

# 4th RadSynch Workshop

---



R. Casey

Redundancy Requirements for Critical Devices

June 7, 2007

1

# Radiation Interlock Systems

---

- Must operate with high reliability
- Failure of any one component should not result in unsafe condition
- Redundancy is often expected in high dose situations
- For example – all U.S. synchrotrons have redundant parallel chains for monitoring status of doors and shutter(s) controlling access to high dose beams

# Critical Devices

---

- Specific accelerator or beam line devices that are used to ensure that the accelerator beam is either inhibited or can not be steered into area where people are present
- Examples
  - Beam shutters
  - Steering magnets
  - Systems that operate on the RF, injector or ion source to inhibit the beam (i.e. eliminate the radiation source)

# Examples of Critical Devices in NSLS-II

---

- Safety shutter in front end blocking beam into FOE
- Safety shutter in monochromatic beam line blocking beam into hutch
- Beam shutter in transport line from linac to booster
- Dipole which bends beam into booster from linac
- Linac or ring RF

# Example of Critical Device Role In Interlock System

---

## Access to experimental hutch

- Safety in hutch is provided through a shutter which establishes the safe condition for access (shutter is “critical device”)
- 2 independent interlock chains are provided, each monitoring status of hutch, shutter, and door(s)
- Any inconsistency in interlock logic requirements will result in order for shutter to close and a reach back to trip the stored beam by turning off RF and ring magnets

# The Issue

---

Are redundant beam shutters required for safety?

# Redundancy Requirements (Continued)

---

- DOE Accelerator Safety Order – Two or more critical devices should be considered for use in interlock systems where a very high radiation area (500 rad/hr) can be produced during operations
- BNL Requirements - For fields  $> 50$  Rem/hr
  - Two independent systems, each of which will interrupt machine operation if the area is improperly entered.
  - The fail-safe & redundant character of the interlock system is vital. The system shall be designed so that the most common failure mode results in a safe condition, and any single failure shall not result in loss of protection

# BNL Interlock Requirements

Requirement Category	Redundant Interlock Protection Systems	Fail Safe	Enforced Sequence Search <small>(Where Appropriate)</small>	Operator Action Required for Restart	Periodic Testing
High Risk	Yes	Yes	Yes	Yes	Yes
Moderate Risk	No	Yes	Yes	Yes	Yes
Low Risk	No	No	No	Yes	Yes
Routine Risk	No	No	No	No	Yes

The probability for the interlock system to fail shall be extremely remote if High Risk hazards exist within the protected boundary.”

High risk defined as potential to exceed 100 rem

# What is the current practice at NSLS?

---

Single beam shutter monitored by two independent interlock logic chains. Any “unsafe” condition (e.g. shutter open when hutch not secure) results in each chain reaching-back to ring RF and ring magnet power supplies

# What is the practice elsewhere?

---

- APS – 2 critical devices
- SLAC - 3 critical devices
- ALS – 1 critical device

# So why would you provide redundant critical devices

---

- Presumably the risk of unsafe failure is lower
- But how low do we wish to go?  
i.e. What is the risk with a single shutter and what risk is acceptable

# Results of Analysis Conducted at SRS<sup>1</sup>

---

- Concluded that the overall risk of a person being in hutch when radiation was present was  $2.6 \times 10^{-8}$  per hutch search
- Greatest risk was related to human error in search process
- Interlock failure estimated at 0.5% of overall risk or  $1.3 \times 10^{-10}$  (per entry)
- Their estimate based on failure of 2 shutters to close and door lock does not engage
- SRS decided to add an additional reach-back to dump beam if second shutter fails to close.

<sup>1</sup> Alexander, Heron, & Quinn, “A Report of the Review and Formal Analysis of the SRS Personnel Safety System”; Proceedings of the 2001 Particle Accelerator Conference, Chicago

# NSLS conducted a failure mode analysis of its interlock systems

---

- We wanted to use it as a basis for extending our test period from 6 months to 12 months. We excluded failures related to human error
- We used an engineer from another BNL department who routinely conducts failure mode analyses for the nuclear power industry. He also has had substantial involvement with the space industry
- Various failure scenarios were evaluated and the failure probability calculated using generic failure data for relays, switches, etc
- However, use of results required definition for “extremely remote” risk of failure.

