INTRODUCTION

SELECTING THE OPTIMAL CONTROLLER

Some form of safety controller is required to meet higher risk categories of the European safety standards, to meet OSHA/ANSI requirements for Control Reliability, and when using coded-magnet switches as safety interlocks. This guide is intended to help you properly select and apply Schmersal Safety Controllers.

It is common for all of us to want to look at safety issues in black and white terms (“Here is Application Number 116 and I can find the solution in my Safety Handbook under Solution Number 116”). Unfortunately, this is seldom possible. You are forced to look at safety issues in various shades of gray. For any given situation, there may be a number of correct solutions depending on total system design.

A safe machine is generally achieved through the combination of safety measures incorporated by design and taken by the machine operator. Ideally such measures should be addressed during the design phase. In addition proper training of machine operators and maintenance personnel is critical for safe operation.

While individual component suppliers can provide general guidance and technical information related to their products, it is the responsibility of the machine designer or retrofitter to ensure the safety system is designed to meet the appropriate standards.

To minimize the possibility of worker injury and address industry safety standards/guidelines, it is recommended that the machine designer follow these general steps:

1) Familiarize himself with the pertinent safety standards
2) Specify the limits of the machine
3) Identify the hazards and assess the risks
4) Remove the hazards or limit the risk by design
5) For remaining hazards, install necessary protective devices
6) Inform and warn the operator of any remaining risks/hazards.

In designing a machine guarding safety system, the following objectives should be considered:

- Design to suit the working environment
- Achieve the desired degree of protection
- Do not interfere with machine operation
- Do not encourage manipulation/bypassing
- Make it difficult to override
- Do not cause any additional dangers/hazards

It is impossible to correctly select and apply a Safety Controller without performing some type of quantitative risk assessment. “Guesstimating” a control category may lead to excessive expense and/or to an inadequate or unsafe system. There are a number of approaches to risk assessment, most of which use some form of decision tree to determine the appropriate safety control category. One such approach is discussed in the next section.

A simplistic approach that can initially point you in the right direction, but which must not be substituted for a formal risk assessment is:

- If a machine can cause an injury that will heal without permanent damage or disability, you most likely can satisfy your needs with a Category 1 safety control system.

- If a machine can cause permanent damage or disability, you probably require at least a Category 3 safety control system.

Note: For additional background material, you may wish to review Schmersal’s “Man-Machine Safeguarding Requirements & Techniques.” This tutorial booklet provides an overview of basic machine safeguarding concepts and terminology.

RISK ASSESSMENT

Different machines and processes have different levels of relative risk. Determining this relative risk level involves evaluating three major factors. These include:

(1) Severity of the potential injury.

(2) Frequency of exposure to the potential hazard.

(3) Possibility of avoiding the hazard if it occurs.

One approach to risk assessment provides guidelines for determining the safety control system requirements based upon five levels of risk. These levels range from the lowest risk (level B) in which the severity of injury is slight and/or there is relatively little likelihood of occurrence, to the highest risk (level 4) in which the likelihood of a severe injury (if the safety control system fails) is relatively high.

This particular method is depicted in Figure 1, in which the following qualitative definitions apply:

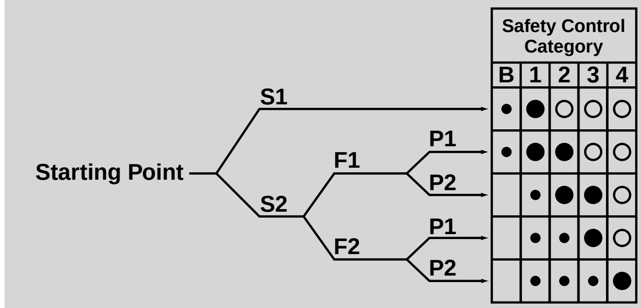
S: Severity of potential injury
S1: slight injury (bruise)
S2: severe injury (amputation or death)

F: Frequency of exposure to potential hazard
F1: infrequent exposure
F2: frequent to continuous exposure

P: Possibility of avoiding the hazard if it occurs (generally related to the speed/frequency of movement of hazard point and distance to hazard point)
P1: possible
P2: less possible

The levels of risk and related safety control system requirements are defined in Figure 2.

These safety control system categories are not to be regarded as a hierarchy. The goal is to reduce the ultimate risk of all machines to acceptable levels regardless of initial assessed risk.



Selection of the Safety Control Category:
A brief overview of these safety control categories is provided in Figure 2.

