Journal of Scientific & Industrial Research
Vol. 79, December 2020, pp. 1074-1079

Practical Design of Electronic Emergency Stop Devices for Machine Safety

J Alvaro Fernandez-Muñoz*, J Ignacio Suarez-Marcelo and M Dolores Moreno-Rabel

Dept. Ingeniería Eléctrica, Electrónica y Automática, Universidad de Extremadura, Badajoz, Spain

Received 24 February 2017; revised 16 October 2020; accepted 03 November 2020

A variety of safety protective devices (SPDs) are currently available on the machinery safety market. SPD complexity and cost depend on the safety feature implemented as required for a specific piece of machinery in its working environment. However, one type of inexpensive SPD is mandatory for many types of machines: the emergency stop device (ESD). This paper introduces a novel ESD recently developed by the authors. This electronic ESD is capable of automatically performing emergency stop actions as commanded by a suitable external supervisory safety system connected to it, which may replace or reinforce the human action expected for the provision of safety. In addition, the device allows integration with any emergency stop circuit already designed for machinery by means of configurable features. Both practical design and implementation issues are discussed in detail through a fully exemplified concept-design-prototype-validation procedure.

Keywords: Electronic design, Emergency stop device, Machinery safety, Prototyping

Introduction

Machine safety is a growing technical discipline with a solid foundation in the development of so-called electrical and electronic safety protective devices (SPDs). According to the principles of machine safety integration given in standard ISO 12100[(1)], SPDs are designed to avoid or at least mitigate those risks associated with a particular human-machinery interaction, which cannot be eliminated from the design stage.

Generally speaking, a set of SPDs can be adapted to a machine to minimise its associated risks. However, ISO 12100 establishes a mandatory SPD for use in almost any industrial machinery, except for portable and hand-guided types—the emergency stop device (ESD).

An ESD is a manually operated type of control that provides an emergency stop function, i.e., it stops the machine as soon as possible without creating additional hazards. It consists of two parts: an emergency stop switch (ESS), and a manual mechanical actuator that operates on the ESS. ESDs are typically classified according to its actuator into three types[2]: emergency stop buttons (ESBs), hand rope/cable pull switches, and foot pedal operated switches. The most common type of ESB is a red mushroom-shaped push-button attached to a bright yellow housing for improved visibility. ESDs are electrically connected in series to a single-function machinery circuit called emergency stop circuit (ESC). ESDs comply with international standards ISO 13850[(3)], and IEC 60947-5-5 .[4]

A hierarchical supervisory safety system (HSSS)[5] has been recently developed for active protection of workers using a relevant group of semi-automatic industrial machinery, including Cartesian cutters and welders. This HSSS combines visual worker detection and machine cycle tracking for safety purposes, while seamlessly accessing the machine's ESC.[5,6]

For achieving this active sensing principle, a general purpose electronic ESD (e-ESD) has also been developed.[7] It is devised to actuate in its intended behaviour (i.e., to latch in or release) in response to external commands delivered from a HSSS via a standard communication link. Similar to conventional ESD, it also provides manual operation under the requirements of ISO 13850.[3]

This paper concentrates on the main design and implementation issues to consider when building an e-ESD prototype, with a stress on ease of customisation for use in non-specific machine ESCs.

Materials and Methods

Concept Design

The concept design scheme of a general-purpose electronic ESD (*e*-ESD) is depicted in Fig. 1. Its main feature is to provide automatic activation and release actions that can be monitored and commanded by a

