Redundancy Requirements for Critical Devices

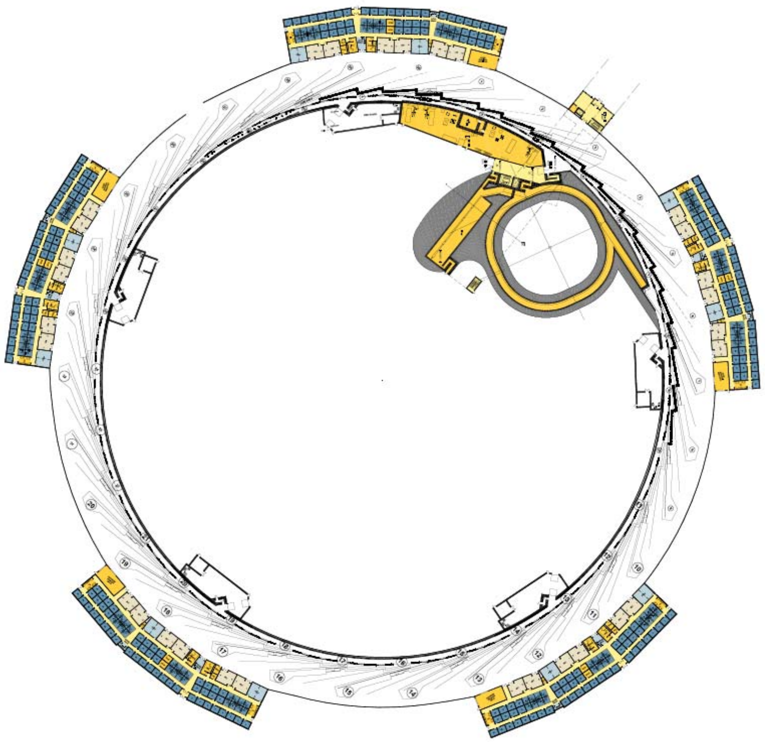
R. Casey

August 8, 2007

Office of Science
U.S. DEPARTMENT OF ENERGY

BROOKHAVEN NATIONAL LABORATORY
BROOKHAVEN SCIENCE ASSOCIATES

NSLS-II Design