● Preferred categories

• Possible categories, which require additional measures

○ Excessive measures for the relevant risk

FIGURE 1

FIGURE 2

Safety Cat.	General Safety System Requirements	General Safety System Behavior
B	Safety system designed to meet operational requirements and withstand expected external influences. (This category is usually satisfied by selecting components compatible with the application conditions … e.g. temperature, voltage, load, etc.)	A single fault or failure in the safety system can lead to the loss of the safety function.
1	Safety system must meet the requirements of Category B, but must use “well-tried” safety principles and components. “Well-tried” principles and components include those which: • avoid certain faults … e.g. short circuits. • reduce probability of faults … e.g. over-rating selected components, over-dimensioning for structural integrity. • detect faults early … e.g. ground fault protection. • assure the mode of the fault … e.g. ensure an open circuit when it is vital that power be interrupted should an unsafe condition arise. • limit the consequences of the fault.	A single fault or failure in the safety system can lead to the loss of the safety function. However, the use of “well tried” safety principles and safety components results in a higher level of safety system reliability.
2	Safety system must meet the requirements of Category B. In addition the machine shall be prevented from starting if a fault is detected upon application of machine power, or upon periodic checking during operation. (This suggests the use of a safety relay module with redundancy and self-checking. Single-channel operation is permitted provided that the input devices … such as machine guard interlocks, E-stop pushbuttons, et al … are tested for proper operation on a regular basis.)	Here, too, a single fault or failure in the safety system can lead to the loss of the safety function between the checking intervals. However, periodic checking may detect faults and permit timely maintenance of the safety system.

Safety Cat.	General Safety System Requirements	General Safety System Behavior
3	Safety system must meet the requirements of Category B. In addition the safety control system must be designed such that a single fault will not lead to the loss of the safety function. And, where practical, the single fault will be detected. (This requires redundancy in the safety circuit monitoring module and the use of dual-channel monitoring of the input and output devices such as machine guard interlock switches, E-stop pushbuttons, safety relays, etc.)	Here a single fault or failure in the safety system will not lead to the loss of the safety function and, where possible, will be detected.
4*	Safety system must meet the requirements of Category B. In addition the safety control system must be designed such that a single fault will not lead to the loss of the safety function and will be detected at or before the next demand on the safety system. If this is not possible, then the accumulation of multiple faults must not lead to the loss of the safety function. (This also requires redundancy in the safety circuit and the use of dual-channel monitoring of the input and output devices such as machine guard interlock switches, E-stop pushbuttons, safety relays, etc. Here the number of allowable faults will be determined by the application, technology used, and system structure.)	Here a single fault or failure in the safety system will not lead to the loss of the safety function, and it will be detected in time to prevent the loss of the safety function.

*Category/Level 4 safety requirements are usually associated with extremely high-risk applications. Since general machine design practice respects classic safety hierarchy, in which most machine hazards are either:
- designed out,
- guarded against (if they cannot be designed out), and,
- (as a last resort) warned against,

Level 4 requirements may arise relatively infrequently.

ACHIEVING “CONTROL RELIABILITY”

“Control Reliability” as defined by ANSI/OSHA essentially states that the safety system be designed, constructed and installed such that the failure of a single component within the device or system should not prevent normal machine stopping action from taking place — but shall prevent a successive machine cycle from being initiated until the failure is corrected.

Note that this definition closely follows the definitions of a safety control category 3 as defined by European machinery safety standard EN954-1.

It is helpful to break down the definition of Control Reliability in order to better understand how it might be achieved.

- Any single fault shall not lead to a loss of the safety function. This strongly implies redundancy in the safety circuit.
- Successive machine cycles shall be prevented until the fault is corrected. This means the fault must be detected. This is achieved by cross-monitoring of the redundant safety circuits.
- The device that is cross-monitoring (safety controller) must also be checked to prevent a loss of the safety system due to a fault in this device.

Thus the following are required to achieve “Control Reliability”:

- Redundancy
- Fault Detection
- Cross-Monitoring
- Self-checking of the monitoring device

Let’s look at a basic safety system and develop it to a control reliable level.

Assuming the components are selected with appropriate electrical ratings and agency approvals, this system will generally meet category B requirements per European standards.

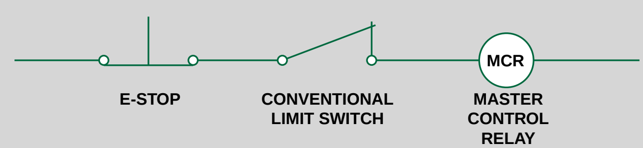


FIGURE 3
Basic Safety Control System (Category B)

We can improve the safety system reliability by using an E-Stop and a safety interlock switch with positive-break contacts. This will generally meet category 1 requirements per the referenced European standards. However, it does not yet meet the requirements for control reliability.

FIGURE 4:
Basic Safety Control System (Category 1)

To increase the reliability, let's next add additional positive-break contacts to our E-Stop and safety interlock switch (Figure 5).

