Controlling Risks
Safety Instrumented Systems

Safety Instrumented Systems

- The purpose of an SIS is to monitor a potentially dangerous condition and mitigate the consequence of a hazardous event
- An SIS
  - Does not improve the yield of a process
  - Does not increase efficiency
  - Does save money by loss reduction
  - Does reduce the risk cost$

Why are the operators angry?

The machine tripped off.

Risk Cost

- Risk is the probability of a failure event times the consequence of the failure event
- The consequence is measured in terms of cost of event
- The concept of risk cost is the actual cost of an event in incurred only after a failure
- The cost is averaged over the number of years of a non-failure
- Improving PFD improves the chances that a failure will not occur

Risk Reduction

- Risks inherent in a process may be lowered by
  - Changing the process
  - Adding physical control
  - Adding a safety instrumented system

Risk Reduction Factor

- The risk reduction factor (RRF) may be defined as:

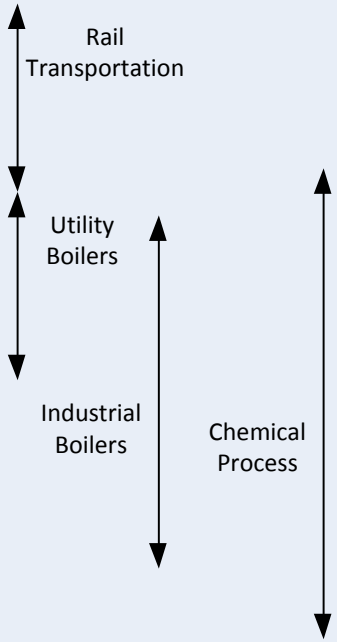
$$RRF = \frac{Inherent\ Risk}{Acceptable\ Risk}$$

- PFD is important in Safety Instrumented Systems because it is the probability that the system will fail to provide the safety function when needed

