OSC|12
Ohio Safety Congress & Expo

WELL AT HOME. SAFE AT WORK.

484 Machinery Safety: Safe Designs for a Safe Workplace

Dennis Aulbrook, CFPS, CME

Thursday, March 29, 1 to 2 p.m.

Ohio | Bureau of Workers' Compensation

Machinery Safety - Safe Designs for a Safe Workplace

Dennis Aulbrook
Advanced Safety & Energy, Inc.
810-417-0220 mobile
dennis.aulbrook@gessafety.com

Introduction

• What makes a "Safe Work Place"?

- Conscientious Employees
- Alert Personnel
- Proactive Approach to Safety
- Safety Procedures
- Safety Guarding
- Safety Controls
- Training
- Safety Awareness– (Signs / Alarms)
- PPE – Personal Protective Equipment
- Clean Work Environment

3

Risk Reduction – Quick Review

Hierarchy of Protective Measures

Design it out		Most Effective
Fixed enclosing guard		
Energy Control / Interlocked Gates/ Safety Valves etc.		
Awareness Means, Training and Procedures (Administrative)		
Personal protective equipment		Least Effective

4

Standards for Machine Safety

What guidelines are there for designing a safety system?

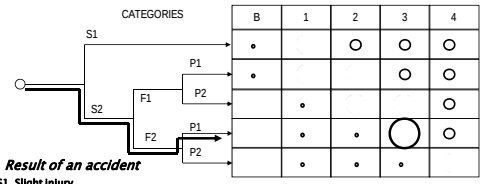
Mandatory
- OSHA

Voluntary
- ANSI
- NFPA
- ASME
- EN
- CSA
- IEC
- ISO

OSHA
Occupational Safety and Health Administration
www.osha.gov

5

Risk Assessment – Quick Review According to EN 954-1



- S *Result of an accident*
  - S1 Slight injury
  - S2 Serious or irreversible injury to one person, or death of a person
- F *Frequency of exposure to hazard*
  - F1 Rare to fairly frequent
  - F2 Often to permanent
- P *Possibility of avoiding the hazard*
  - P1 Possible in certain circumstances
  - P2 Virtually impossible

● Preferred control system category

o Possible categories which can require additional measures

○ Measures which may exceed min. requirements for relevant risk

6

Risk Assessment – What's New? ISO – 13849

US / Canada		European Community (EN-954)
Simple	Close approximation →	Cat. B Low Risk
Single Channel	→	Cat. 1
Single Channel with Monitoring	→	Cat. 2
Control Reliable	→	Cat. 3 Cat. 4 High Risk

European Community (ISO13849) - 2009
Performance Level $P_L a$
$P_L b$
$P_L c$
$P_L d$
$P_L e$

Architecture Based | Blended

7

NFPA 79 and IEC/EN 60204-1 Stop Categories

- The E-stop must be a Category 0 or 1 stop
  - **Category 0**
    - Immediate removal of power to actuators (*coast to stop, uncontrolled stop*)
  - **Category 1**
    - Controlled stop and then removal of power to actuators

  Note: Per NFPA 79 Par. 9.2.5.4.1.3 the Category Shall be determined by a Risk Assessment
- E-stop – the final removal of power must be by electromechanical components*

8

Control Reliable – Quick Review

- High and Very High Risk Areas – must use "CONTROL RELIABLE" circuit(s) according to the standards
- No single failure will cause the loss of safety
  - Redundancy (Dual Channel)
  - Diversity
  - Monitoring/Diagnostics
  - Manual Reset(s)
  - Fail to Safe
  - Fault Tolerant