*Author for Correspondence
E-mail: jalvarof@unex.es

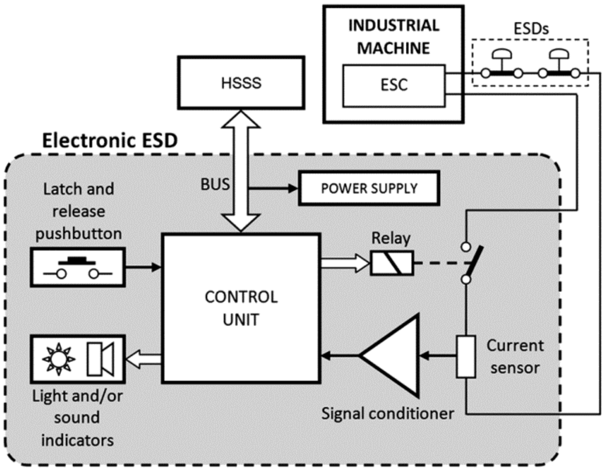

Fig. 1 — Concept design scheme of an electronic ESD[7]

Table 1 — Conventional vs electronic ESD

Feature	Conventional ESD	Electronic ESD
Activation method	Manual	Manual / Electronic
Release method	Manual	Manual / Electronic
ESC status readout	No	Yes
Remote activation	No	Yes
Remote release	No	Yes
Communication bus	No	Yes

HSSS via a non-specific standard bus (e.g., RS-485, RS-232, and USB). Its conceptual design allows the device to be easily adapted for use on different machines, as its implementation is not limited to a specific technology. The main differences of this device compared to conventional ESD are summarized in Table 1.

Wireless communication between HSSS and e-ESD is completely discarded from the design stage, as these means have been shown in practice to be much more prone to electromagnetic interference (EMI) issues than standard wired solutions. EMI is an unwanted, but expected, guest in industrial environments that drastically hampers radio link reliability.[8]

To reduce system complexity, the e-ESD is designed to be powered from the bus. It can also be operated manually, similar to conventional ESD. An internal control unit manages HSSS communication and supervises the machine ESC. It continuously detects and stores ESC status without delay, so it can readily send both the ESC and the internal states to the external HSSS via the communication bus. It also provides suitable connections for visual and/or audio information devices that report these readings.

Two key elements are connected to the machine ESC in Fig. 1: a relay with its contact in series with other machine ESDs, and an instantaneous current sensing system that determines the emergency stop condition. Its operation principle follows. If no current is detected at the ESC, the emergency stop function is active, i.e., at least one of the machine ESDs, or the e-ESD itself, is latched (relay contact in open state). Otherwise, the machine is in normal operating mode, since each ESD connected to the ESC, including the e-ESD, has its contacts closed, allowing current to flow in the ESC.

The communication protocol between the e-ESD and the HSSS is asynchronous and command-based, in a typical master-slave configuration. From the e-ESD side, these commands fall into two categories: reception (RX) and transmission (TX).

On the one hand, the RX commands received from the HSSS include the following action requests: ESD automatic latch, ESD automatic release, and ESC status. On the other hand, the TX commands delivered to the HSSS include the ESC status report, as requested by the HSSS, and the following unrequested reports: ESC emergency status; ESC back-to-normal status after emergency status; ESC emergency status as self-activated by the e-ESD, including its push-button; and ESC back-to-normal status as self-activated by the e-ESD, including its push-button.

In short, RX commands comprise activation, deactivation and request for information commands, while TX commands report data previously requested by the HSSS, or alarm conditions without request.

Design Methods

Several design issues must be considered before implementing a working e-ESD prototype. First, a suitable method must be chosen to measure the current flowing in the ESC. From the comprehensive review of current sensing techniques of Ziegler *et al.*[9], two simple sensing techniques stand out among others: shunt resistor and Hall effect.

Shunt resistor method causes power loss in the current path, limiting its use to low current applications. However, it is by far the simplest and cheapest detection method, allowing both AC and DC measurements. On the other hand, current sensors based on the Hall effect avoid resistive losses since their output voltage is driven by a magnetic field. Moreover, they are a robust and affordable sensing solution for harsh environments. However, they add some complexity and cost due to the use of magnetic field concentrators (toroidal cores) to reduce misalignment errors.[9]

In an e-ESD, the current sensor module must provide ESC current measurements with sufficient resolution so that the control unit can reliably determine ESC status. Since the standardised ESC DC limit is 2 A[4], and high-resolution measurements are not required to assess ON/OFF circuit status, the shunt resistor method is our preferred choice.