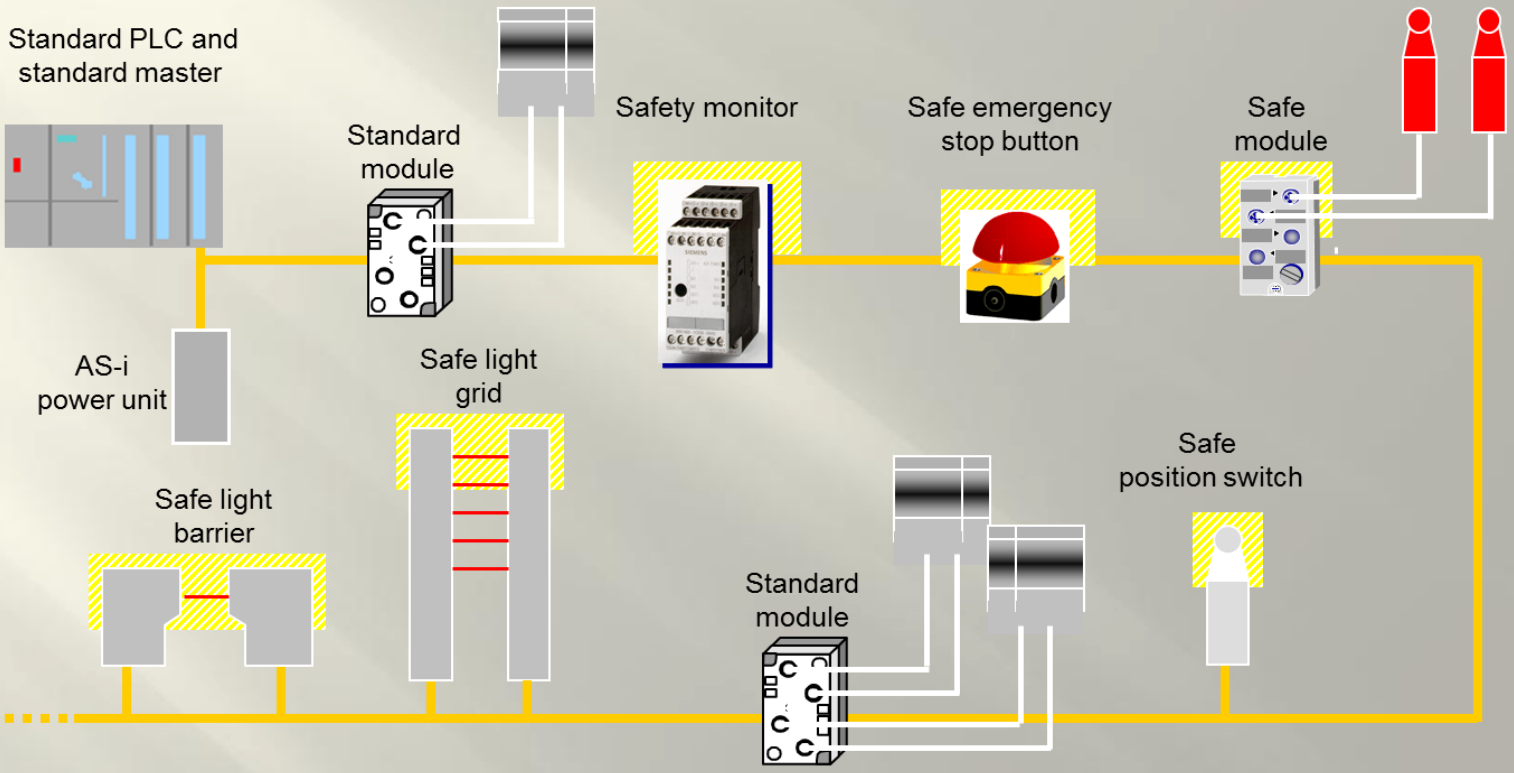
$$RRF = \frac{1}{PFDavg}$$

Risk Reduction Categories

Safety Integrity Level	Average Probability of Failure on Demand	Risk Reduction Factor	Typical Applications
4	< 0.0001	> 10,000	
3	0.001 – 0.0001	1.000 – 10.000	
2	0.01 – 0.001	100 – 1,000	
1	0.1 – 0.01	10 - 100	



So, You Got Yourself an SIS?



What SIL are you going to use?

Interlock Requirements Document

- If the hazard analysis of an accelerator indicates the need for an interlock system then an interlock requirements document must be produced [DOE G 420.2-1, II.A.1.c]
- The requirements for facility interlocks must be documented in an interlock requirements document that has been reviewed and approved by line management. [DOE G 420.2-1, II.B.3.a.3] [10CFR835 835.704(b)]
- The interlock requirements document should document the selection of control measures that reduce risks to acceptable levels and include a functional description of the interlock system. [DOE G 420.2-1, II.B.3.a.3]

Fail-safe and Redundant Circuits

- The protective functions of the interlock system should be robust against single-point failures, and designed such that they fail in a “safe” manner, including loss of power or pressure, open circuits, and shorts to ground. [DOE G 420.2-1, II.B.3.a.1)i]
- Control panel lights or system indicators should be fail-safe. Two or more indicators representing different device or machine states may be used to provide the status of a system. The use of multiple lamps for a single status should indicate dissimilar states such as open/closed or in/out. [DOE G 441.1-1C, 7.4.0.2]
- Redundant devices should be considered for use in interlock systems where a very high radiation area, as defined in 10 CFR 835, can be produced during operations. [DOE G 420.2-1, II.B.3.a.1)iii(a)]

Programmable Logic Controllers

- PLCs may have multiple, and often difficult-to-recognize, failure modes which may result in potentially unsafe conditions.
- Failure rates of overt fault (detected or revealed) failure modes or covert fault (hidden, concealed, undetected latent, etc.) failure modes are influenced by
  - component design
  - manufacturer's quality
  - Installation
  - environmental conditions.
- Measures to ensure that abnormal PLC operation is detected include the use of
  - external verification programs
  - power monitors
  - internal run-time diagnostics.
- Ideally, all will provide interlockable signals that move the facility into a safe state when errors are detected. [ANSI/HPS N43.3-2008, 6.9]

PLC Selection

- The selection of PLCs should be made only after an evaluation of the electrical and physical environment in which the PLCs will be used.
- The selection of *commercial PLCs* should be made with due caution, since they normally do not have sufficient safety integrity.
- Only PLCs designed and designated as a Safety PLC should be used for *radiological interlock functions*. [ANSI/HPS N43.3-2008, 6.9]