We now have redundancy but still lack fault detection. To provide this fault detection, we must add additional devices.

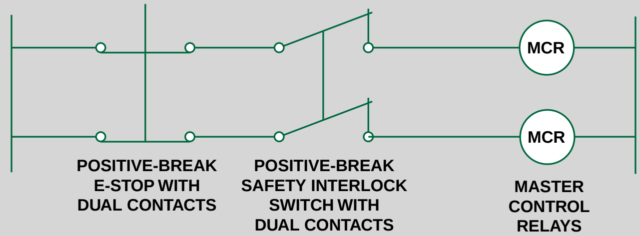


FIGURE 5:
Basic Safety Control System with Redundancy

This black box provides safety system fault detection as well as cross-monitoring and self-checking. While this can be achieved with a complex hard-wired circuit utilizing 3 positive-guided relays and over 40 wiring points, it is much simpler and less expensive to utilize a commercially available safety controller.

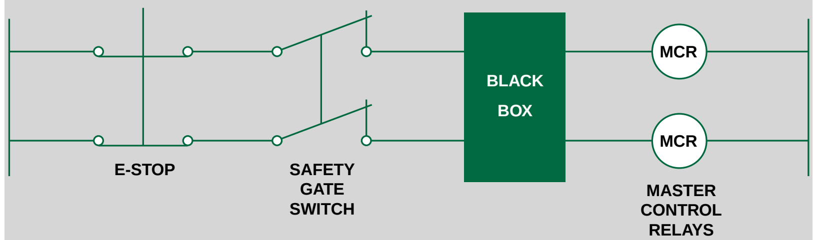


FIGURE 6:
Basic Safety Control System (Category 3 or 4)
with Redundancy and Fault Detection

Figure 7 shows a typical example of a control reliable circuit utilizing a safety controller.

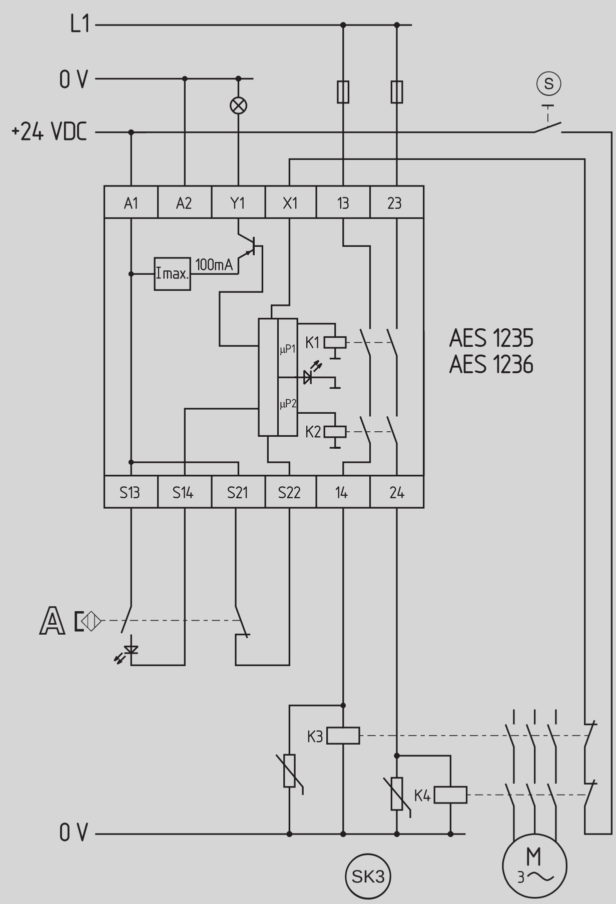


FIGURE 7

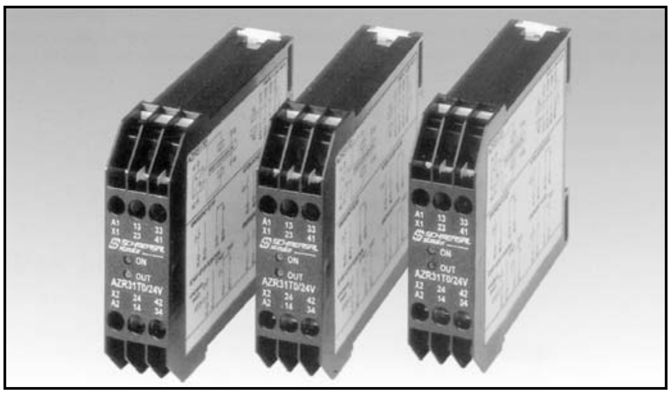
BASIC FUNCTION

The SCHMERSAL family of safety controllers includes two basic designs. One utilizes relay logic. The other uses solid-state (microprocessor) logic. Pioneered by SCHMERSAL, these “smart” safety controllers provide added features and capabilities unachievable with conventional safety relay modules.

