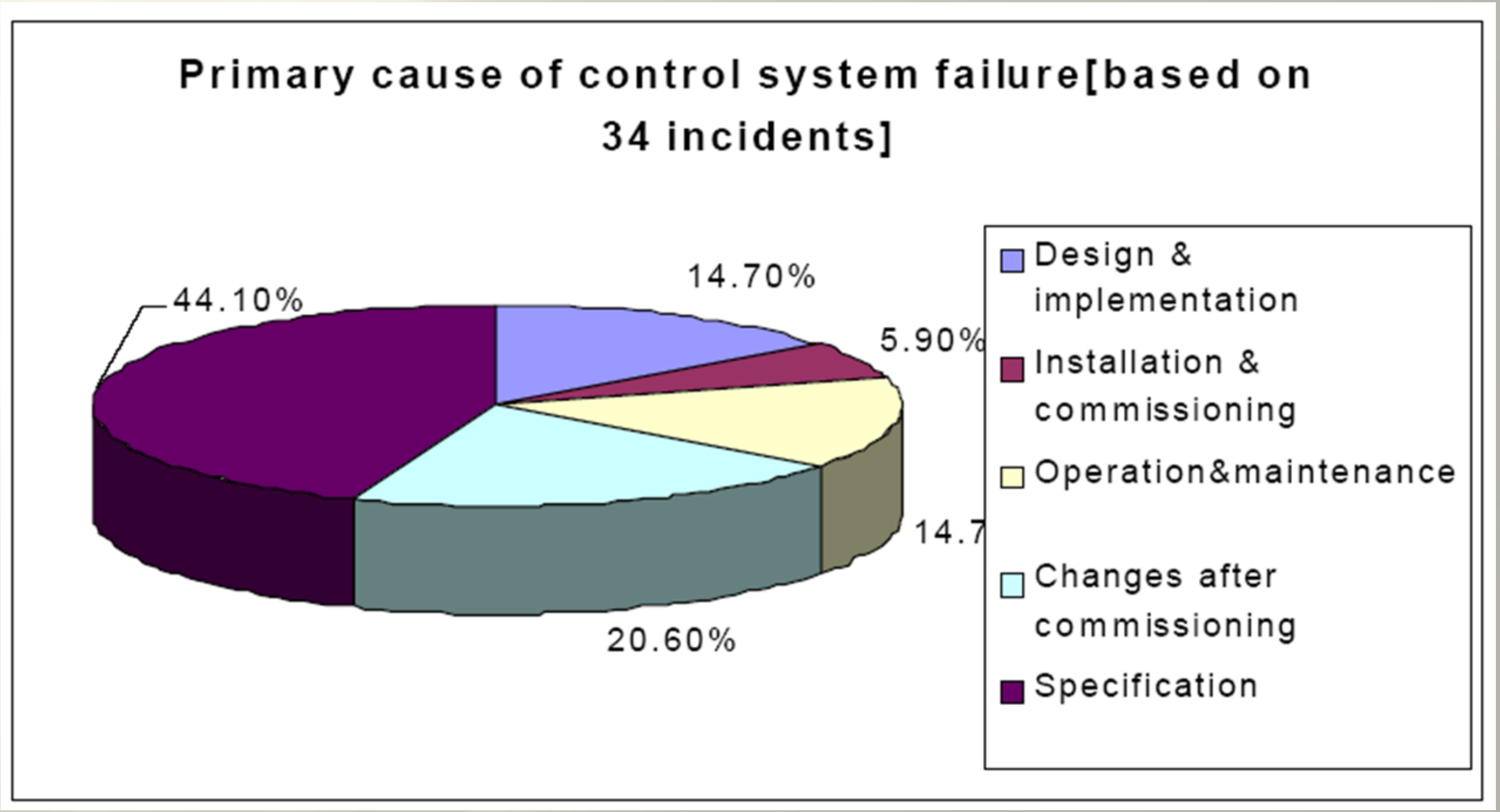
Controlling Risks
Installation, Certification and Testing

HSE Report on Causes of Safety System Failure

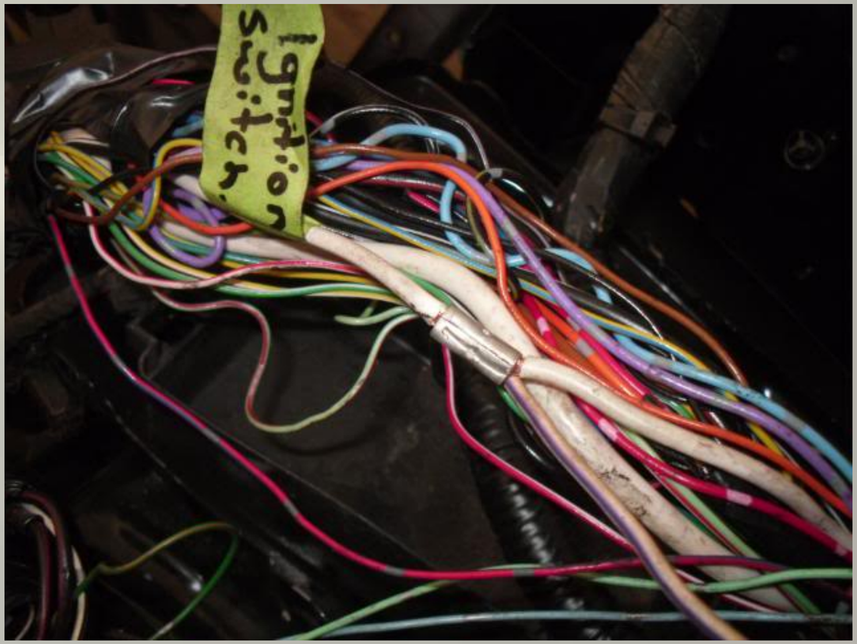


Installation

- Individuals responsible for installing radiological interlock systems must have the appropriate education, training and skills to complete the installation with minimal errors.
- Task complexity and associated hazards should dictate the technical level of skills and managerial level of oversight necessary for the work to be completed.