Solid-State Relays

- Solid-state relays may have unsafe failure modes and have limited applications in interlock circuits.
- The IEC 61508 standard may be consulted as a reference. [ANSI/HPS N43.3-2008, 6.9]

System Monitoring

- Interlock system hardware and/or software should indicate the state of the interlock components at the console.
- Interlock system hardware and/or software should indicate off-normal events at the console with a light or an audable signal to notify cognizant personnel of abnormal events and conditions. [DOE G 441.1-1C, 7.4.0.2]
- General control system software may be used to display interlock status and perform access control functions.
- The interlock system must be independent of the control system software and include isolation to prevent the control system from preventing the interlock system from performing critical interlock functions.

  [DOE G 420.2-1, II.B.3.a.1)iii(b)]

Very High Radiation Areas

- A radiological enclosure that contains a Very High Radiation Area shall have the following features within the exclusion area
  - An Emergency Shutdown Switch (i.e., a 'run-safe' box) [ANSI N43.3-2008 5.1.4; 5.1.5.2] [21 CFR 1020(7)(i)]
  - Search and secure controls (e.g. timed key-lock watchman stations) [DOE G 441.1-1C, 7.4.0.1]

    (More about this later)

High Radiation Areas

- Each entrance or access point to a high radiation area shall have a control device that prevents entry to the area when high radiation levels exist or upon entry causes the radiation level to be reduced below that level defining a high radiation area. [10CFR835, 835.502(b)(1)]
- In other words… Locked and Interlocked
- Additional measures shall be implemented to ensure individuals are not able to gain unauthorized or inadvertent access to very high radiation areas. [10CFR835, 835.502(c)] [ANSI/HPS N43.3-2008, 7.5.3]

Emergency Exit

- No control(s) shall be established in a high or very high radiation area that would prevent rapid evacuation of personnel. [10CFR835, 835.502(d)]
- Emergency exit mechanisms as required by OSHA standards (29 CFR 1910.37) should be provided at all doors, even when interlocked. Emergency entry features for interlocked doors should not be precluded. [DOE G 420.2-1, II.B.3.a.2)iii]
  - This is different than 10CFR835 in that the exit mechanism must be OSHA

NFPA 101, Life Safety Code

- Door assemblies in the means of egress shall be permitted to be electrically locked if equipped with approved, listed hardware that incorporates a built-in switch, provided that the following conditions are met:
  - (a) The hardware for occupant release of the lock is affixed to the door leaf.
  - (b) The hardware has an obvious method of operation that is readily operated in the direction of egress.
  - (c) The hardware is capable of being operated with one hand in the direction of egress.
  - (d) Operation of the hardware interrupts the power supply directly to the electric lock and unlocks the door assembly in the direction of egress.
  - (e) Loss of power to the hardware automatically unlocks the door assembly in the direction of egress.

Story Time

- OSHA requirements for doors
  - Emergency exit devices not attached to door leaf

Warning lights

- All RGD warning lights should be red or magenta for consistency. A sufficient number of lights should be installed so that at least one light is easily visible from all reasonably occupied areas that may have dangerous radiation levels and from reasonable avenues of approach to such areas. [DOE G 441.1-1C, 7.4.0.2]

Audible Warning

- An audible signal should warn personnel that radiation is about to be introduced to the exclusion area. The audible signal should be:
  - Incorporated into the interlock system.
  - Of a frequency or sound pressure level that can be heard over background noise. (ANSI N43.3-2008 5.1.5.1)
  - Generally consistent for all RGDs operated within the same facility so that personnel can immediately recognize the signal's meaning.
  - Intermittent (i.e., pulsating) Klaxon horns are typically used to signal evacuation.
  - Specifications for audible evacuation signals found in ISO 11429:1996 should be used whenever practicable.