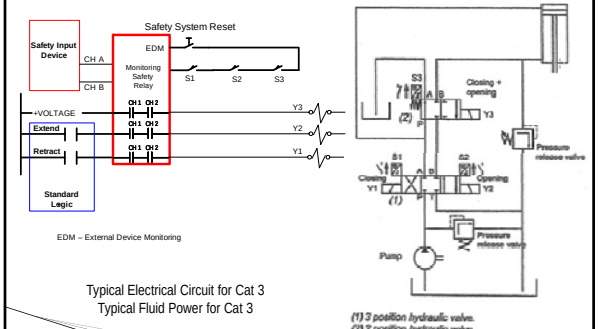
9

Control Reliable – Quick Review

- **OSHA 1910.217(b)(13)**
- **Control reliability**. When required by paragraph (c)(5) of this section, the control system shall be constructed so that **a failure** within the system does not prevent the normal stopping action from being applied to the press when required, but does prevent initiation of a successive stroke until the failure is corrected. The failure shall be detectable by a simple test, or indicated by the control system.
- ANSI B11.19, Performance Criteria for Safeguarding
- ANSI RIA R15.06, Industrial Robots and Robot Systems ANSI B11.TR3, Risk Assessment and Risk Reduction
- ANSI B155, Safety Requirements for Packaging Machinery
- ANSI B151, Safety Requirements for Plastics Machines
- NFPA 79-2007, Electrical Standard for Industrial Machinery
- ISO 13849-2009, Safety of Machinery . . .
- EN 954, Safety of Machinery . . .

10

Control Reliable – Quick Review



Typical Electrical Circuit for Cat 3
Typical Fluid Power for Cat 3

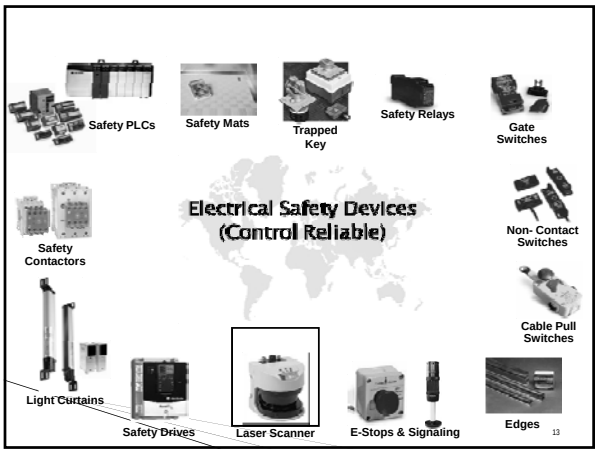
11

Machine Safety – Energy Types

Energy Sources

- Electrical
- Hydraulic
- Pneumatic
- Mechanical
- ~~Radiation/Laser~~
- ~~Kinetic~~
- ~~Chemical~~
- ~~Thermal~~

12



Safety Control Systems

- Safety controllers (programmable and non-programmable) should be control reliable safety rated devices with dual channel inputs that employ continuous self-checking and are capable of open circuit detection; short-circuit detection and ground fault detection. Monitoring and error checking of peripheral safety output devices (such as safety contactors, hydraulic safety valves, pneumatic safety valves etc.) should be performed at each cycle of the safety system or each time the safety system is interrupted.
- Bonus if safety controls can be configured for a variety of different functions and inputs such as OSSD and Test Pulse continuous error checking.
- Bonus if non-safety rated outputs are available at a lower cost (for non-safety functions like indicator lights and stack lights).


Programmable


Non-programmable

14

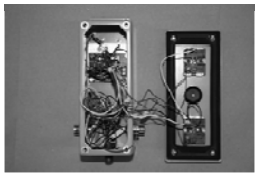
Safety Control Systems – What's New?

- Smart Safety Relays (Non-programmable)
- Single or Dual Input Selection
- OSSD or Test Pulse Input configuration
- AND – OR Functions
- Single wire communication

15

Safety Control Systems – What's New?

- Smart interfaces for non-safety I/O
- Signaling and indicator lights + Flashing or delay functions
- Can be used with "dumb" safety devices like safety relays
- Reduces cost due to reduction in I/O & no programming required



16

Safety Control Systems – What's New?

- Safety Buss + Plug & Play Devices
- Reduces installation & replacement time


E-Stops & Signaling

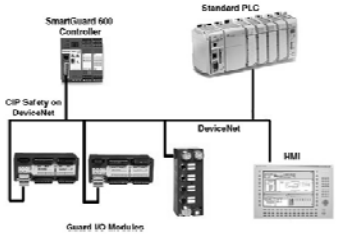

Non- Contact Switches


Laser Scanner

17

Safety Control Systems – What's New?