Installation Management

- Sufficient oversight should be provided by the lead engineer to ensure that the installation is to laboratory standards



Protection of Components

- System components should be protected from damage, tamper resistant, and conspicuously labeled to reduce the likelihood of inadvertent modification and note that tampering is strictly forbidden. [DOE G 420.2-1, II.B.3.a.4)i]
- Cable runs outside of cable trays should be armored cable or run in conduit.[DOE G 420.2-1, II.B.3.a.1)ii]
- While the purpose of locking these areas is to maintain a high level of positive access control, it is recognized that these controls cannot absolutely prevent determined circumvention of the physical barrier such as with the use of wire cutters or unbolting the hinges to a doorway. Instances of such determined circumvention should be addressed with appropriate disciplinary action.

Verification

- Verification: Verification is a quality control process that is used to evaluate whether a product, service, or system complies with regulations, specifications, or conditions imposed at the start of a development phase.
  - A verification plan should check that the hardware is installed correctly and meets the intent of the specification
  - The verification may be as simple as a spreadsheet to check that everything was addressed

Validation

- Validation: Validation is a quality assurance process of establishing evidence that provides a high degree of assurance that a product, service, or system accomplishes its intended requirements.
  - ***ev'·i·dence,*** noun: The available body of facts or information indicating whether a belief or proposition is true or valid

Validation Procedures

- Devices that have a bearing on radiation protection must be tested for proper operation. These include audible or visible warning signals, interlocks, emergency-off devices, timer delay switches, and mechanical or electrical devices that restrict positioning of the radiation source.
- Validation test procedures should be approved by the Interlock Engineer and a person who is actively involved in the operation of the facility.
- The successful execution of a validation test procedure should be acknowledged by the qualified and authorized test leader and a line manager who is actively involved in the operation of the facility.

Validation Procedure Content

- Validation test procedures must include
  - descriptions of the tasks to be performed
  - appropriate safety and health precautions and controls
  - requirements for initial conditions to be verified
  - operating conditions to be maintained
  - data to be recorded

Procedures

- Interlock test procedures must have sufficient detail to ensure a complete functional test of the interlock system.
- Testing should be executed with a check sheet with a check-off for each observed response, thus providing an auditable record.

  [DOE G 420.2-1, II.B.3.a.5)iii]

Interlock Test Procedure

- A typical interlock test procedure would include: (a) the objective of the procedure,

  (b) identification of the hazards associated with the activity and safety and health precautions/controls to be applied during the activity,

  (c) roles and responsibilities for individuals or organizations as they pertain to the successful execution of the procedure,

  (d) detailed instructions for performing the task,

  (e) requirements for record keeping and logs, and

  (f) review and approval status, and the effective date.

  [DOE G 420.2-1, II.A.5.a]

Functional Testing

- The functional test of the interlock system should exercise the system inputs and verify each protective response.
- If a digital system using software in mission critical applications is employed, then both “black box” functional testing and “white box” structural testing should be performed where the known safety functions are tested against likely input parameters as well as the potential mis-use of the system.
- The structural testing should include a verification and validation program for the life cycle of the code.

  [DOE G 420.2-1, II.B.3.a.5)iii]

Black Box vs. White Box

- **Black box test:** Black Box testing is a technique that uses the system requirements specification to select the test data used to examine the outputs.
  - The test is a functional test of the system requirements without regard to the engineering design.
- **White box test:** White Box testing is a technique that uses explicit knowledge of the internal workings of the system to select the test data used to examine the outputs.
  - The test is valid only for determining if the program diverges from its intended functionality. White box testing does not account for errors caused by omissions.

Critical Devices

- **Critical devices:** Critical devices are specific accelerator or beam line components that are used to ensure that the accelerator beam is either inhibited or cannot be steered into areas where people are present.
- It is important that critical devices are tested in their operating configuration, and at least once during the test the system should be exercised from end to end. For example, it should be verified that opening an entry door causes the expected result at the RGD.

  [DOE G 420.2-1, II.B.3.a.5)iii(c)]

Redundancy and Fault Tolerance

- Integrity of redundant interlocks should be determined.

  [DOE G 420.2-1, II.B.3.a.5)iii(b)]
- Testing should also verify that the system provides protection in response to likely improper actions.

  [DOE G 420.2-1, II.B.3.a.5)iii(d)]

Specific Test Requirements

- Interlock test procedures should be implemented to ensure that the radiological safety interlock control devices are such that
  - radiation cannot be produced until the interlock system logic has been completely satisfied
  - production of radiation cannot be resumed by merely reestablishing the interlock circuit at the location where an interlock was tripped
  - the safety circuit cannot be re-energized or reestablished automatically (i.e., there should be a manual safety circuit reset on or near the main control console).

[DOE G 441.1-1C, 7.4.0.2]

Records Management

- The verification test is your evidence that provides the high degree of assurance that the interlock system accomplishes its intended requirements
- The verification test must be managed and auditable

Break Time

- Stretch or something