Mowers to the limits

Lorenzo Fraccaro and Antonio Silvestri (Autec Safety Remote Controls)

Cleaning vegetation in hazardous environments that are close to roads, rivers or railways lines, requires heavy-duty mowers capable to move on steep slopes and uneven ground. The operator usually drives the mower by control means installed on the machine, thus being exposed to physical risks and to uncomfortable working conditions. The need to protect the operator from risks and provide a comfortable point of control became paramount and has been solved by use of electronics. A specifically designed wireless control system has solved safety and control issues by removing the operator from the machine and providing all the maneuverability required by the application. The radio control interface has been studied in cooperation with the mower manufacturer to independently adapt track speed to different slope inclinations by real time adjustments from the portable console. The use of a wireless control system with safety functions certified according to ISO 13849-1 (PL d / e) provides an increased level of safety. The solution, originally employing a radio control directly interfaced to hydraulic valves, has now evolved into a system based on a simple CAN network with improvements in flexibility, diagnostics, size and cabling.

In recent years, safety remote controls specifically designed for mobile hydraulic applications has helped increase the productivity and safety level of many applications. The availability of radio control systems certified for functional safety by independent bodies provides a high level of confidence for OEMs and end users.
The example presented here involves a tracked vehicle for which we developed specific solutions. The vehicle is suitable for civil applications such as professional mowers and for military applications such as mine clearers. The solutions employed has been successfully implemented in bigger and more complex machines, providing a safe and reliable remote control.

Environment description

The mower manufactured by our customer has been developed for the maintenance of motorway or railway embankments, steep riverbanks, roundabouts, etc. Keeping these kind of areas clean used to be a labor-intensive and time-consuming task. In addition, those activities are often carried out in potentially hazardous areas or in dirty conditions.

The requirements and features of the mower can be summarized as follows:

- ability to climb slopes up to 55° requires high-grip track technology
- movement in confined space requires high maneuverability
- command responsiveness requires a remote control system with short lag
- operation from a safe distance requires a remote control with a range of up to 150 m
- different working conditions require the ability to mount and control a range of tools.

Figure 1: the mower working on a steep slope

Figure 2: mine clearer

Use of a radio remote control improved working conditions allowing the operator to stay a safe distance away from the working area.
The radio remote control safety functions are available to the operator on the transmitting unit whenever a potentially dangerous situation may occur.
Data from the machine are accessible from the graphic display on the portable control unit.

Figure 3: radio remote control for the mower, with and without display

The mandatory tasks given to us by our customer were:

1) the ability to move forward and backward with variable speed,
2) the ability to turn left and right during forward and backward movement and with variable turning radius,
3) the ability to turn CW / CCW on the vertical axis with variable rotational speed.

These mandatory tasks have been achieved by a specific “crawler” function implemented in the remote control. The function automatically manages the direction and speed of the tracks, depending on the position of the joysticks. Two options were required: one with two joysticks and one with a single joystick. In the former, the left joysticks sets direction and speed, the right joystick sets the turning radius. In the latter, a single joystick controls all parameters.

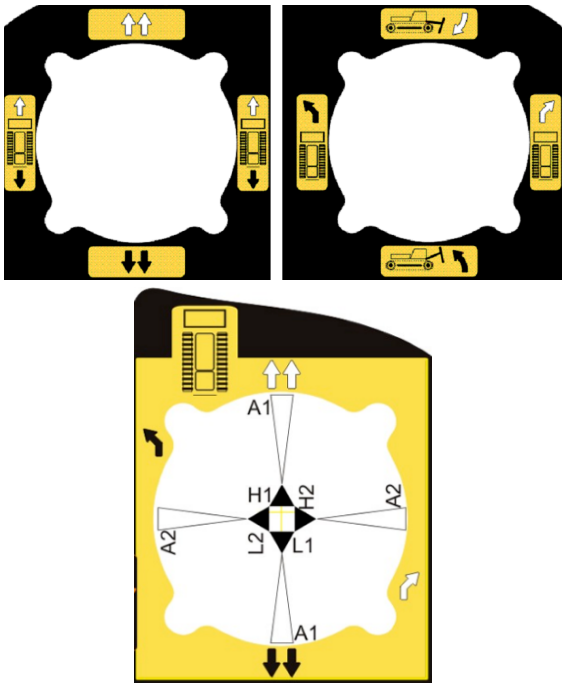


Figure 4: track control can be made by either a dual joystick configuration or a single joystick configuration