Both designs feature redundant, dual-channel cross-monitoring logic circuits. These continuously check for, and detect, faults in the system’s safety circuit components and interconnection wiring. Modules also detect when a machine guard interlock/E-stop switch is actuated and, depending upon the model, are capable of detecting the following types of potential safety circuit faults:

- Welded interlock/E-stop switch contacts
- Misaligned guard
- Open circuits, short circuits or ground faults
- Welded/stuck contacts in module’s safety relays
- Fault in the module’s monitoring circuits
- Inadequate supply voltage to module
- Welded/stuck contacts in controlled output motor contactor/control relay
- Capacitive/inductive interference on module inputs

All controllers are designed to increase the level of safety in the machine guarding and/or E-stop control circuit.



SERIES SRB/AZR SAFETY CONTROLLERS

The SRB/AZR Series safety controllers are conventional electro-mechanical relay-based units. Many feature the latest relay technology utilizing only two internal relays to achieve cross-monitoring, self-checking and redundancy. This results in a smaller, highly cost-effective solution for up to safety control category 4 system performance per European standards.

Models are available to satisfy most safety application requirements. They offer a wide variety of important features including:

- 1 or 2 channel triggering
- Crossed wire detection
- STOP Category 0 & 1 modules
- Manual monitored reset
- Monitoring of non-potential free contacts
- Feature selection via base mounted dip switches
- Output expanders
- Special 12VDC for use on battery power
- Dual channel antivalent input circuits for humid environments

SERIES AES MICROPROCESSOR-BASED SAFETY CONTROLLERS

SCHMERSAL’s AES Series features microprocessor-based monitoring logic. In addition to performing the functions provided by traditional relay-based modules, the AES Series “smart” controllers provide added capabilities typically unavailable in relay-based designs. These include:

- Fault identification diagnostics … the AES provides a variety of flashing, colored LED patterns which indicate specific types of faults and their location (thus minimizing equipment downtime).
- Auxiliary semiconductor outputs … for alarm and/or signaling purposes.
- Modular component design … permitting realization of the most cost-effective monitoring solution.
- “Diverse redundancy” … use of different components and/or programs in the redundant monitoring circuits eliminates “common cause” failures and heightens module reliability.
- Multiple inputs.

While initially designed for use with Schmersal coded-magnet switches, most controllers can also be used with E-Stop or conventional machine guard safety interlock switches. These controllers are separated into several categories for ease of selection.

SELECTION CRITERIA

It helps the selection process to view a safety controller as having four basic characteristics, each determined by the application requirements. This approach can be applied to any safety controller.

FOUR BASIC SAFETY CONTROLLER CHARACTERISTICS

SUPPLY VOLTAGE REQUIREMENTS

Select your supply voltage. While many voltages are possible (24VDC, 24VAC, 24VAC/DC, 115VAC and 230VAC), 24 VDC gives the most flexibility since virtually all controllers are available in this voltage. Also, since a transformer and rectifier are not required, this unit generally is less expensive and smaller than a 115VAC model.

Regardless of supply voltage, it is always converted by the controller electronics to 24VDC for internal operation and for powering monitored input devices. Hence monitored devices only need to be rated for 24VDC.

INPUT MONITORING REQUIREMENTS

The first step is to determine whether you need single channel (up to control category 2) or dual channel (control category 3 & 4) operation.

Single-channel systems must monitor one NC positive-break contact. Dual-channel systems can monitor 1NO/1NC or 2NC contacts. Generally, these need to be isolated dry contacts since most controllers will view C-form contacts as a short circuit. Remember that 24VDC is supplied by the safety controller for monitoring these contacts.

Safety controllers are available for monitoring non-potential free contacts (such as PNP outputs from light curtains). Models are also available that allow users to field select the monitored contact configuration.

Another consideration is crossed wire detection (a short between channels). This requires special circuitry in the safety controllers and is required for category 4 safety control systems.

FEEDBACK & RESET CIRCUIT REQUIREMENTS

Safety controllers with feedback capability can also monitor control relays and motor contactors with positive-guided contacts. Such feedback is required for safety control category 3 & 4 systems. A NC auxiliary contact is wired into the feedback loop (with or without a reset (start) button) to detect welded contacts in these external control devices. The safety controller detects the existence of a weld when the relay shuts down due to a power loss or open machine guard and prevents a restart.

In order to reset the controller, the feedback loop must be closed (at least temporarily). If the NC auxiliary contact stays open due to a contact weld, the controller cannot be reset.