Now, as the e-ESD is connected in series with the machine ESC, the equivalent total circuit resistance R_T will be increased. Typically, the practical range of values for R_T is limited by the electrical characteristics of a monitoring safety relay (MSR), which properly initiates the machinery emergency stop function. MSR working limits can be expressed as minimum current $I_{ESC\min}$ and voltage $V_{ESC\min}$, which in turn determine the maximum allowable ESC resistance, $R_{T\max}$, according to:

$$R_{T\max} = R_R + \frac{V_{CC} - V_{ESC\min}}{I_{ESC\min}} \qquad \ldots (1)$$

where V_{CC} is the ESC voltage supply and R_R is the MSR internal resistance. This deviation from R_R is due to both the length and conductance of the ESC wiring, and the equivalent series resistance of the released ESDs connected to the ESC.

When the e-ESD is inserted into the machine ESC, the combined resistance of its relay contact and shunt resistor (R_S) is upper-bounded to

$$R_{S\lim} = R_{T\max} - R_{ESC} \qquad \ldots (2)$$

where R_{ESC} is the equivalent series resistance of the initial ESC in its release state, and $R_{T\max}$ is given by Eq. (1). Typically, high R_S values are preferred to improve the available signal-to-noise ratio (SNR) at the current sensor. Moreover, the e-ESD response should be as independent as possible of the exact location of the ESC insertion point, since this insertion point may be favoured by e.g. accessibility factors.

To achieve better SNR and insertion point independence, a differential voltage measurement across the shunt resistor (V_S) from an I/V converter is often preferred (see Fig. 2). These converters generally feature an adjustable gain A_V that modifies the analogue-to-digital converter (ADC) input voltage V_O, where ADC is a required component for reading data from the control unit.

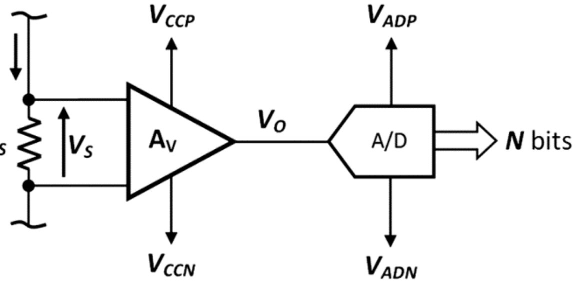

Fig. 2 — Circuit for differential current measurement

By choosing a shunt resistor value R_S for the circuit of Fig. 2, a minimum value $R_{S\min}$ can be effortlessly found as

$$R_{S\min} = \frac{R_{ESC}}{A_V V_{CC} / V_{O\min} - 1} \qquad \ldots (3)$$

Hence, setting $R_S = R_{S\min}$ yields a minimum I/V converter output $V_{O\min}$ to obtain adequate digital current measurement resolution at the ADC. On the other hand, the shunt resistor also has an upper limit value $R_{S\max}$ for which V_O is within the ADC power supply limits, V_{ADP} and V_{ADN}. This value can be found as

$$R_{S\max} = \frac{R_{ESC}}{A_V V_{CC} / V_{AD} - 1} \qquad \ldots (4)$$

where $V_{AD} = V_{ADP} - V_{ADN}$ is the ADC voltage operating range.

Finally, the ESC insertion point also affects the I/V converter common mode input voltage V_{Scm}. Therefore, both positive (V_{CCP}) and negative (V_{CCN}) I/V converter power supply limits must be checked to ensure proper sensing circuit operation.

Results and Discussion

Implementation

In this section, we discuss the implementation details of a fully functional and low-cost e-ESD prototype, in particular, those related to the available prototyping options derived from Fig. 1.