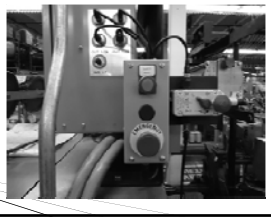
- Distributed I/O Modules for large installations
- Ethernet & other safety protocols



18

Emergency Stop Devices

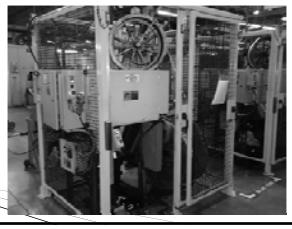
- Emergency stop devices may include push buttons, pull-ropes or other devices. Emergency stop devices should be dual channel, have positive opening contacts, latch in place when depressed or activated and require a reset. Emergency stop should be red in color with a yellow background, unguarded, with a mushroom head to meet the requirements of NFPA 79. To enhance circuit performance, employ continuous self-checking (test pulse).



19

Emergency Stop Devices

- Emergency stop devices should be in every operator station
- Shall override all other functions & operations in all modes (automatic, manual, jog, inch etc.)
- Resetting an emergency stop shall not start the machine cycle
- Some standards require E-Stops inside the hazardous area where personnel could be trapped and on portable "jog" pendants.



20

Emergency Stop Devices – What's New?

- Emergency stop push buttons with monitored contacts. Stops if the contact block decouples from the operator
- Modular E-Stop stacks

21

Non-Locking Safety Rated Switches

- Also known as "interlocks" – dual channel and safety rated
- Electro-mechanical with a tongue/keyed actuator. Please note that a single fault causing the loss of safety will occur if the switch actuator breaks or separates from the door. It is possible however, for this type of switch to be electrically control reliable.

22

Non-Locking Safety Switches – What's new?

- Non Contact switches
- Maintain category 4 when wired in series
- Not easy to defeat if magnetically coded or RFID
- Some have built in indicator lights & diagnostic colors.
- Some require an interface module

23

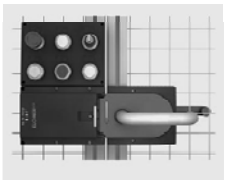
Locking Safety Rated Switches

- Also known as "solenoid locking interlocks" – dual channel and safety rated
- Mechanical rod, tongue or keyed actuator that is capable of being locked.
- Typical usage to prevent unauthorized entry into an area; force a controlled stop of the equipment prior to entry and/or prevent entry before the hazardous motion has stopped. Stop of machine monitored by time or motion controller
- Can be power to lock or power to unlock
- Typically coupled with a "request to enter" operator station and emergency release on the inside of the gate
- Please note that when using electro-mechanical interlocks, a single fault causing the loss of safety will occur if the switch actuator breaks or separates from the door. It is possible however, for this type of switch to be electrically control reliable.

24

Locking Safety Switches – What's new?

- Modular "request to enter" operator station
- Non-contact locking switches (light duty)

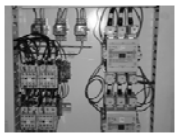


25

Safety Contactors (force guided)

- Safety controllers are not generally capable of switching high current electrical loads, so safety contactors are used to isolate loads with higher current draws (sometimes as low as 1A).
- Safety contactors should be installed in pairs and be equipped with force guided contacts
- Safety contactors should be energized with separate outputs from the safety control system and be monitored by the safety controls to ensure proper operation.
- Surge suppressors should be installed on the coils to reduce the risk of false triggering.
- If the primary energy source is not isolated, then the circuit is NOT control reliable.

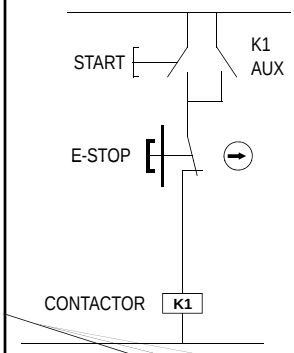
Not control reliable

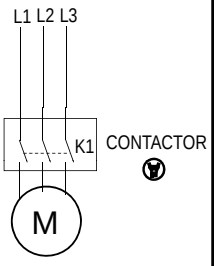


Control reliable

26

Safety Contactors & Control Reliability





Circuit Performance: Simple Circuit, not control reliable.

27

Safety Contactors – What's new?