Audible Visual Warning

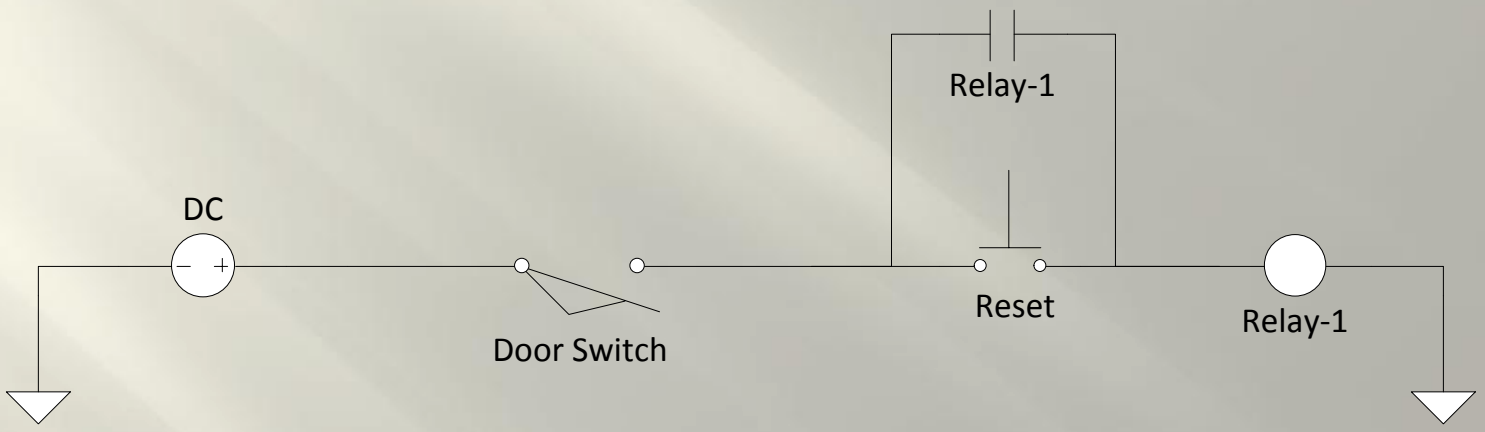
- Visible warning signals should remain on throughout the exposure period.
  - However, they may be turned off for conservation
- Audible and Visual warnings must actuate prior to radiation production giving personnel in the area enough time to safely actuate an emergency shut-off device. [ANSI N43.3-2008 5.1.5.1]
  - During normal operations, constant use of audible signals that can be heard outside the RGD room is discouraged due to the potential desensitization of workers toward responding to alarms. [ANSI N43.3-2008 5.1.3.2]

Interlocks

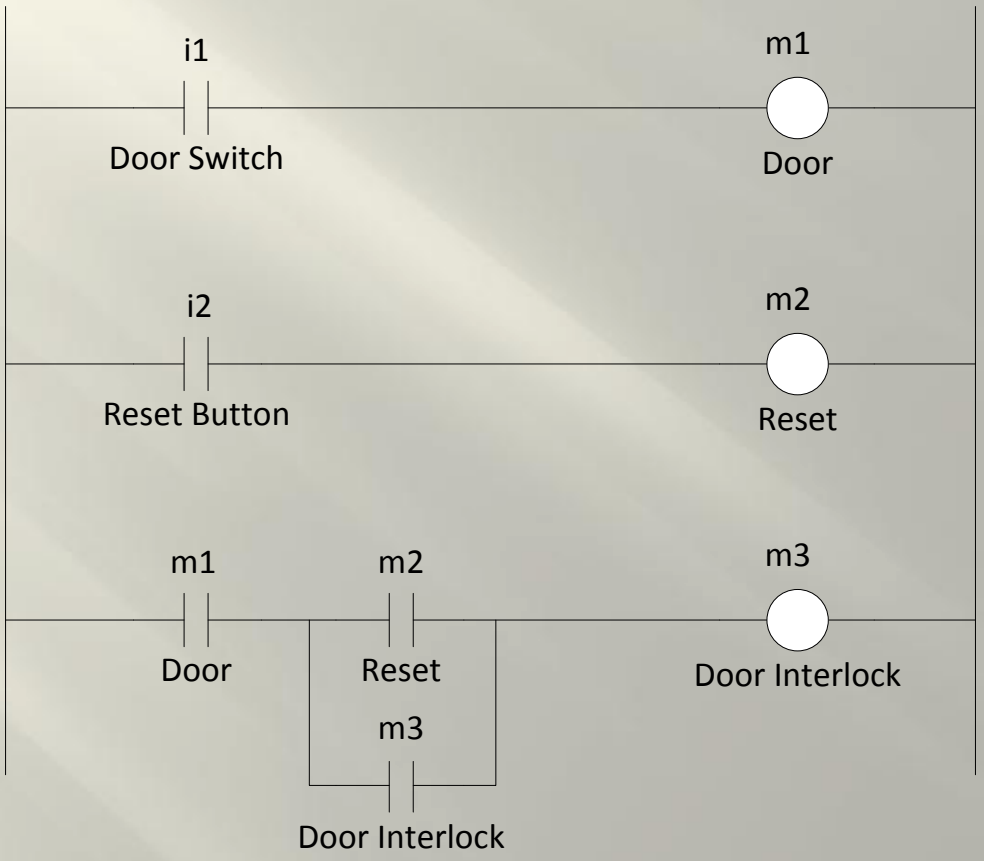
- Interlocks shall be provided to prevent irradiation during personnel access to a radiological exclusion area. [DOE G 441.1-1C, 7.4.0.2] [ANSI/HPS N43.3-2008, 5.1.2]
- If the exposure of any radiation source has been interrupted by the opening of a door or panel to an installation, it shall not be possible to resume operation by merely closing the door or panel. In addition, to resume operation it shall be necessary to manually re-energize a suitable device located on or near the control panel. [ANSI/HPS N43.3-2008, 7.5.4]