# BNL Risk Matrix

						FREQUENT	PROBABLE	OCCASIONAL	REMOTE	EXT. REMOTE	IMPOSSIBLE
						Likely to occur repeatedly in life cycle	Likely to occur several times in life cycle	Likely to occur some time in life cycle	Unlikely to occur in life cycle but possible	Likelihood of occurrence ~ zero	Physically impossible to occur
CONSEQUENCE											
>100 rem to an individual						HIGH RISK	HIGH RISK	HIGH RISK	MODERATE RISK	LOW RISK	ROUTINE RISK
>25 rem						HIGH RISK	HIGH RISK	MODERATE RISK	LOW RISK	LOW RISK	ROUTINE RISK
> 5 rem						MODERATE RISK	MODERATE RISK	LOW RISK	LOW RISK	ROUTINE RISK	ROUTINE RISK
< 2 rem						ROUTINE RISK	ROUTINE RISK	ROUTINE RISK	ROUTINE RISK	ROUTINE RISK	ROUTINE RISK

# Hazard Probability Rating Levels Taken from LCLS SAD

Category	Category Estimated Range of Occurrence Probability (per year)	Description
High	$> 10^{-1}$ year	Event is likely to occur several times in a year
Medium	$10^{-2}$ to $10^{-1}$ year	Event is likely to occur annually
Low	$10^{-4}$ to $10^{-2}$ year	Event is likely to occur during the life of the facility or operation
Extremely Low	$10^{-6}$ to $10^{-4}$ year	Occurrence is unlikely or the event is not expected to occur during the life of the facility or operation
Incredible	$< 10^{-6}$ year	Probability of occurrence is so small that a reasonable scenario is not conceivable.

# Proposed Risk Matrix for Evaluating Interlock Failure Probability

	Probable Likely to occur several times in life cycle > 10 <sup>-1</sup> /yr	Occasional Likely to occur sometime in life cycle 10 <sup>-2</sup> - 10 <sup>-1</sup> /yr	Remote Unlikely to occur in life cycle, but possible 10 <sup>-4</sup> - 10 <sup>-2</sup> /yr	Extremely Remote Likelihood of occurrence ~ zero 10 <sup>-6</sup> - 10 <sup>-4</sup> /yr	Impossible < 10 <sup>-6</sup> /yr
Consequence of Occurrence					
High Consequence - Can deliver > 100 rem to an individual	High Risk	High Risk	Moderate Risk	Low Risk	Routine risk
Medium Consequence - Can deliver > 25 rem to an individual	High Risk	Moderate Risk	Low Risk	Routine Risk	Routine Risk
Low Consequence - Can deliver > 5 rem to an individual	Moderate Risk	Low Risk	Routine Risk	Routine Risk	Routine Risk
Extremely Low - Can deliver <5 rem to an individual	Low Risk	Routine Risk	Routine Risk	Routine Risk	Routine Risk