- Safe-off drives (category 3)
- Small (inexpensive) force guided relays for smaller loads like hydraulic valves, pneumatic valves, PLC outputs and even to drive larger contactors

28

Presence Sensors

- Can be Light curtain; Laser scanner, Multiple beam devices, Pressure sensitive mats or bumpers
- Curtains & scanners typically rated at Category 4 but Category 2 are available for reduced cost.
- In some cases, double acknowledgement systems can be used in place of a presence sensor
- Mats & bumpers should be 4-wire devices to be connected to a control reliable circuit
- Keep in mind stop time distances; wash down requirements and chemical resistance ratings.

Light Curtains

Laser Scanner

Safety Mats

Edges

29

Presence Sensors – What's new?

- Safety Cameras
- Smart Light Curtains with built in blanking and mute functions – can be used with "dumb" control systems
- Less expensive laser scanners
- Inexpensive laser lights to indicate protected area

30

Two-hand controls

- Used to inhibit reach into a hazardous area by making the operator press buttons with both hands to activate machine movement.
- Use anti-tie down and anti-repeat; which ensures that the buttons are pressed and released each cycle, reducing the risk of tampering with or defeating the safety circuit.

31

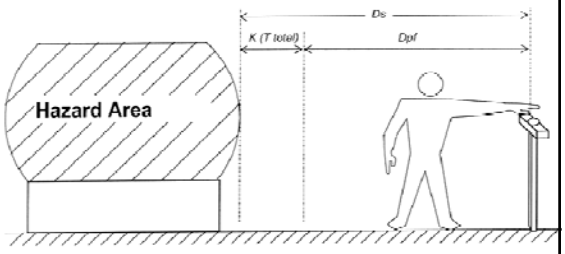
Two-hand controls – What's new?

- Ergonomic push-buttons (to reduce tendon injuries)
- Portable two-hand control stations which can be disconnected and moved to other machinery (saves investment on multiple fixed units)

32

Annex D Figure D.7

Figure D.7: Single Control Device



Safety Distance (*Ds*) for a Single Control Device includes a large *Dpf* of 2 meters (6.5 feet) due to the ability of the operator to stand between the device and reach towards the hazard.

Annex D Figure D.2

Figure D.2: *Dpf* for ground level devices that can be reached over (30° or less)

Examples include safety mats, area scanners, and horizontally mounted electro-optical devices.

REACH-OVER
Dpf = 1200 mm (48 in) for horizontal sensing field applications without vertical sensing.

Allowable Sensing Field Heights in mm. (in)

Objects Sensitivity (S)	Mounting Height (h) Minimum	Maximum
< 50 (2)	0	990 (39)
64 (2.5)	190 (7.5)	990 (39)
76 (3.0)	380 (15)	990 (39)
89 (3.5)	570(22.5)	990 (39)
102 (4.0)	760 (30)	990 (39)
108 (4.25)	860 (33.75)	990 (39)
117 (4.6)	990 (39)	990 (39)

Minimum mounting height (*h*) can also be determined by the following.
h = 15 (*S* – 50) mm
h = 15 (*S* – 2) in
where *S* is the object sensitivity.

NOTE - Minimum depth-of-field or sensing area must hinder an individual from stepping over the electro-optical presence-sensing device or safety mat. This distance is 1.2 m (4 ft) if an individual can step over and pass unrestricted; 900 mm (3 ft) if supplemental safeguarding or physical barriers are used such that an individual must stand within the sensing area. For electro-optical presence-sensing devices inclined greater than 30° from horizontal, and for which you cannot reach over without being detected, use Figure D.1.

Stop Time Distance Measurements
Ds=K(Ts+Tc+Tr+Tbm)+Dpf

- **Ds**= **Minimum Safety Distance** between the device and the pinch point (hazard).
- **K**=**Hand Speed constant** of 63 in./second.
- **Ts**=**Stop Time** of **Equipment** (seconds)
- **Tc**=**Control System** response time (seconds).
- **Tr**=Response time of **Presence Sensor** in seconds.
- **Tbm**=Variable for **Clutch Brake Response**.
- **Dpf**=**Depth Penetration Factor** calculated by the following formula: Dpf=3.4(S-.276). Where S=Presence Sensor **Minimum Object Sensitivity** in inches (14mm & 30mm is common).

- * Measure Ts & Tc times with a Stop Time meter .