The final solution took advantage of the configurable logic provided by the receiver unit of the remote control. The receiver unit directly drives the crawler’s hydraulic

valves by means of voltage signals. The logic was also useful to prevent undesired change of directions that could possibly cause abrupt rotations of the mower on its axis at full speed.

While travelling on steep slopes the mower can side slip, due to the gravity. To maintain a straight direction, the downstream track must travel at higher speed than the upstream track. The original mechanical solution was rather complex adding costs and reducing reliability. Even in this case, the configurable logic of the remote control offered a simpler solution. Now a potentiometer on the portable unit allows the user to dynamically adjust the relative speed for the 2 tracks and maintain a straight direction.

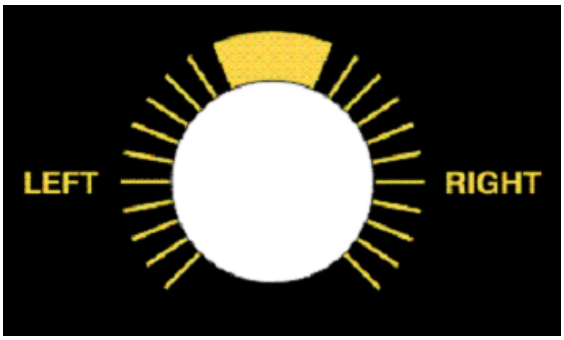


Figure 5: adjusting the relative speed of the tracks is made by rotating a potentiometer on the portable unit.

Controlling the vehicle while it is travelling in the direction of the user is not simple because the user reference system and the mower reference system are rotated by 180° around Z axis. In this case, “right” for the user means “left” for the mower and vice versa. This results in a counter intuitive association between joystick movements and vehicle movements, which was resolved by a “track swap” function, activated by a switch on the portable unit.

Figure 6: “track swap” function reverses the meaning of “right” and “left“ for the vehicle.

Different vegetation conditions -such as thickness and height- require different speed ranges for the mower. Therefore another function was needed to select the maximum speed value while maintaining the precision given by the full travel of the joystick. The user decides the maximum speed by means of a potentiometer on the transmitting unit.

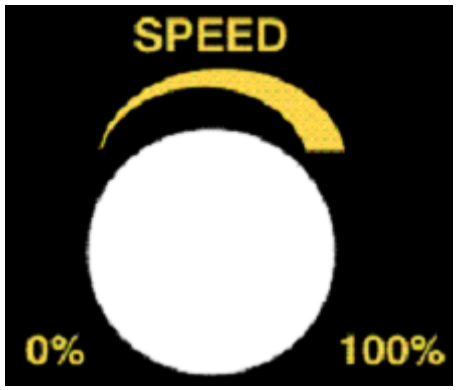


Figure 7: different maximum speeds that are selected by rotating a potentiometer on the portable unit.

Taking advantage of the bi-directional radio link, the user checks the relevant machine parameters in a graphic display located on the portable unit. Parameters like temperature, fuel levels, lubricant levels, cutting settings can be seen. All parameters are collected via CAN bus by the remote control fixed unit and sent to the portable unit.

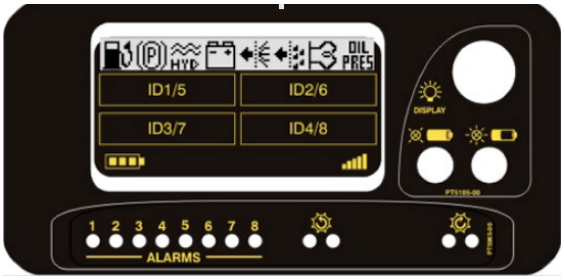


Figure 8: user checks vehicle parameters on the graphic display

The vehicle functions for the mine clearer application are more or less the same as the mower application. For smaller mine clearers, the remote control includes additional commands to control the gripper, that are not needed for the bigger version of the mine clearer. In both cases, the range of the remote control has been extended to one mile, to be sure the operator is clear from the mine area.