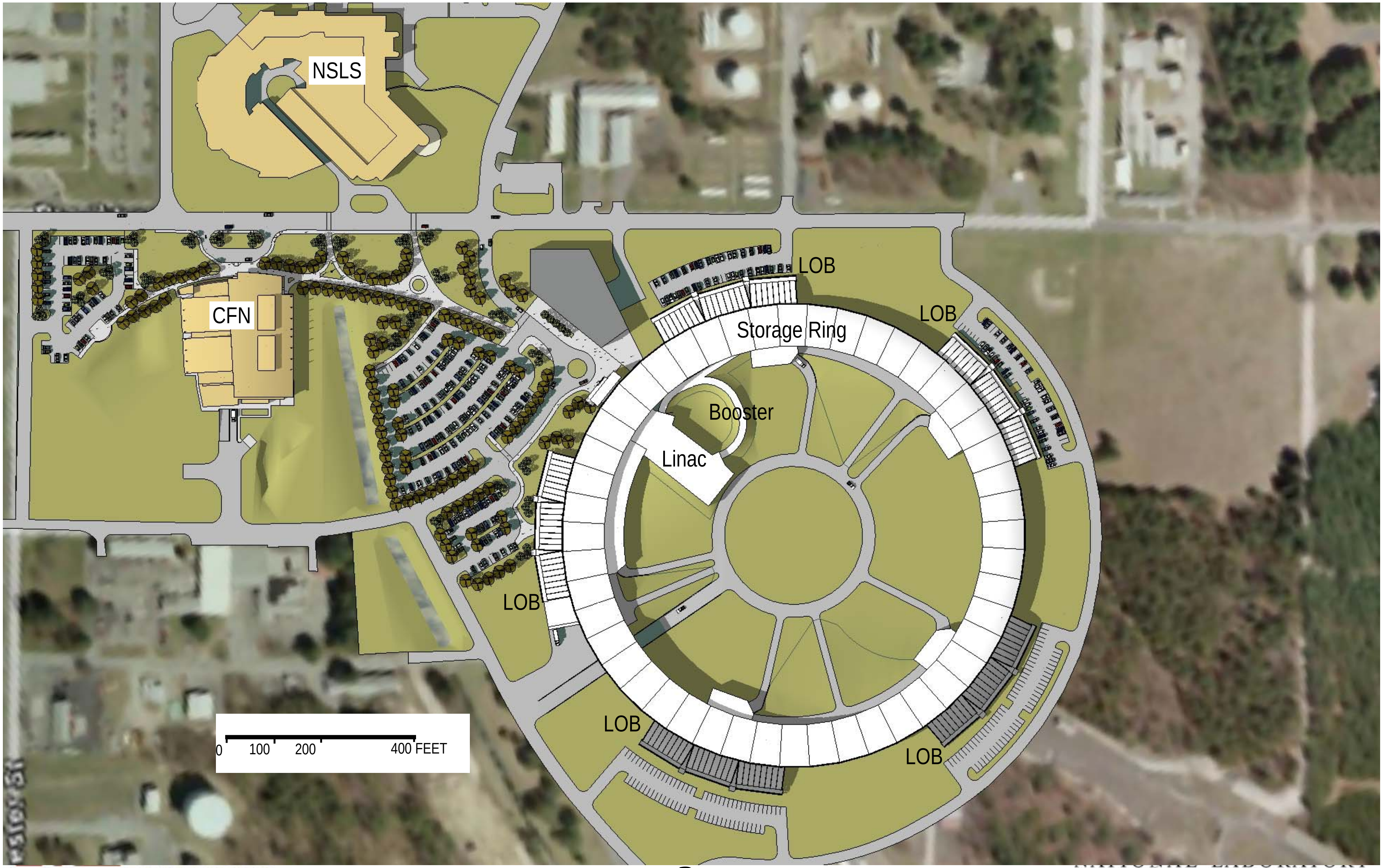
NSLS-II Machine Concept

- 3 GeV Electron Storage Ring
- Large Circumference (791.5 m)
- “Compact” (~158m) booster
- Large Current (500 mA)
- Top-Off Operation
- Ultra-high brightness beams