First, selecting a USB bus for HSSS communication provides the designer with some advantages, including direct power supply across the bus and faster prototype development and testing. In this work, we selected the USB development kit from microChip.[10] It contains a USB-powered high-performance PIC18F47J53 microcontroller, including a 10-bit ADC, a push-button and two high-efficiency

LEDs. While these features are all basic elements of the e-ESD (see Fig. 1), other required components cannot be directly implemented on this kit. Thus, we developed an additional PCB to incorporate the remaining features, namely a relay, a resistor-based current sensor with I/V converter, signal conditioning circuits, ESC connection terminals, and an inverter for controlling the I/V converter power supply limits.

The USB development kit was attached to our custom board with a header connector, yielding the compact two-layer assembly shown in Fig. 3. The relay drive circuit was designed to keep its contacts openwhen power fails, indicating an emergency stop condition. Finally, the current sensor was implemented with the TSC103 chip[11] as its principal component, as it provides four different gains A_V.

The e-ESD prototype was programmed to detect three emergency conditions: EM1, initiated by the HSSS; EM2, initiated by on-board push-button actuation; and EM3, initiated by activation of other ESD connected to the ESC. These emergency conditions were visually coded on the kit's LEDs (L1 and L2).

The device switches between two states: latched (relay contact open) and released (relay contact closed). Its operation was set as follows. The e-ESD starts by default in its latched state by activating EM1 and EM2. In this way, a safe start of the machine is guaranteed. To change this initial state, the e-ESD requires the HSSS to command a deactivation message EM1, informing the absence of risk in the machinery workplace, and a manual on-board push-button actuation to deactivate EM2. On meeting these two conditions, the machine ESC will allow machine operation when each ESD connected to the ESC is in its released state (EM3 deactivated).

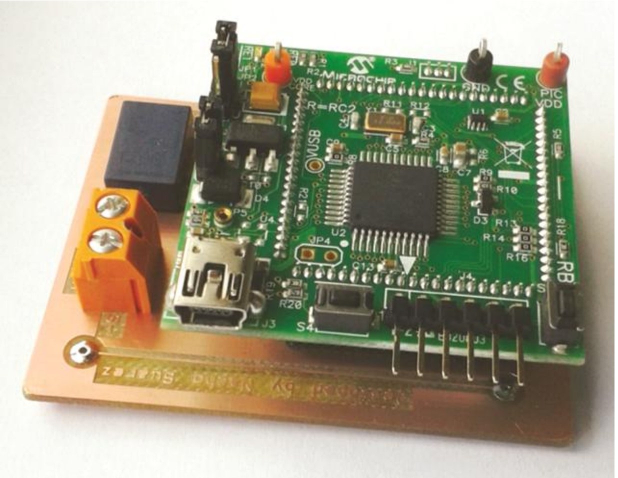

Fig. 3 — A low-cost e-ESD prototype

After initialization, the e-ESD enters a continuous operation mode in which, according to foreseeable events, it switches between its latched and released states. In its released state, its behaviour is as follows:

- ESC current is shortly measured at each processing cycle.
- If ESC current is below a threshold *T*, EM3 activates (both L1 and L2 blink). Otherwise, EM3 deactivates.
- The e-ESD switches to its latched status if the HSSS reports a dangerous condition (EM1) or if the on-board push-button is activated (EM2).
- If no emergency condition is detected, both L1 and L2 remain off.

The operation of the e-ESD in its latched state is as follows:

- The relay is inactive (open), which disables EM3 assessment.
- Latched status is indicated by powered L1 (EM1 on) and/ or L2 (EM2 on).
- The e-ESD changes to its released state if the HSSS reports a safe condition (EM1 off) and/ or if the integrated push-button is manually deactivated (EM2 off).
- Any change in EM2 condition is automatically signalled to the HSSS.

Verification and Validation

After completing the design and implementation stages, verification and validation tests required to configure the e-ESD to meet the ESC requirements of the test machine. We chose to test our prototype on a plasma cutting machine installed in a controlled laboratory. The ESC of this machine contains three conventional ESBs mounted on different locations for easier operator access. One terminal of this ESC is connected to the chassis ground, while the other terminal is powered from a XPSATE safety relay.[12] The operating parameters of the machine ESC prior to testing were as follows: V_{CC} = 21.0 V, $V_{ESC\mathrm{min}}$ = 17.0 V, $R_{T\mathrm{max}}$ = 2100 Ω, and R_{ESC} = 1726.9 Ω.