# Many scenarios evaluated - one scenario of interest

---

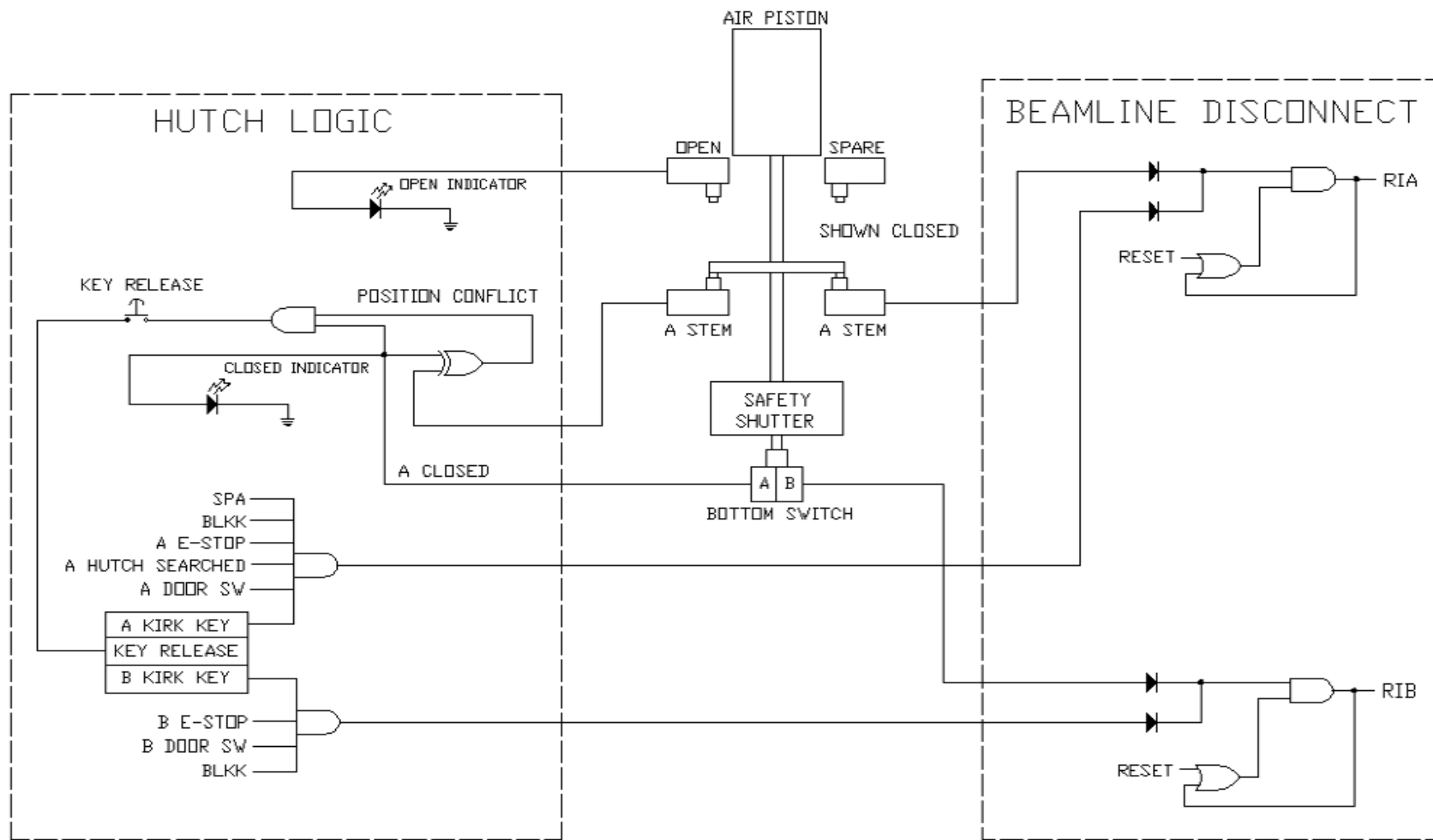
- Scenario – person enters hutch using proper procedure; interlock logic is satisfied, but in fact shutter did not close
- Risk of this failure/event was calculated at:
  - 1.12 E-7 for 6 month test interval
  - 4.5 E-7 for 12 month test interval
- Risk is driven by common mode failure of 4 switches