The solution has evolved toward a control unit that is external to the remote control fixed unit which communicates via CAN bus. All logic described previously is now implemented by the control unit, allowing a much smaller remote control receiver with only a CAN bus interface and the safety relevant outputs.

Fail-safe radio remote controls

As a minimum, the radio remote controls for these applications must be equipped with a safety related function to bring the machine to a safe state. For example, the safe state of a machine is when the engine is stopped. The ability to stop or bring a machine to a safe condition is mandated by the European Machinery Directive. The “stop” function of the remote control is triggered by pressing the stop pushbutton on the portable unit and causes the de-activation of corresponding output(s) in the fixed unit.

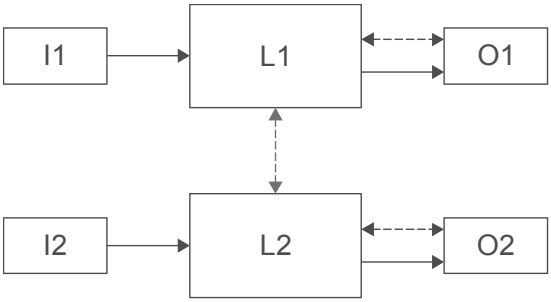
Depending on the risk analysis of the machine, this function may require a Performance Level between “c” and “e” according to EN ISO 13849-1 and / or a SIL between 1 and 3 according to EN IEC 62061. These safety standards can be understood as: the ability of stopping the machine can’t be compromised by a single fault, a glitch or a disturbance. This problem is addressed by implementing the measures specified either in ISO 13849-1 or IEC 62061 standards, among which are:

- Redundancy and diversity
- Diagnostics and self-monitoring
- Reliability of components.

Redundancy and diversity

A predictable hazardous fault for a radio remote control system is that the Stop output does not turn off when required, for example due to a welded relay contact. Providing two stop outputs, the machine can still be taken to a safe state with the redundant output. This principle applies wherever a single failure may compromise the safety of the stop function: the contact of the stop button, the microprocessor that encodes or decodes the stop messages, the relay that energizes the machine. A redundant system has at least a “dual channel” structure: dual inputs, dual elaboration, dual outputs.

Nonetheless, some failures may affect both channels and are thus called common cause failures (CCF). For the tracked vehicle application, the most relevant causes were temperature and vibrations. Others are EMI noise, over-voltages and software errors. CCF can be tackled by selecting different components for equivalent functions in the two channels. For example, different microprocessors are affected in different ways by temperature, reducing the probability of a common cause (the temperature, in this case) to compromise both microprocessors.



I1,I2 = redundant inputs (switches, sensors …)

L1,L2 = redundant elaboration (PLC, processors …)

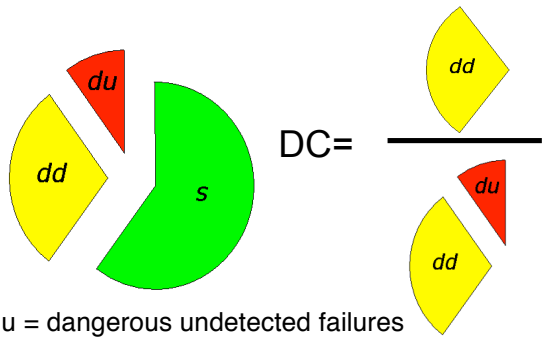
O1,O2 = redundant outputs (tranistors, relays …)

Figure 9: Example of a redundant system: dual channel architecture

Diagnostics and self-monitoring

If there is no indication that the one stop output has failed, the radio control can operate without the protection of a second stop output. A manual inspection may reveal the problem, but it is impractical to schedule close enough maintenance intervals to ensure that a fault is detected before a second fault occurs.