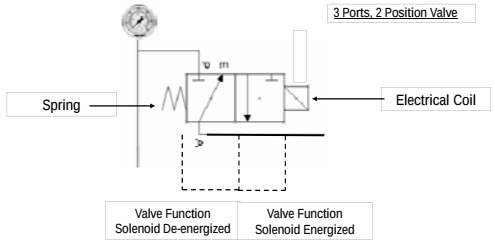
Hydraulic & Pneumatic Safety

Hydraulic & Pneumatic Hazards

- Hazards
  - Crushing / Severing / Entrapment etc. from failures in cylinders, actuators or motors that are driven by fluid or air
  - Falling / Gravity / Mechanical etc. when fluid or air is released
  - Impact / Burns / Fire etc. when hoses, fittings or other equip. fail

36

2-Way Pneumatic Valve Overview



3 Ports
P – Pressure
E – Exhaust
A – Port to Cylinder

When Solenoid is Energized, Pressure (P) is supplied to Port (A)

When Solenoid is NOT Energized, Port (A) is routed to Exhaust (E)

37

Failure Mode – Hyd. & Pneumatic

Failure Mode Review

- What are some of the failures that occur?
  - Valve Spool Sticking (because of varnish, contamination, dirt, grit, rust, internal wear etc.)
  - Short Circuit / Open Circuit on Solenoid
  - Broken Hose or Fitting – Loss of pressure
  - Mechanical Failure (Couplings, Cylinder Rods, Springs, etc.)
  - Cylinder O-Ring Failure / Valve Seal Failure

38

Failure Mode – Hyd. & Pneumatic

Failure Mode Review

- What are possible causes of these failure modes?
  - System Contamination / Lack of Filtration
  - Over Pressure
  - Over Temperature
  - Lack of Maintenance
  - Wrong Components / Loose fasteners
  - Bad Design (wrong size, wrong type, hose length incorrect, etc.)

39

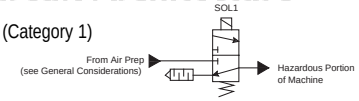
What could go wrong?

- Any failure in the fluid power or pneumatic system can cause hazardous movement

40

Safety Circuit Architecture

Single Channel Circuit (Category 1)



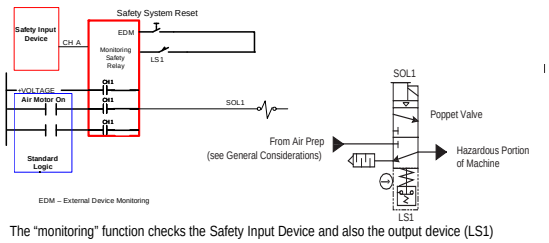
Safety Function:	When the electrical command signals are removed, the valve exhausts fluid power from the hazardous portion of the machine.
Faults to Consider:	• Valve stuck in actuated position. • Pilot seal failure – Can lead to unexpected valve element movement • Pilot section manual actuator seal failure - Can lead to unexpected valve element movement • Valve element not actuating or de-actuating properly due to fluid contamination or internal wear. • Broken components (piston, poppet, spring) within a valve element could cause valve to shift unexpectedly or not shift.
Fault Exclusion:	None

Note: There is no "monitoring" of the components by the control system

41

Safety Circuit Architecture

Single Channel Circuit with monitoring (Category 2)



The "monitoring" function checks the Safety Input Device and also the output device (LS1)

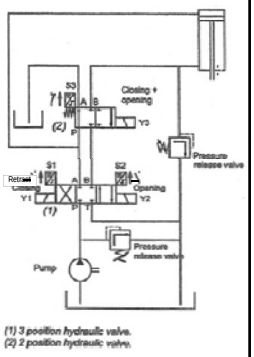
Some standards consider an overall safety system to be "control reliable" if this monitored output circuit is coupled with other safety devices that block all other energy sources (elec., hyd., pneu., mech. etc.) & are monitored. Inputs must be control reliable (not as shown)