Finally, a Circuit!

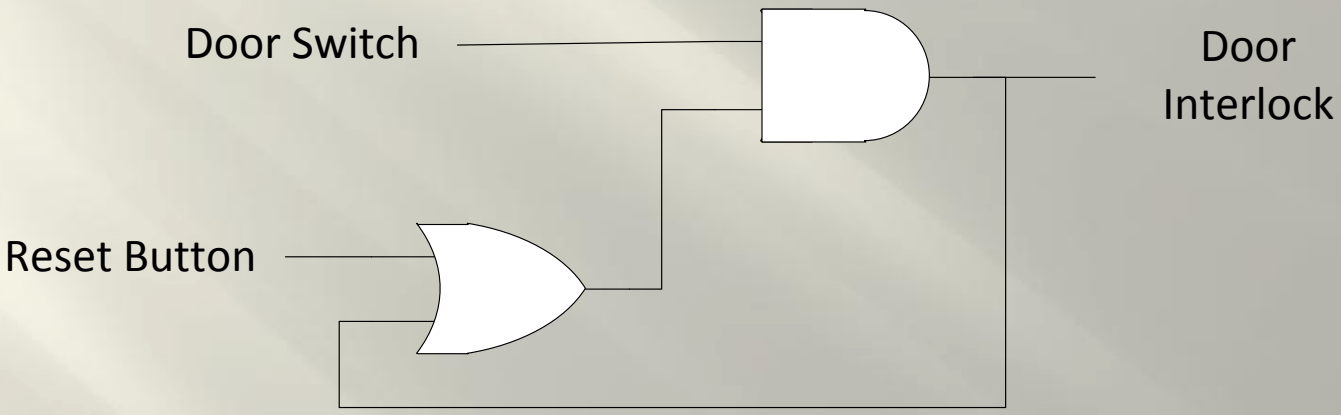
Not possible to resume operation by merely closing the door or panel



PLC Program


i1
Door Switch
m1
Door
i2
Reset Button
m2
Reset
m1
Door
m2
Reset
m3
Door Interlock
m3
Door Interlock

Logic Diagram



Defense-in-Depth

- Additional measures shall be put into place to prevent any unauthorized or inadvertent access to very high radiation areas.[10CFR835, 835.502(c)]
- Duplicate interlocks and other defense-in-depth strategies such as the use of multiple technologies should be considered.
- NCRP Report 88 states, “the decision as to which components should be duplicated rests in large measure on judgments based on reliability and failure criteria and statistics…access control and alarm systems should be selected on the basis of the potential dose to personnel from the radiation source.” [ANSI/HPS N43.3-2008, 7.5.3]