Office of Science
U.S. DEPARTMENT OF ENERGY

BROOKHAVEN NATIONAL LABORATORY
BROOKHAVEN SCIENCE ASSOCIATES

Conceptual NSLS-II Site Plan

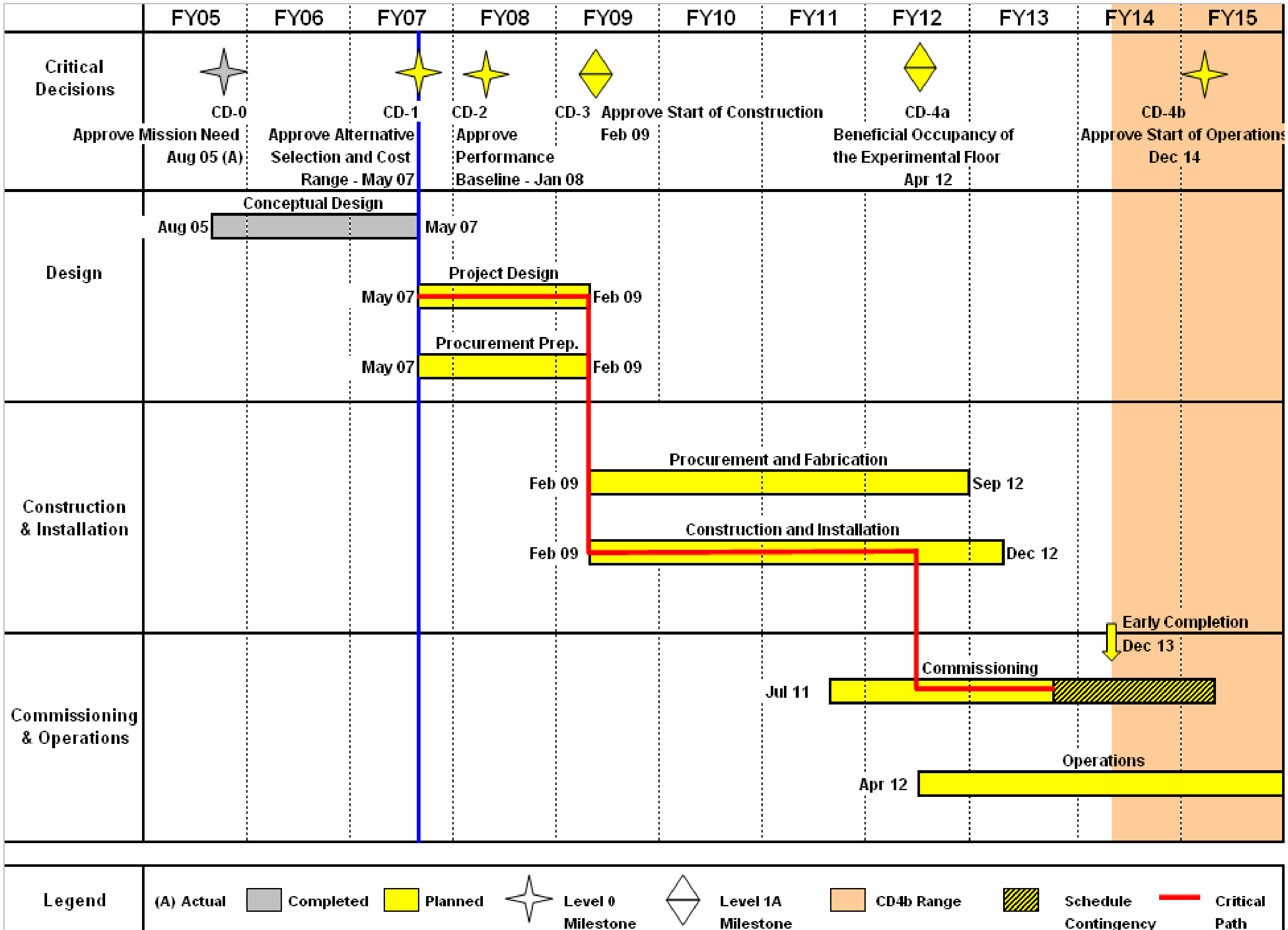


Preliminary Cost Estimate ($M)

Project Management	40
Acelerator Systems	181
Conventional Facilties	210
Experimental Facilties	74
Contingency (38% of costs listed above)	190
Total Estimated Costs (TEC)	695
Research and Development	60
Pre-Operations	95
Other Project Costs (OPC)	155
Total Project Cost (TPC)	850

Cost Range $750M to $900M

Preliminary Summary Schedule



Office of Science
U.S. DEPARTMENT OF ENERGY

BROOKHAVEN NATIONAL LABORATORY
BROOKHAVEN SCIENCE ASSOCIATES

Critical Devices

- Specific accelerator or beam line devices that are used to ensure that the beam is either inhibited or can not be steered into an area where people are present (DOE Guidance)
- The final part of an interlock system that implements the physical action necessary to achieve a safe state
- Examples
  - Steering magnets
  - Beam stops
  - collimators
  - Systems that operate on the 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
- Safety shutter (photon shutter) in monochromatic beam line
- Power to dipole which bends beam into booster from linac
- Beam shutter in transport line from linac to booster
- Power to RF Cavities in main ring or to Linac modulators