Reset can be automatic or be manual monitored/trailing edge. With automatic reset the controller will automatically reset (outputs close) when the machine guard is closed. A reset or start button can be added to the feedback loop if desired. The controller only needs to momentarily see a 24VDC signal at the feedback terminals to reset.

With a manual monitored/trailing edge reset, some type of manual pushbutton is required. The feedback loop circuitry is designed so that it needs to see a 24V to 0V transition (trailing edge) in order to reset. This method of reset is generally required when a person can actually get inside a machine guard (where they would be at risk if the equipment should automatically restart when the guard closes).

OUTPUT REQUIREMENTS

Determine the number and type of safety controller outputs required for machine control elements and signaling. Following are the types of safety controller outputs:

A. NO safety enable circuits — either instantaneous or timed.

B. NO or NC auxiliary relay contacts — these are not to be used for safety functions, but only for annunciation/signaling.

C. Semiconductor outputs for annunciation.

SAFETY CONTROLLER SELECTION GUIDE

The following selection charts have been created to help you select a safety controller that satisfies your application requirements. Unlike other selection methods that usually start with identifying the appropriate safety control category, this method begins with the application requirements and leads to a possible safety relay solution.

To begin, select the application category in the Master Index Chart below. This will direct you to the appropriate selection chart. Then starting at the top of the appropriate chart move through the application selection criteria until a safety controller(s) is suggested. This selection should then be examined to ensure it is adequate for the assessed level of risk.

Note:

- Models with 4 digits such as 1235 are part of the AES series.
- Models with a mixed number such as 31R2 are part of the AZR series.
- Models such as C.xx or MO are part of the SRB series.

Safety Controller Key

Maximum Recommended Safety Control category per EN954:

- Safety Control Category 1/2 (CC1)
- Safety Control Category 3 (CC3)
- Safety Control Category 4 (CC4)