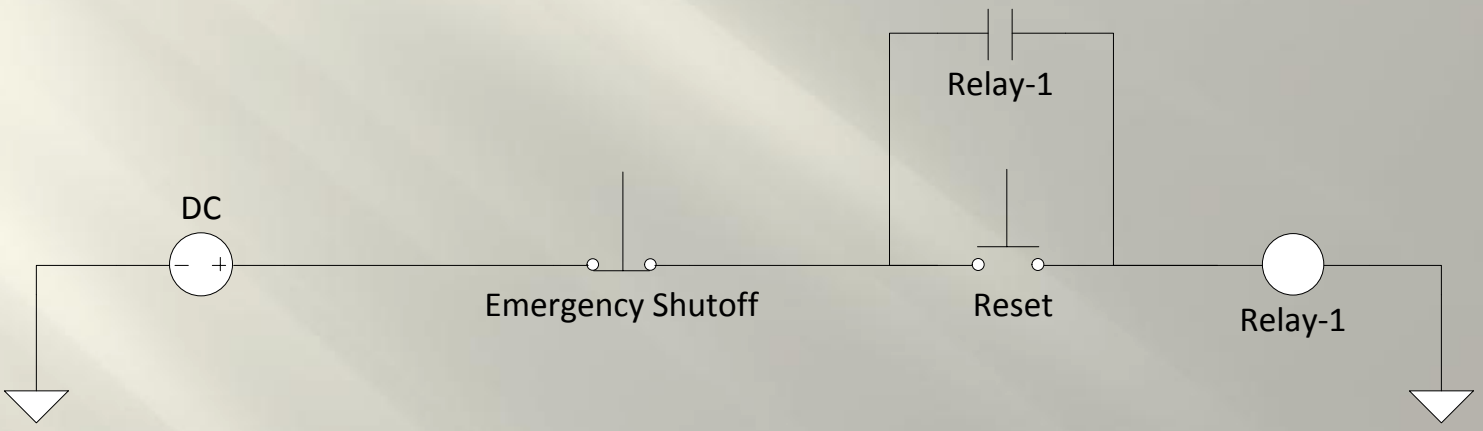
Master Keys

- One or more physical control devices should be used to secure the RGD to prevent unauthorized access and use. The control system governing the production of radiation should be equipped with a lock and key to prevent unauthorized use.
- The key controlling the production of radiation in one RGD should not control the production in another. [DOE G 441.1-1C, 7.4.0.3]

Emergency Shut-Off

- Effective means shall be provided within the enclosure for preventing or quickly interrupting the irradiation.
- The use and function of the device used shall be clearly labeled.
- The device shall be readily accessible.
- Once interrupted, irradiation shall not be able to be resumed unless the switch within the exposure area is reset and the operator control is reset. [ANSI/HPS N43.3-2008, 5.1.5.2]

Also Useful for Emergency Shutoff



Search and Clear

- Exclusion areas shall be searched before the beam is introduced to ensure that no people remain inside. Procedures to ensure the reliability of the search process should be comparable with the design procedures to ensure the reliability of the interlock system. [DOE G 420.2-1, II.B.3.a.2)v(a)]
- Search confirmation buttons, or check stations should be placed to ensure that the search team views each area. [DOE G 420.2-1, II.B.3.a.2)v(a)]
- If entry control is compromised, the interior shall be checked for personnel prior to resuming radiation exposure. [DOE G 420.2-1, II.B.3.a.2)v(c)] [ANSI/HPS N43.3-2008, 7.5.4]

Search and Clear Logic

- The intent of the search is to clear personnel from the radiological area before beam operation.
- There should be two states
  - Search and Clear
  - Search Complete

Search and Clear

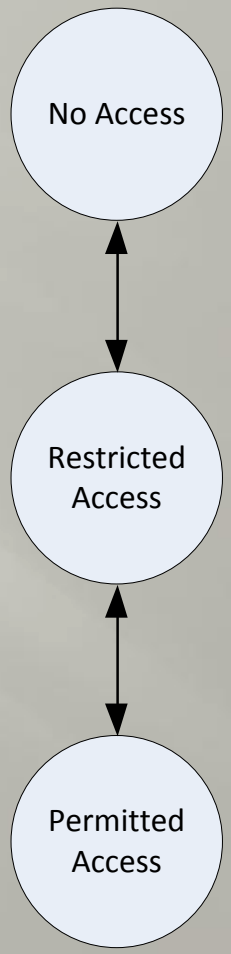
- During the search and clear state
  - Doors should be monitored to make sure no one has entered during the search
  - Doors must have a bypass method to allow searchers to exit the enclosure
  - There should be at least 1 switch in the enclosure to indicate a person has searched the enclosure
  - This state may be time limited to force the search to occur within a certain time frame