Comments on Radiation Interlock Systems

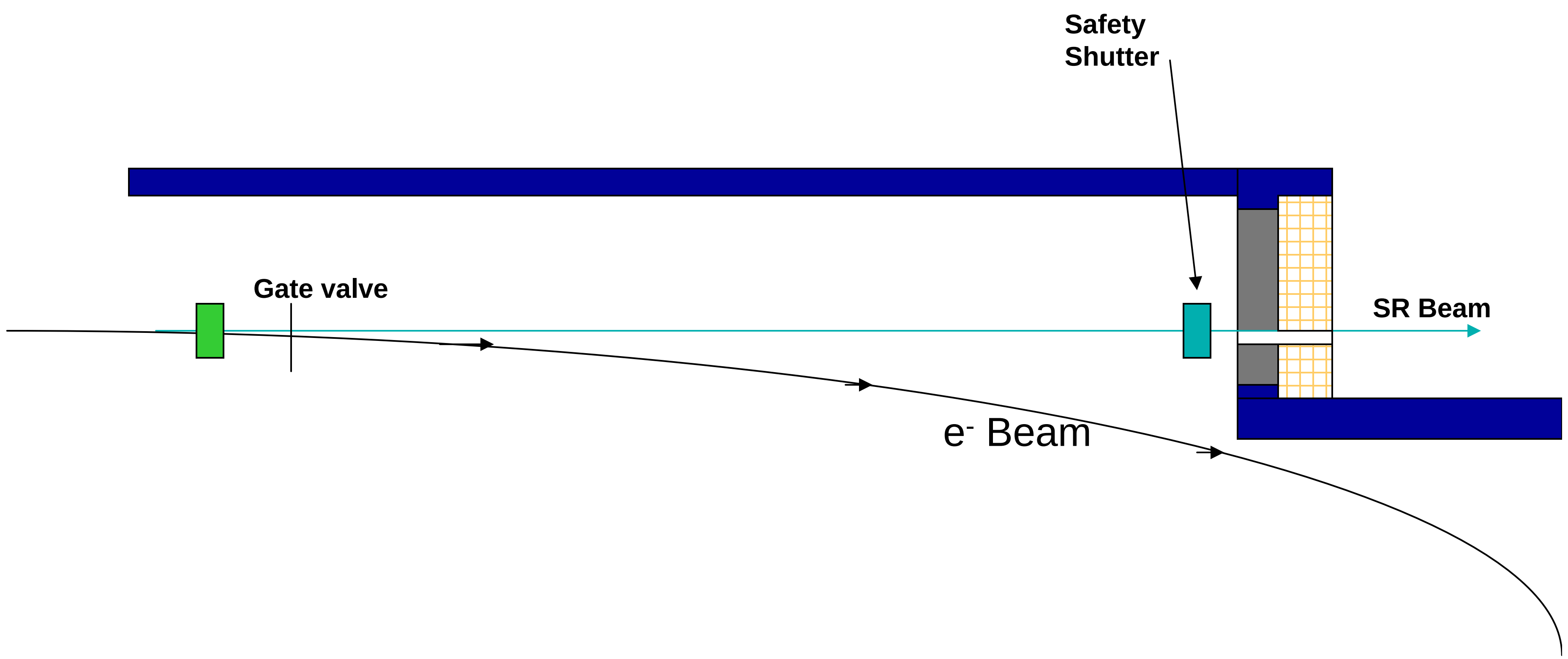
- Must operate with high reliability
- Very detailed design requirements have been established
- Failure of any one component should not result in unsafe condition
- Redundancy is often required based on consequence of unintended exposure
- For example – all U.S. synchrotrons have redundant parallel chains for monitoring status of doors and shutters controlling access to high hazard radiation areas