As discussed in the previous section, the ESC insertion point should provide the machine operator with safe and easy access while introducing minimal variation to the ESC. In this case, the chassis ground terminal was chosen. Also, since our prototype is USB powered, this choice required the use of an additional DC/DC converter to extend the I/V converter input common-mode range $V_{S\mathrm{cm}}$.

Using Eq. (2) with initial ESC parameters revealed that R_S values below $R_{S\mathrm{lim}} \approx 370\ \Omega$ ensured a safe

Table 2 — R_S limit values vs I/V converter gain A_V

A_V	20.00	25.00	50.00	100.00
$R_{S\max}(\Omega)$	6.82	5.45	2.72	1.36
$R_{S\min}(\Omega)$	13.70	10.94	5.45	2.72

operation of the ESC. However, in order to obtain adequate digital current resolution on the 10-bit ADC, $V_{O\min}$ was chosen as half of the ADC's voltage operating range, V_{AD} = 3.3 V, providing a maximum resolution loss of 1 bit. This configuration proved to be an acceptable value for assessing significant current variations in the ESC.

Since the chosen I/V converter [11] allows using four conversion gains A_V, we obtained the set of $R_{S\min}$ and $R_{S\max}$ values in Table 2 using Eqs (3) and (4). These data show that actual R_S limits are normally imposed by the I/V converter, regardless of its gain. In this case, we chose A_V = 20 and R_S = 10 Ω, yielding V_O values over 73% V_{AD}.

Next, to test and validate our prototype, we linked it to a PC via USB to simulate a generic HSSS. Verification tests ensure meeting design specifications, whereas validation tests ensure compliance with the operational needs of the intended use.[13] We devised two groups of tests for verification and validation: operational and response time tests.

We repeated 1,000 times the following operational tests, obtaining zero faults:

- Power switch on (USB). Outcome: start in latched state.
- Power switch off (USB). Outcome: change to latched state.
- Release command (HSSS). Outcome: keep (all EMs off) or change (EM3 on) to released state.
- Release command (on-board push-button). Outcome: keep (EM3 on) or change (all EMs off) to released state.
- Random, single EM condition in released state. Outcome: change to latched state; send EM2/ EM3 on to HSSS; L1/L2 on.
- Random, multiple simultaneous EM conditions in released state. Outcome: change to latched state; send EM2/EM3 on to HSSS; L1/L2 on.
- Random, single EM condition deactivation in latched state. Outcome: change to released state; send EM2 off to HSSS; L1/L2 off.

The results obtained from these operational tests show high prototype reliability in every foreseeable situation.

Finally, we also measured the following prototype response times:

Table 3 — Electronic ESD response times

HSSS Command	Response time	Average (ms)	Standard Deviation (ms)
Latch	T_{SL1}	0.003664	~ 0
	T_{SL2}	1.1815	0.0031
	T_{SL}	1.1852	0.0031
Release	T_{SR1}	0.003914	~ 0
	T_{SR2}	1.5918	0.0114
	T_{SR}	1.5957	0.0114

- Supervised latch time (T_{SL}): timespan between a received USB latch command and e-ESD relay deactivation, comprising two non-overlapping intervals:
  - T_{SL1}: from latch command reception to internal relay deactivation command delivery.
  - T_{SL2}: from internal relay deactivation command delivery to hardware relay deactivation.
- Supervised release time (T_{SR}): time interval from reception of USB release command to e-ESD relay activation, also comprising two non-overlapping intervals:
  - T_{SR1}: from release command reception to internal relay activation command delivery.
  - T_{SR2}: from internal relay activation command delivery to hardware relay activation.