42

Safety Circuit Architecture

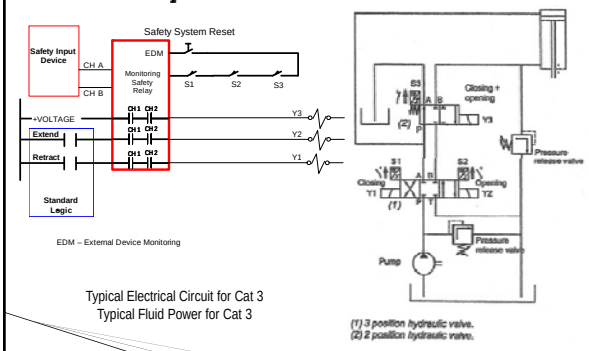
Dual Channel (Category 3) Valve Set Up

- Fault exclusion –Valve(s) sticking, Solenoid failure, Some hose / fitting failures
- Redundancy
  - -Valve (1) – 3 position hydraulic valve
  - -Valve (2) – 2 position hydraulic valve
- Monitoring
  - -S1 monitors retracting spool position
  - -S2 monitors extending spool position
  - -S3 monitors the spool position



43

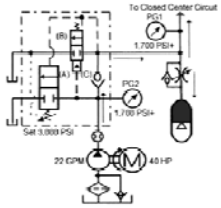
Safety Circuit Architecture



44

Controlling Stored Energy

- How do we control stored energy?

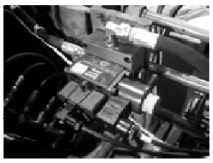


Accumulators:
Install safety valve(s) downstream of accumulator
Accumulator dump valve may be required for safety system (depending on risk; either manual dump valve, monitored dump valve or control reliable solenoid valve)

Lockout / Tag Out:
OSHA requires the release of trapped energy prior to maintenance & servicing tasks. A dump valve can serve this purpose.

45

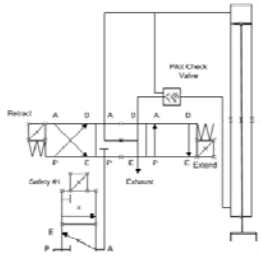
Circuit examples



46

Vertical Load Holding

- How do we keep vertical loads from falling?



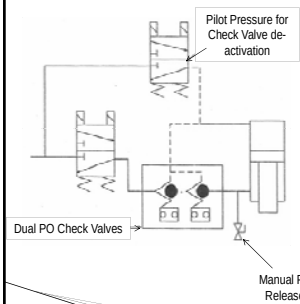
Air and Hydraulic Cylinders:
The Pilot Operated (PO) Check Valve would engage once the pressure source is isolated. This would hold the cylinder in a suspended state. If the seals are bad, the cylinder would drift. A second PO check valve on the cap end of the cylinder would resolve a leakage problem. Counter-balance valves can accomplish the same goals.

Other Benefits:
The cylinder would remain stationary on the loss of voltage, loss of air pressure or decoupled hose(s), if the PO check(s) were installed directly into the cylinder ports.

47

Vertical Load Holding

- How do we keep vertical loads from falling?



Air and Hydraulic Cylinders:
Dual Pilot Operated (PO) Check Valves add redundancy for high risk areas. PO check valves can also be monitored into the control system. Counter-balance valves are not as versatile.

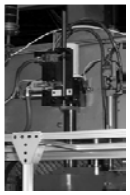
Lockout / Tag Out:
OSHA requires the release of trapped energy prior to maintenance & servicing tasks. A manual release valve can serve this purpose.

48

Vertical Load Holding

- Mechanical Failures (Loads & Gravity)

Manual Die Blocks, use of administrative controls required.



Ratchet Style Mechanical Safety monitored by safety system

Rod Locks monitored by safety system

49

Hoses and Fittings

- High pressure hoses will whip when they decouple and can cause serious injury or death.

5000 psi hose within inches of an operator for 3 shifts a day

Potential Solutions:
Install "Hose Restraints"
Engineer safety system – add interlocked guard doors that would not open until pressure is at a safe state.
Interlocks to limit / shut down energy

Hose restraint

50

Control reliable valves – What's new?

- Pre-Packaged Safety Valves offer other alternatives when it comes to off the shelf control reliable valves

Ross dual air valve

GPA dual air valve

SVC dual hydraulic valve. Can be configured 6 different ways

51

Thank You !
Machinery Safety - Safe Designs for a Safe Workplace

Dennis Aulbrook
Advanced Safety & Energy, Inc.
810-417-0220 mobile
dennis.aulbrook@asesafety.com

o Points of view, ideas, products, demonstrations or devices presented or displayed at the Ohio Safety Congress & Expo do not constitute endorsements by BWC. BWC is not liable for any errors or omissions in event materials.

OSC 12
Ohio Safety Congress & Expo