Under Stop Category 1, Safe Outputs are shown as

STOP 0 / STOP 1

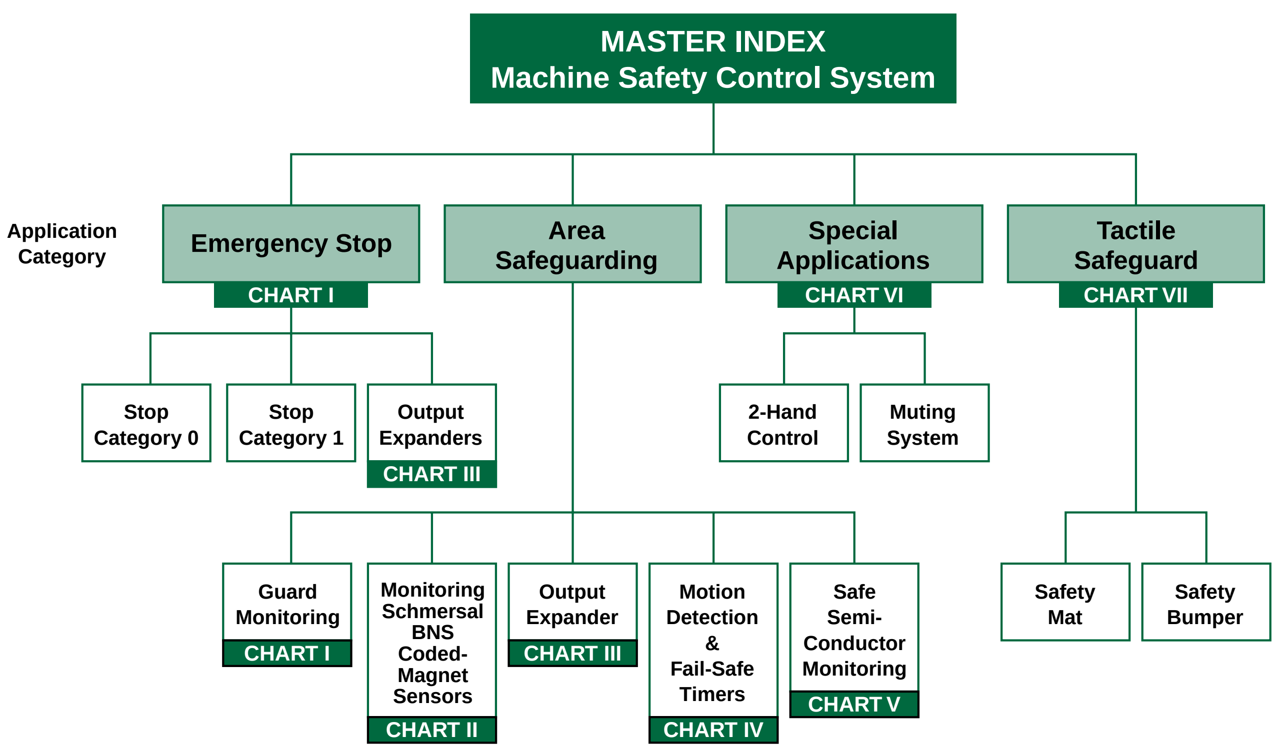


CHART I

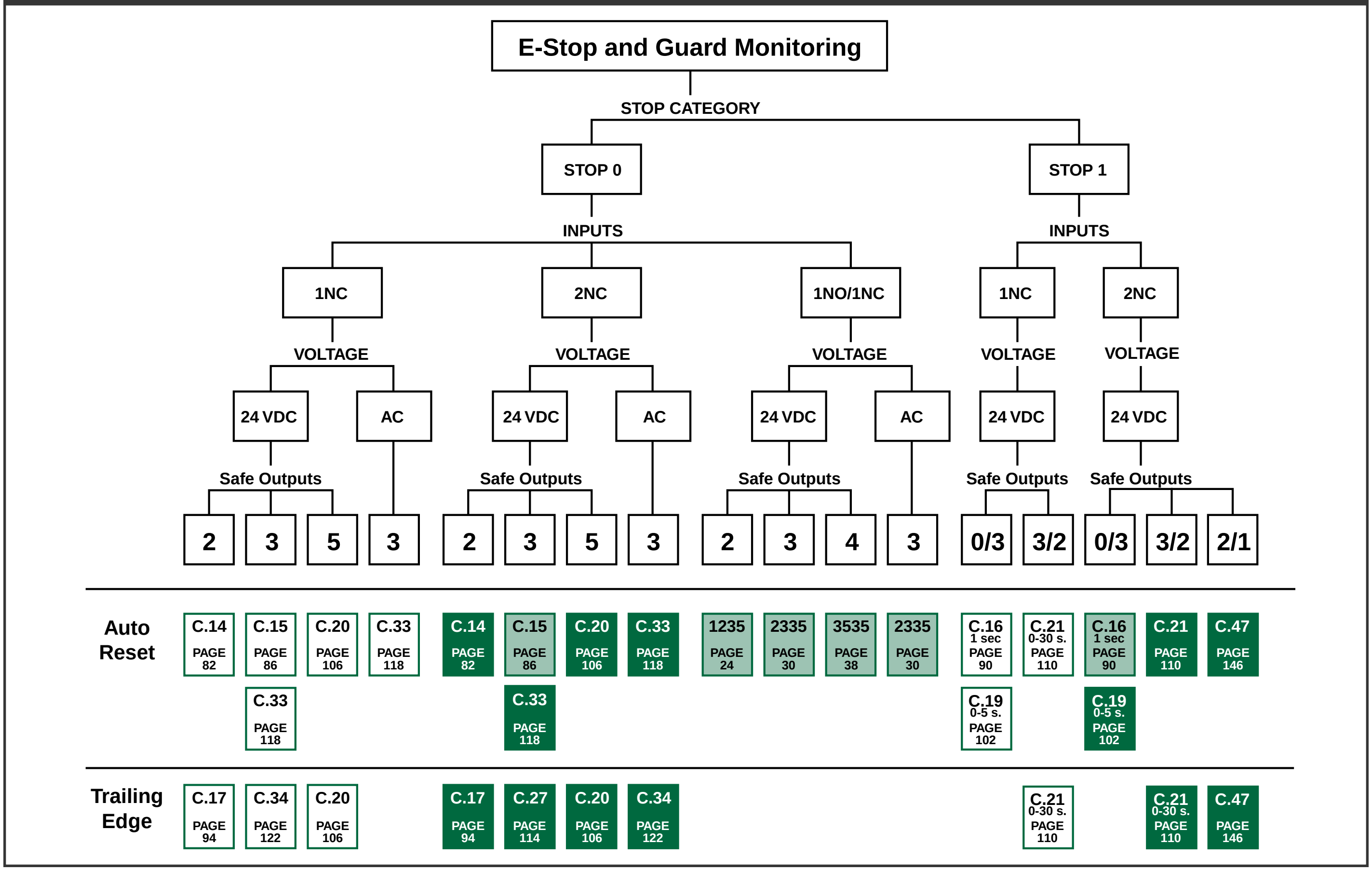