We measured a series of 100 response time tests using a Tektronix TDS2024B digital oscilloscope, obtaining the results provided in Table 3. T_{SL1} and T_{SR1} response times were nearly constant since microprocessor execution cycles do not vary. Also, both relay deactivation and activation times (T_{SL2} and T_{SR2}) were fairly accurate. Finally, the average total latch time (T_{SL}) was 0.4 ms slower than average release time (T_{SR}), both being much smaller than the nominal response time of the XPSATE safety relay[12] installed at the machine control system. From these results, our developed prototype shows high reliability and a fast and accurate response. Moreover, the proposed verification and validation tests proved to be adequate for their intended purpose.

Conclusions

In this paper, we discuss the practical aspects of designing and implementing an e-ESD prototype in detail, from the initial concept to the final verification and validation stage. From a low-cost prototyping perspective, our design choices highlight using USB kits for rapid development, the preference for shunt resistor method for current sensing, and the development of custom PCBs to obtain a compact and configurable product. Measured response times on our device were significantly lower than those of modern safety relays. This validates our design, since the processing delay is negligible in all foreseeable situations.

Moreover, the modular structure used in prototyping makes studying future expansions and improvements a more flexible and cost-effective endeavour. Among these, the use of Hall effect sensors for current measurement is of particular interest. This method further facilitates e-ESD installation on longer and more complex ESCs, where the practical limits for R_S are more restrictive.

References

1 ISO 12100, *Safety of machinery – general principles for design – risk assessment and risk reduction* (International Standards Organization, Geneva, Switzerland) 2010.

2 Caputo A C, Pelagagge P M & Salini P, AHP-based methodology for selecting safety devices of industrial machinery, *Safety Sci*, **53** (2013) 202–218. doi:10.1016/ j.ssci.2012.10.006

3 ISO 13850, *Safety of machinery – emergency stop – principles for design* (International Standards Organization, Geneva, Switzerland) 2015.

4 IEC 60947-5-5, *Low-voltage switchgear and control gear – part 5-5: control circuit devices and switching elements – electrical emergency stop device with mechanical latching function* (International Electrotechnical Commission, Geneva, Switzerland) 2016.

5 Fernandez-Muñoz J A & Moreno-Rabel M D, System for active and immediate detection and prevention of risks in industrial machinery, *WIPO International Patent WO/2013/ 093163* (to Universidad de Extremadura, ES) 27 Jun 2013.

6 Moreno-Rabel M D & Fernandez-Muñoz J A, An access detection and machine cycle tracking system for machine safety, *Int J Adv Manuf Tech*, **87** (2016) 77–101. doi:10.1007/s00170-016-8446-2

7 Fernandez-Muñoz J A, Suarez-Marcelo J I & Moreno-Rabel M D, Dispositivo electrónico de parada de emergencia con reposición automática supervisada, *Spanish Patent ES1116830* (to Universidad de Extremadura, ES) 18 Jul 2014.

8 Willig A, Matheus K & Wolisz A, Wireless technology in industrial networks, *P IEEE*, **93** (2005) 1130–1151. doi:10.1109/JPROC.2005.849717

9 Ziegler S, Woodward R C, Iu H H-C & Borle L J, Current sensing techniques: a review, *IEEE Sens J*, **9** (2009) 354–376. doi:10.1109/JSEN.2009.2013914

10 Microchip Technology, PIC18F4XJ5X full-speed USB demonstration board user’s guide, *available online* (2010): https://ww1.microchip.com/downloads/en/DeviceDoc/51806 b.pdf

11 ST Microelectronics, TSC103 Datasheet, *available online* (2014): https://www.st.com/resource/en/datasheet/tsc103.pdf

12 Schneider Electric, XPSATE5110 safety relay datasheet, *available online* (2009): https://www.se.com/ ww/en/product /download-pdf/XPSATE5110

13 Maropoulos P G & Ceglarek D, Design verification and validation in product lifecycle, *CIRP Ann-ManufTechn*, **59** (2010) 740–759. doi:10.1016/j.cirp.2010.05.005