The system must be able to detect the failure and prevent the machine from operating while only one stop output is operational. The ability of the system to self-diagnose dangerous faults is measured by the Diagnostic Coverage (DC), the ratio of dangerous faults detected by the system over all dangerous faults.



du = dangerous undetected failures

dd = dangerous detected failures

s = safe failures

Figure 10: The diagnostic coverage is the ratio of dangerous detected faults over all dangerous faults.

Reliability of components

A component is said to be reliable if the probability of failing during its mission time is low. Safety functions cannot be built around unreliable components. Consider the dual relay outputs for the stop function. If the reliability of the relays is low, the higher will their probability of failing be. The probability of both relays failing is lower than the probability for a single relay to fail, being the product of the single probabilities that are a number less than 1:

P(both relay fail) = P(relay 1 fails) x P(relay 2 fails)

For example, if the probability of failure for a single relay is 0,01, the probability of simultaneous failure for both relays is :

P(both relay fail) = 0,01 x 0,01 = 0,0001

Nonetheless, with unreliable components the probability cannot be neglected and may compromise the redundancy principle: if both relays fail simultaneously there is no second chance to stop the machine.

For safety systems, the reliability of components is measured by the “mean time to dangerous failure” or MTTFd. This value represents the time resulting in the dangerous failure of 63,2% of the whole population of components.

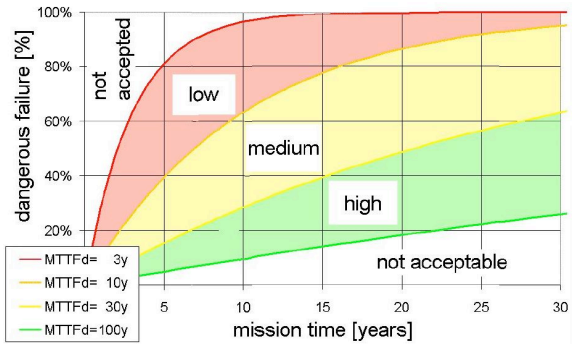


Figure 11: When MTTFd has elapsed, it is likely that 63,2 % of the components have failed dangerously.

Reliable digital communication

The portable unit accepts operator commands from actuators such as pushbuttons or joysticks and encodes these commands into a message that is sent to the fixed unit. The fixed unit decodes it and performs the commands that it was given. In most cases, these messages are sent over a radio link that is exposed to several hazards:

- Communication errors due to EMI noise
- Controlling the wrong machine
- Long response time of commands.

Communication errors

The commands sent by the transmitter must be correctly understood at the receiver side, any corruption of the messages should not result in erroneous machine motion. Each message includes an error-checking code so that the receiver can ensure that the message was received correctly. For a coding system to be effective, a small change in the commands shall cause a large change in the code.

COMMANDS	CODE
... 0000 0000 ...	D2E3402BA05D
... 1000 0000 ...	7FA4D3C0E109

Figure 12: A small change in the commands results in a big change in the error checking code.

This minimizes the chance that two or more errors could cancel each other out, and make a damaged message appear valid. The number of simultaneous errors needed to defeat an error-detection system is a measure of its effectiveness, and is called Hamming Distance.

Unique identity codes

In a radio remote control application, we can never guarantee that the receiver will not be exposed to messages being transmitted by other remote control systems. The use of proprietary telegram protocols protects against interference from other types of systems.

To ensure that the user only controls the correct machine, different radio systems must be distinguished from each other by each having a different ID number, common for each receiver / transmitter pair. One common method is to use small switches to set the code number in the transmitter and receiver. A safer approach is to assign an ID code to each system guaranteed unique by the manufacturer and stored in a sealed module to prevent tampering.

