture provides a full redundancy on the safety-critical controls, and is equipped with two microcontrollers. Furthermore all the safety related sensors, as well for the commands, are redundant and singularly diagnosable. In case of fault, the system is driven in a "fail silent" state, deactivating some functionalities, providing a minimum operational level, depending on the nature and

gravity of the fault. The architecture presented in this paper moves a step further in the definition of a cost-effective ECU for Agricultural and Construction machines because it has been integrated in the dashboard, realizing a smart dashboard with machine controller that covers the requirements demanded by the upcoming ISO25119 standard. The proposed approach is suitable for small-medium sized machines and it can be reusable for different applications since it embed a rich set of functionalities in a unique device. In this paper will be explained what the state of the art imposes for the electronic components design and how the functional safety requirements must be implemented to achieve an adequate PL.

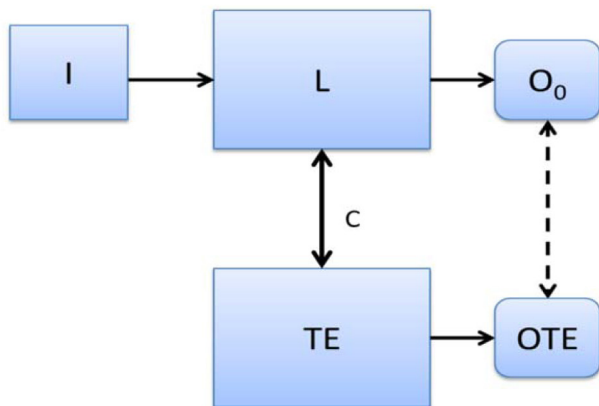


Figure 1. Hardware category 2 scheme

SAFETY PRINCIPLES INTRODUCED BY STANDARDS

The standards that involve functional safety, such as ISO25119, rather than impose constraints and solutions, introduce some general principles that lead the designers through the evaluation, development and test of the systems. These principles can be summarized in:

1. Safety,
2. Reliability,
3. Redundancy,
4. Diversity,
5. Fault detection.

The term *safety* involves the definition of the “safe-state” where the system is driven in case of faults, in order to minimize the risks and to avoid further hazards. The identification of a safe-state is a critical task because some systems must provide a *fail-silent* approach, so they can be deactivated in case of failure, while others must retain the same functionalities (*fault-tolerant*) or a subset of them (*failure-operational*).

The *reliability* comprises the PL estimation, based on several factors, such as the MTTF of the components, the diagnostic coverage (DC) and the hardware category of the system. This classification only covers the channel responsible of the safety-related functions rather than the entire system. The

demanded PL can be achieved with different strategies, evaluating the optimal trade-off between these factors. Regarding the agricultural machines, the PL C is the standard required by the channels that operate on electro-mechanical or hydraulics systems. This level can be reached both with lower hardware categories but “well-trying” components, or with higher hardware categories without the need to provide a full software safety certification.

Regarding the *redundancy*, ISO25119 defines several hardware category that can cope with the safety requirement of the applications. For instance an hardware category 2, as showed in [fig. 1](#), is composed by an electronic programmable block L that operates on the signals from the input block I, in order to drive the output state of the block O. In the architecture is also reported a supervisor block, the Test Equipment (TE) that monitors the input stage, the logical block and the output, enabling or disabling the outputs through the Output Test Equipment (OTE). The adoption of diagnostic blocks or signals allows to extended the *fault-detection* capabilities, identifying malfunctioning and configuring the system in the safe-state. Nonetheless, to achieve the highest PL, a complex architecture should be used, such as the hardware category 3 and 4, showed in [fig. 2](#). These are usually implemented in fault-tolerant systems because they ensure the operational state even in case of faults. The components are replicated in both channel paths and, in addition to this, the outputs are monitored by feedback signals detecting unexpected behaviors and extending the diagnostic coverage. The difference between a category 3 and 4 resides in the MTTF of the components and in the diagnostic coverage of the system.

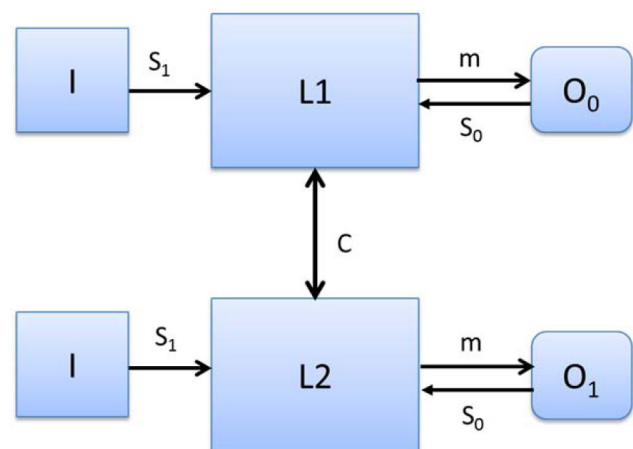


Figure 2. Hardware category 3-4 scheme

The redundancy concepts itself is not sufficient, since systematic errors could afflict the same redundant components, thus it is important to bear in mind the *diversity* principle, that impose the use of different hardware/software for the electronic components, different output characteristics for sensors and path to route the signals. In this way the system is resilient to systematic faults.