# Is $1 \text{ E-}7$ / event an acceptable risk

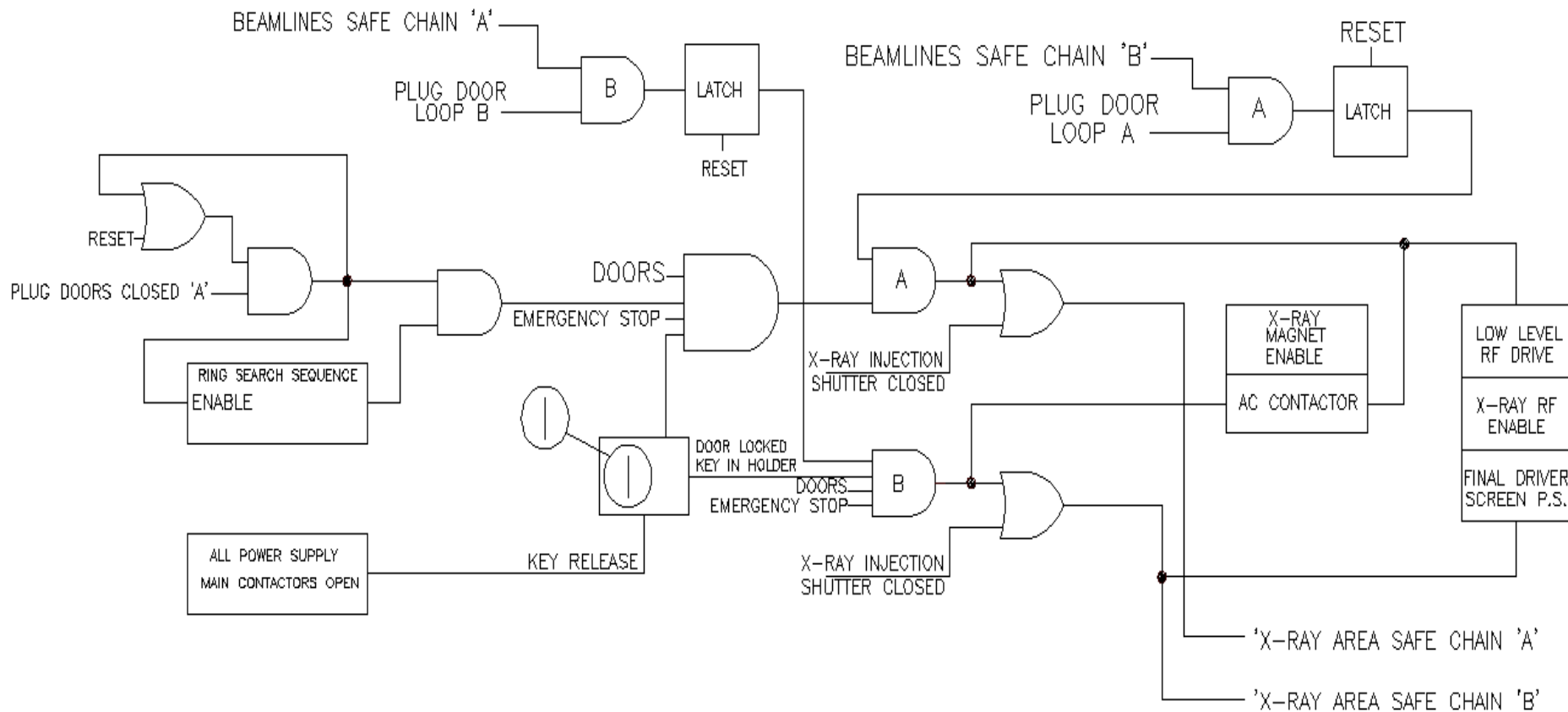
---

- Risk is calculated per demand
- NSLS has 60 hutches which are accessed many times per day
- It is easy to estimate that the doors are opened more than 10,000 times per year which would produce a facility risk of  $1 \times \text{E-}3$  per year