Search Complete

- A switch outside indicates the search has been completed
  - The circuit should not reset unless the switch inside has been set
  - The search complete indicates that all interlocks are monitored
  - A multi-state enclosure may bypass some of the interlocks

Multi-State Enclosure

- No Access
  - The enclosure is closed for beam operation
- Restricted Access
  - The enclosure has limited access
  - The access is monitored and recorded
- Permitted Access
  - Free access



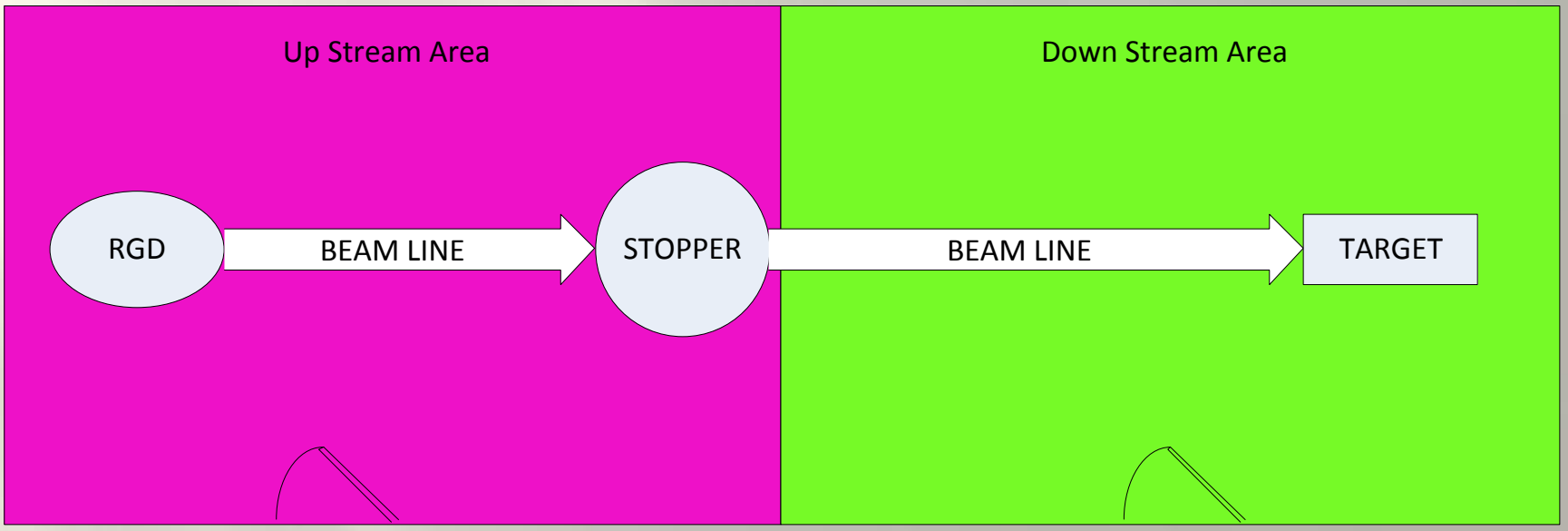
Area Monitors

- Where an area radiation monitor is incorporated into a safety interlock system, the circuitry should be such that a failure of the monitor should either prevent normal access into the area or operation of the RGD. [DOE G 441.1-1C, 7.4.0.2]