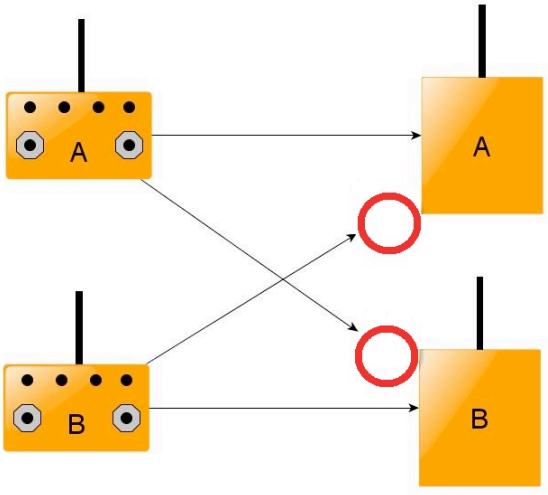


Figure 13: Commands are neglected by fixed unit if they do not originate from the correct portable unit

Response time

For applications like the mower and the mine clearer, response times in the range of 100 milliseconds are required for safely controlling the machine and to be perceived by the user as instantaneous. The response time of a radio remote control is determined by the data rate which depends on the radio hardware, the noise level and the frequency spectrum crush.

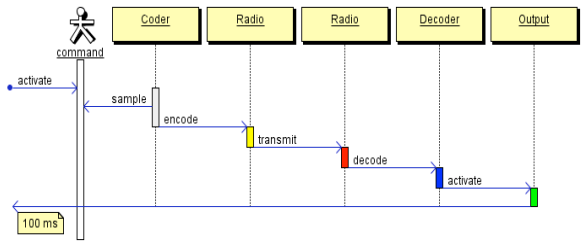


Fig. 14: Commands response time shall be in the range of 100 ms

The latter is becoming the main issue lately and may be tackled by automatic channel management strategies that require a transceiver in both portable and fixed units. The transceivers continuously monitor the traffic on each channel, and switch to the least congested among them. Nonetheless, the actual response time may increase due to interference causing some telegrams to be damaged, and thus rejected.

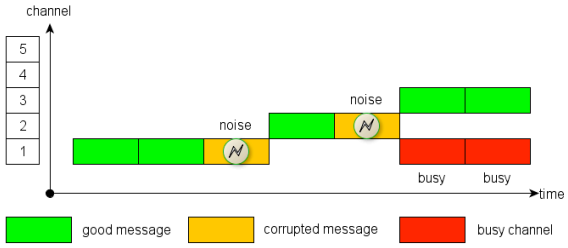


Fig. 16: Channel management reduces delays and eases coexistence of multiple remote controls

After a predetermined amount of time has elapsed without a valid message from the portable unit, the fixed unit must perform a stop and bring the machine to a safe state. As required by EN IEC 60204-32 this time can be between 0.5 and 2 seconds.

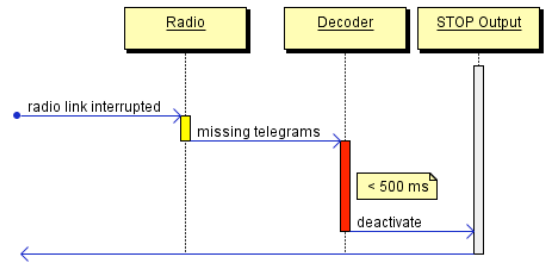


Fig. 17: Definitive loss of radio link triggers an automatic stop

Conclusions

The addition of a wireless remote control to the tracked vehicle improved the safety of the user and its working conditions. The configurable logic of the outputs reduced system complexity, replaced previous mechanical solutions, eased machine commissioning and operation. The availability of a CAN bus on the fixed unit allowed to collect machine data then displayed to the user and further reduced the complexity of the application.

Lorenzo Fraccaro
Autec srl
I -Via Pomaroli, 65 – 36030 Caldogno VI
+39 0444 901000
+39 0444 901011
l.fraccaro@autecsafety.com
www.autecsafety.com

Antonio Silvestri
Autec srl
I -Via Pomaroli, 65 – 36030 Caldogno VI
+39 0444 901000
+39 0444 901011
asilvestri@autecsafety.com
www.autecsafety.com

References

[1] CiA DS 301, CANopen application layer and communication profile
[2] CiA DSP 302, Framework for CANopen managers and programmable CANopen devices
[3] ISO EN 13849-1 Safety of machinery – Safety-related parts of control systems
[4] IEC EN 62061 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
[5] IEC EN 60204 Safety of machinery – Electrical equipment of machines