Example

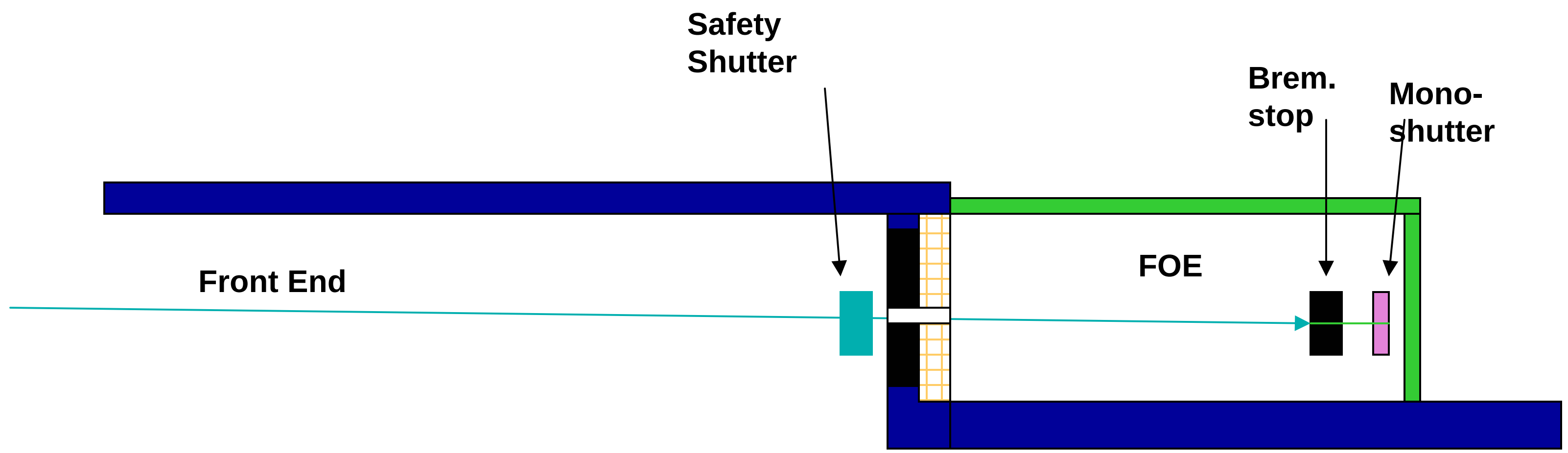
Access to experimental hutch

- Safety in hutch is ensured through a shutter which establishes the safe condition for access (shutter is "critical device")
- Redundant interlock chains are provided, each monitoring status of hutch, shutter(s), and door(s)
- Any inconsistency in logic requirements will result in order for shutter to close and a reach-back to trip beam

Schematic of Beamline Front End Shielding Components



Schematic of First Optics Enclosure Shielding Components



Redundancy Requirements

DOE Health Physics Manual of Good Practices for Accelerator Facilities [SLAC 327 (1988)]

- Duplicate circuits or redundant components should always be used in critical applications. The chains should remain independent and not neck down to a single connection. Independence should be carried all the way from duplicate sensors through to the devices or mechanisms that shut off the radiation source. Wherever possible, two different methods should be in place to remove the beam or radiation source.
- Circumstances may exist where redundancy is not required…. Whether or not redundancy is required must be evaluated and decided by risk analysis processes…

Redundancy Requirements (Continued)

- DOE Accelerator Safety Order Guidance – 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. The specification and use of critical devices should be governed by a documented criterion.
- 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, the beam should be inhibited by operation of other critical devices upstream.

What is the practice for Light Sources?

- APS – 2 safety shutters for access to hutch
- SSRL – 2 safety shutters for access to hutch
- ALS – 1 safety shutter for access to hutch
- NSLS – 1 safety shutter for access to hutch
- Most European light sources have 1 safety shutter
- Practices for similar devices at other types of accelerators has not been reviewed