Reach back Cascade

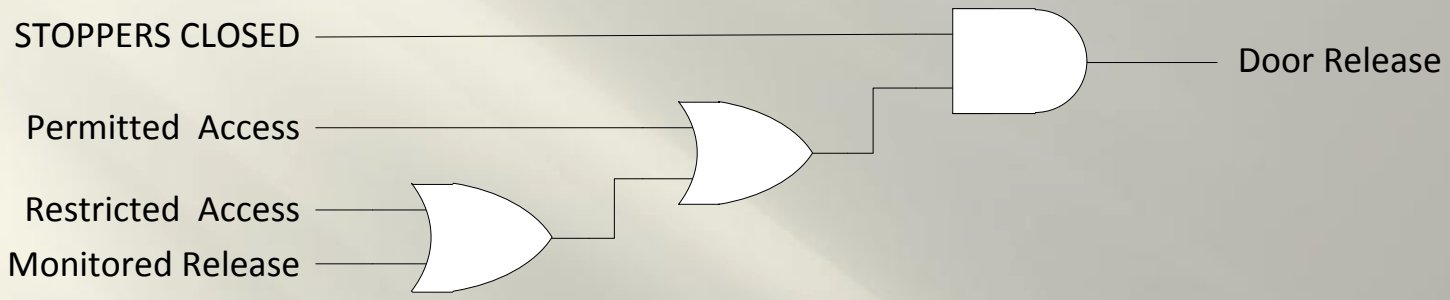
- The status of each critical device should be monitored to ensure that the devices are in the safe condition when personnel access is permitted.
- If the safe condition is lost, then the beam should be inhibited by operation of other critical devices upstream.[DOE G 420.2-1, II.B.3.a.1)iii(b)]

Reach back Cascade

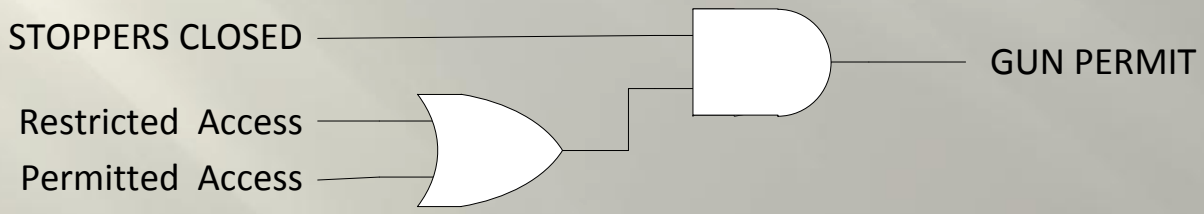


Reach back Cascade

Control access to the enclosure

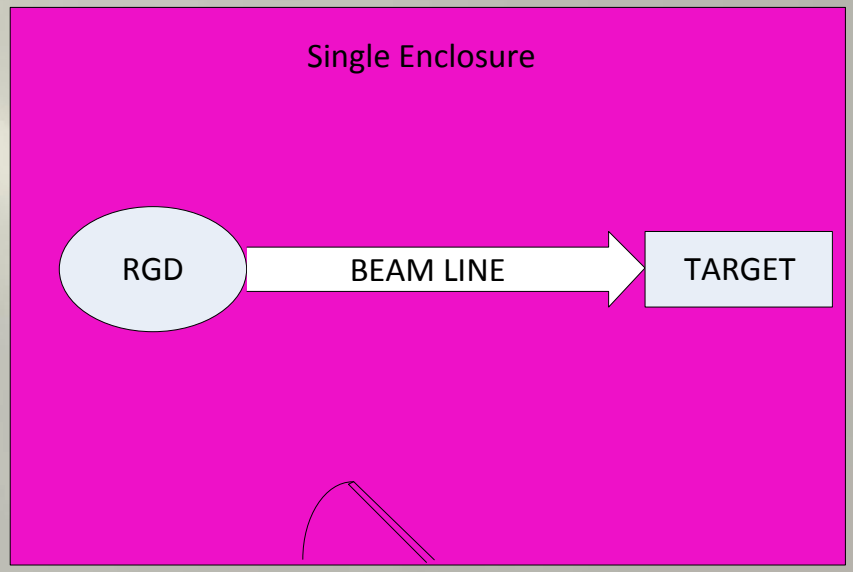


Reach back if the safe condition is lost



Discussion

- What are your options for a single enclosure machine?



Machine operation

- Safety devices should not be used as routine shutdown mechanisms.
- The equipment design and procedures should provide for an orderly means of turning off beams other than activation of an entry interlock before entry is attempted into a controlled access area.
- The entry interlocks should not constitute the normally-used means of disabling beam.
- Interlocked safety devices should be employed to maintain the disabled status of beams.

  [DOE G 420.2-1, II.B.3.a.2)i]

Lots of Information

- Questions?
- Need to look at something again?
- Stories or tall tails?