# NSLS STANDARD SHUTTER LOGIC

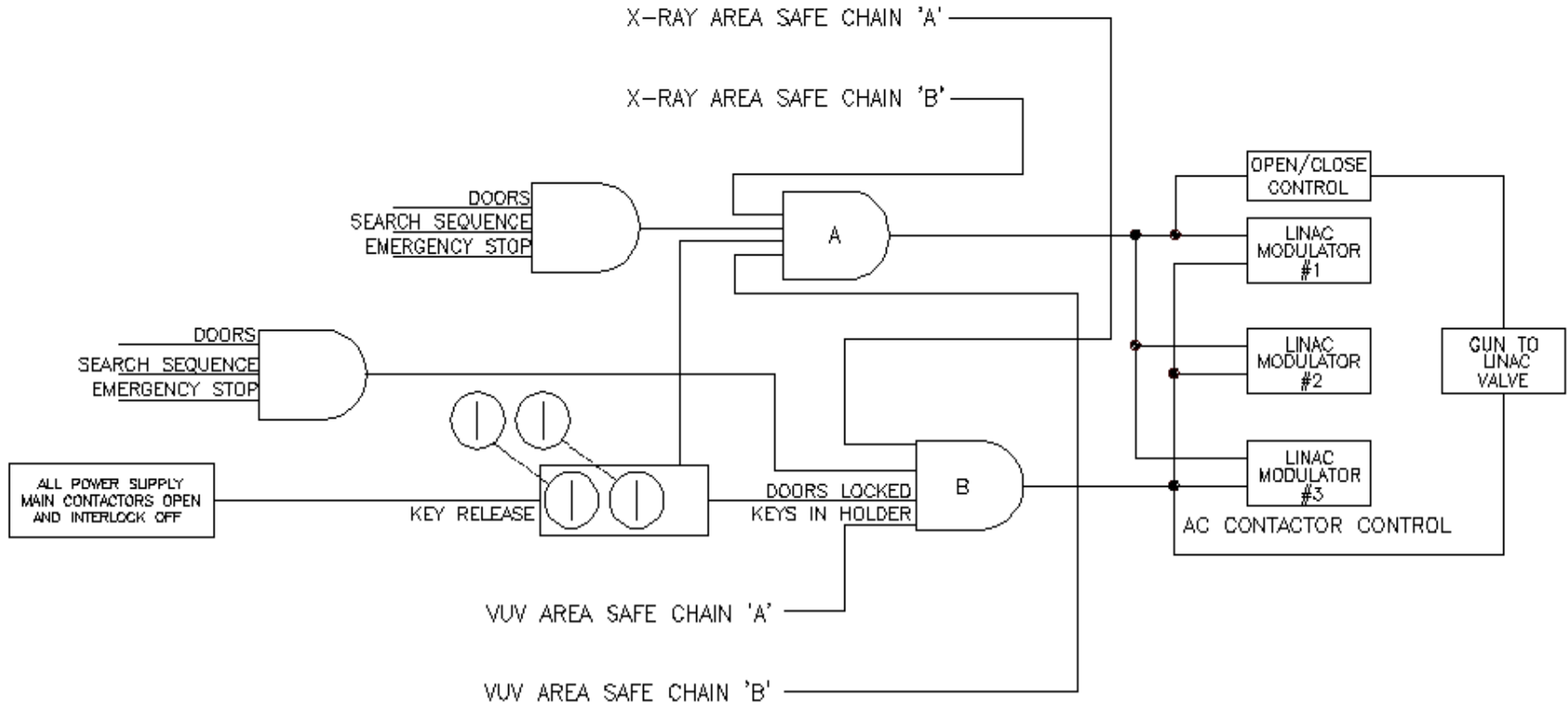


# NSLS X-RAY INTERLOCK LOGIC



NSLS-X-RAY INTERLOCK LOGIC BLOCK DIAGRAM

# NSLS INJECTOR INTERLOCK LOGIC



NSLS-INJECTOR INTERLOCK LOGIC BLOCK DIAGRAM

# There Are Several Ways To Reduce Failure Risk Of Current Design

---

- Increase the diversity of the shutter position indicators  
e.g. sense position with light beam rather than a mechanical switch
- Install radiation sensing device in hutch interlocked to hutch access and stored beam
- Install an additional beam shutter

# Conclusions

---

- Failure mode analysis was a useful study of our interlock design
- Using the data from this study, we conclude that independent interlock chains monitoring a single beam shutter with reach-back to RF and ring magnet power supplies achieve very low and acceptable failure rates
- Common cause failure is an important consideration and can markedly increase the probability of failure
- Redundant safety shutters can reduce failure probability also by a factor of 1000

# Conclusion for NSLS-II Design

---

- Two independent beam shutters are not required to provide for adequate risk reduction
- Two interlock chains each independently monitoring beam line shutter/hutch configuration and each with reach-back capability to ring RF and magnet power supply are needed
- Diversity & isolation of interlock chains to prevent common cause failure is a very important consideration