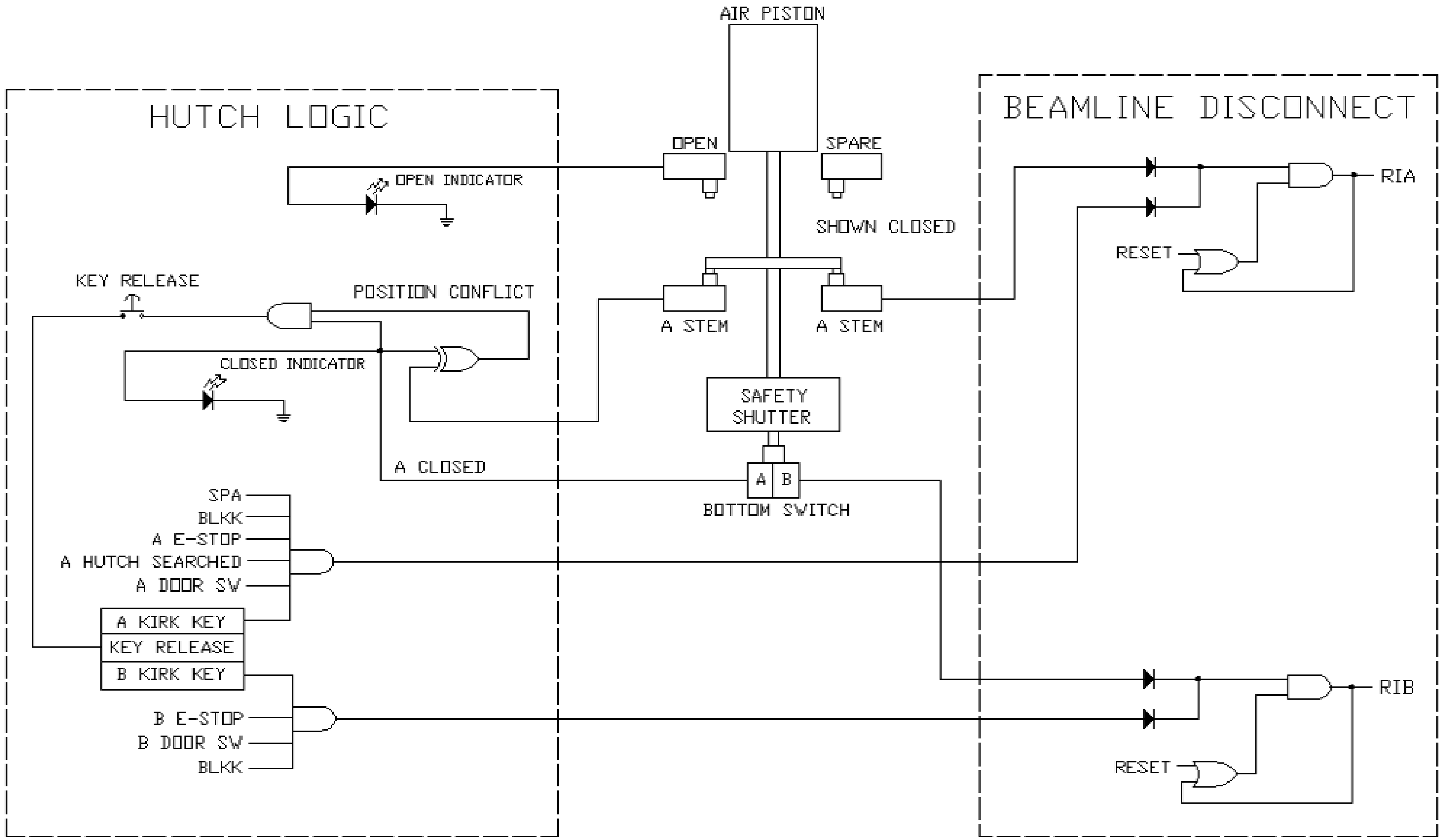
How do we interpret DOE Accelerator Safety Order Guidance?

- What does the guidance document mean when it states that we should consider two or more critical devices?

- Do we need a better definition of critical devices?

  e.g. What constitutes the critical device for beam line hutches?