CHART II

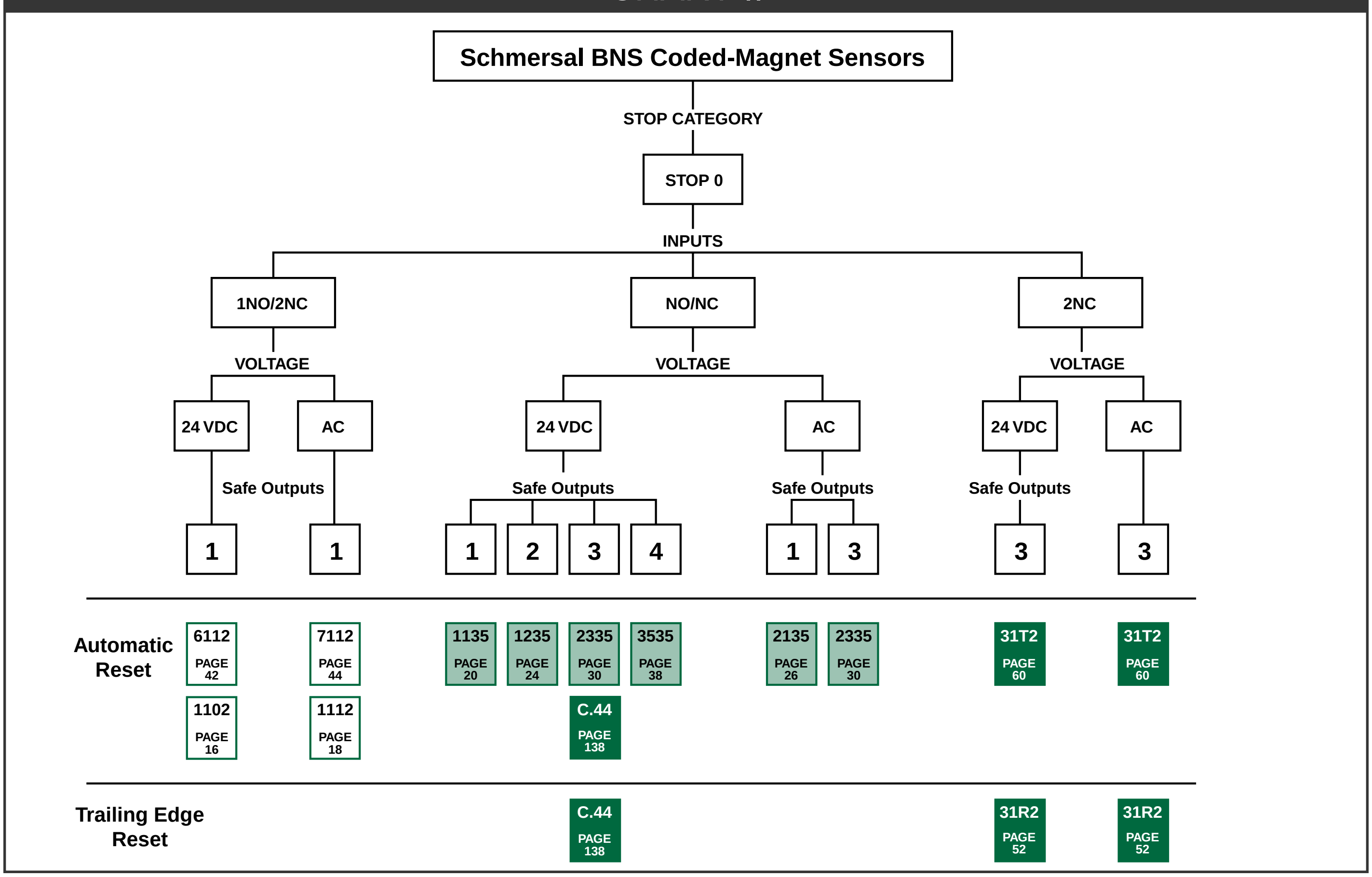


CHART III

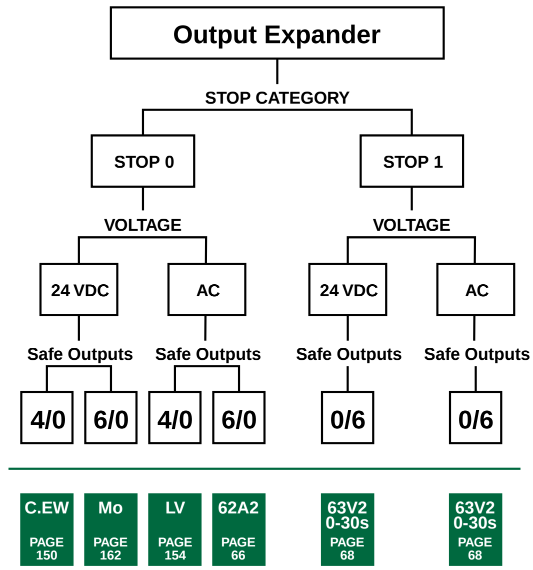


CHART IV

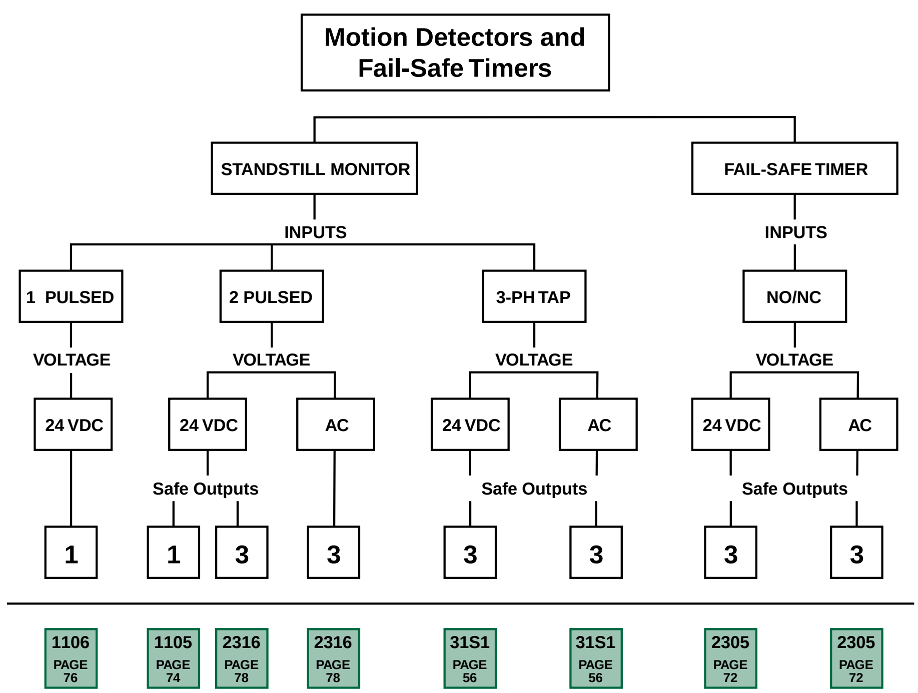
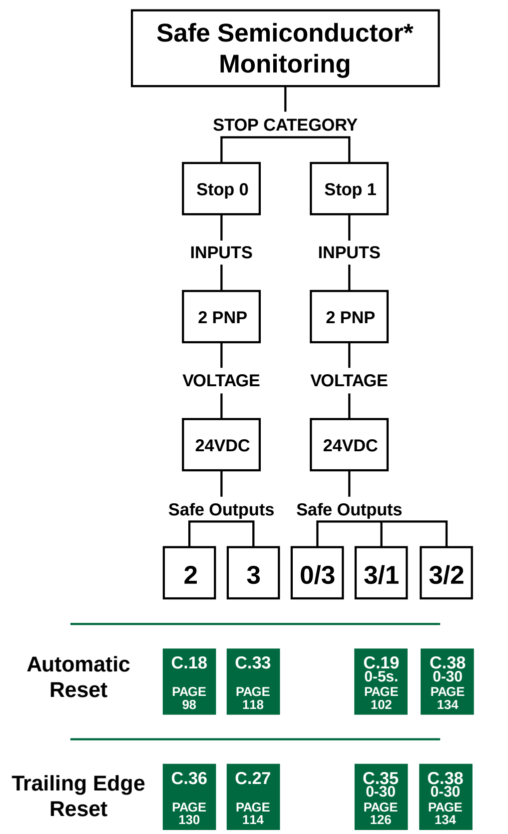


CHART V



*i.e. PNP outputs from light curtains or proximity switches

CHART VI

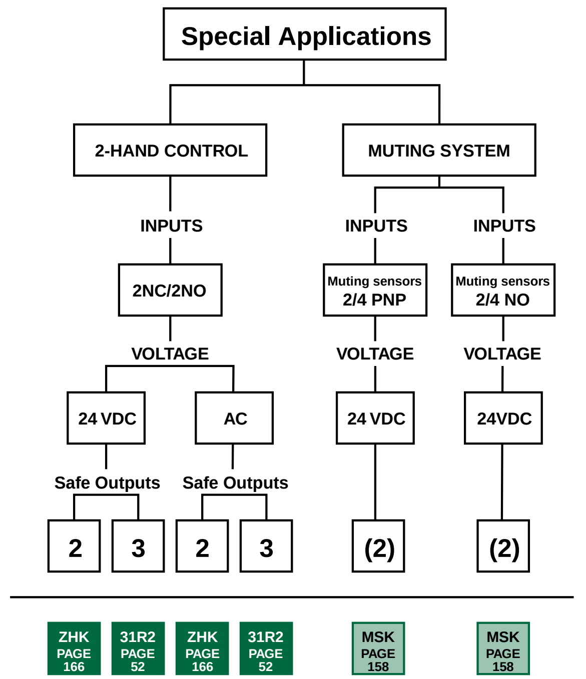


CHART VII