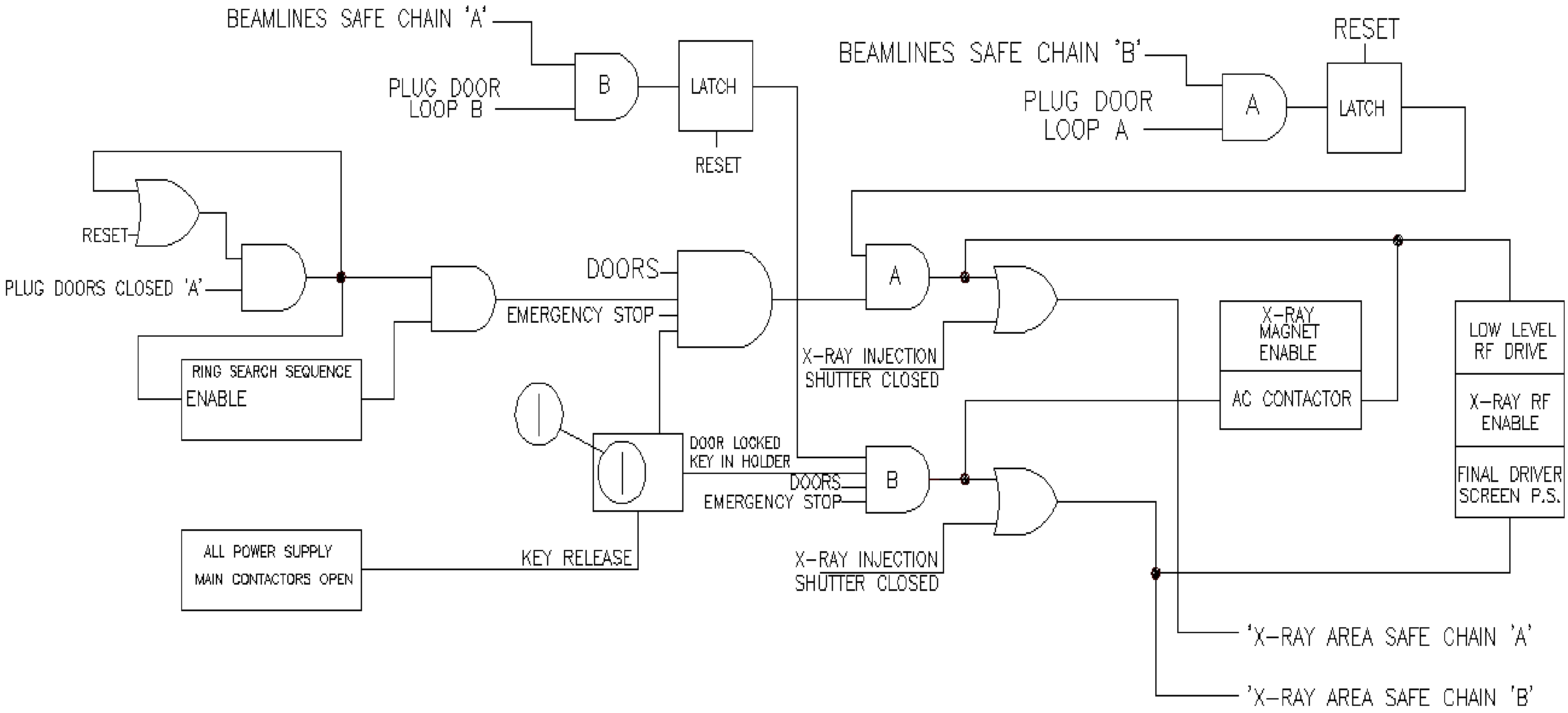
NSLS STANDARD SHUTTER LOGIC



Office of Science
U.S. DEPARTMENT OF ENERGY

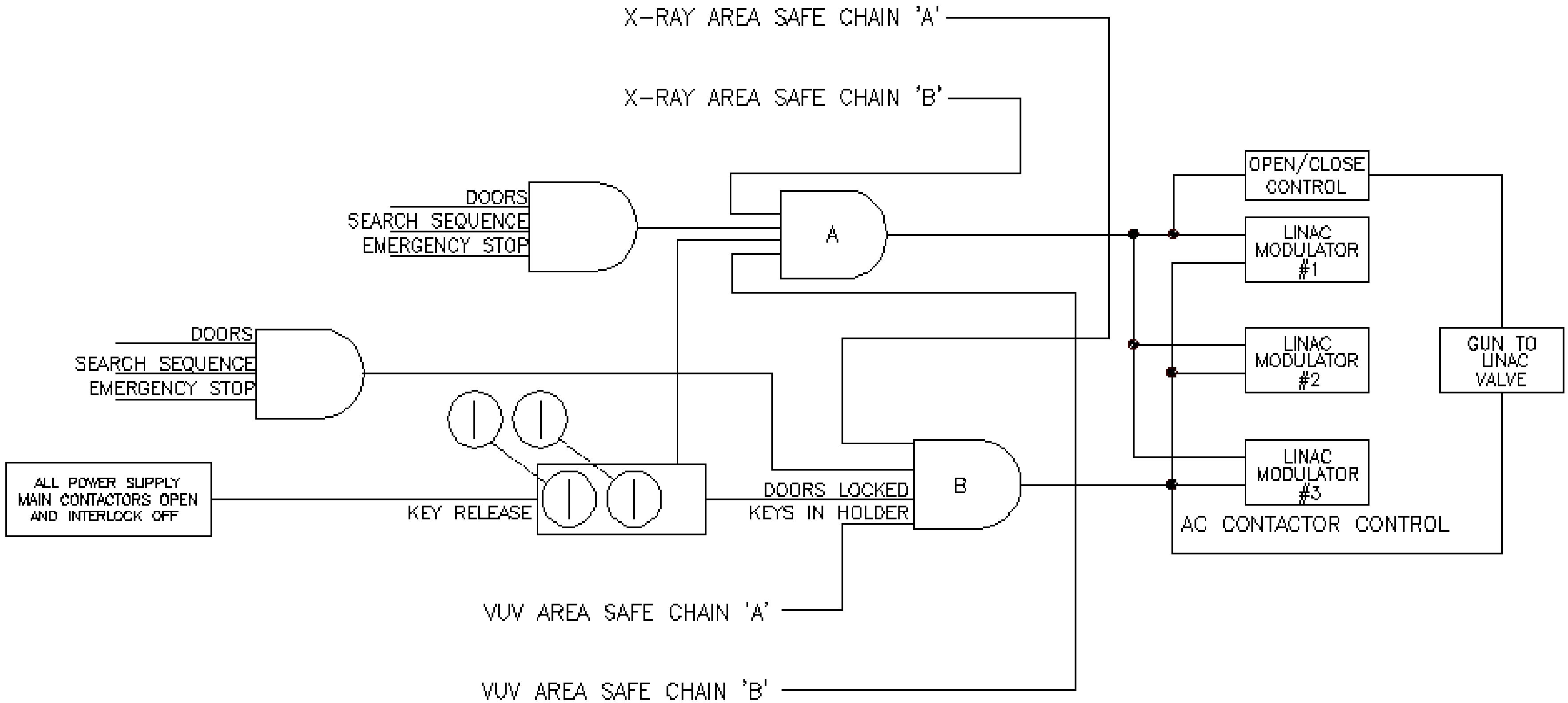
BROOKHAVEN NATIONAL LABORATORY
BROOKHAVEN SCIENCE ASSOCIATES

NSLS X-RAY INTERLOCK LOGIC



NSLS-X-RAY INTERLOCK LOGIC BLOCK DIAGRAM

NSLS INJECTOR INTERLOCK LOGIC



NSLS–INJECTOR INTERLOCK LOGIC BLOCK DIAGRAM

Office of Science
U.S. DEPARTMENT OF ENERGY

BROOKHAVEN NATIONAL LABORATORY
BROOKHAVEN SCIENCE ASSOCIATES

Follow-up actions to this discussion

- We need to clarify BNL requirements for interlock systems
- We should develop risk based criteria for determining interlock redundancy requirements