INTERLOCKS FOR PERSONNEL AND ENVIRONMENTAL PROTECTION

STFC SHE Code No. 40

Issue No 1.0, October 2023

Interlocks for Personnel and Environmental Protection

Contents

Appendices

Document Revisions

	Section/Sheet	Comment	Date
1.0	Safety Code 40	Initial Issue	October 2023

Abbreviations

STFC	Science and Technology Facilities Council
PSS	Personnel Safety System
PPS	Personnel Protection System
SHE	Safety, Health and Environment
CNC	Computerised Numerical Control
E/E/PE	Electrical / Electronic / Programmable Electronic
IMP	Interlock Management Plan
FSMP	Functional Safety Management Plan
TUV	Technical Inspection Association
SIL	Safety Integrity Level
PL	Performance Level
GRRA	Grandfather Rights Risk Assessment

1 PURPOSE

1.1 This Document

This code details the STFC policy for the overall management of the lifecycle of mechanical and electrical interlocks for the protection of personnel and the environment to be applied throughout STFC. It considers current and developing best practice, of which current international standards are a core reference.

Compliance with this code is mandatory when applying interlocks as part of a risk reduction strategy.

1.2 Interlocks

An interlock system can be known by many names. Within STFC common terms used to describe such systems are interlocks, interlock systems, Personnel Safety Systems (PSS) and Personnel Protection Systems (PPS). These are used interchangeably within the organisation, however for the purpose of this code interlocks and interlock system will be used to describe implementations utilising either electrical, mechanical or a combination of both technologies.

Interlocks are widely used across STFC for protection against a range of hazards. These interlocks protect personnel, equipment and the environment as part of a risk reduction methodology. The implementation of such interlocks is achieved utilising either mechanical and/or electrical or electronic systems.

Such interlocks provide significant levels of risk reduction against injuries, ill health and environmental harm. They typically consist of sensors and logic functions that detect a dangerous condition and final elements, such as isolators or contactors that are manipulated to achieve a safe state. However, they can also consist of purely mechanical trapped key based systems that ensure hazards are removed prior to entry into the hazardous area.

The application of such purely mechanical interlocking systems is widespread within STFC. While the safe development and operation of such wholly mechanical systems can be achieved through the use of general good design practice, the policy, rules and procedures set out in this code will make this consistent across the implementation of interlocks within STFC.

1.3 Management of Interlocks

SHE Code 40 provides a framework for the management of the interlock lifecycle that will be employed by STFC to ensure STFC facilities are safe to use. This code should be read in conjunction with those STFC SHE codes for specific hazards where interlock control systems are frequently found such as laser, electricity, ionising radiation etc.

A risk assessment, as detailed in SHE Code 6 (Risk Management), must be undertaken prior to the application of this code, as it provides the essential requirements for the Interlock design.

2 SCOPE

2.1 Applicability

This code applies wherever interlocks are employed to mitigate the risk of harm to:

- People; or
- The Environment

This code applies to all staff, tenants, visitors, facility users and contractors at STFC sites.

The STFC sites house a wide variety of hazards where interlock systems may be employed as critical safety controls. These include, but are not limited to, those presented by the use of electricity, ionising radiation, lasers, oxygen depleted environments, explosive and flammable gases and dusts, cryogenic, radioactive and biological materials, electro-magnetic fields and moving mechanical equipment.

This code applies to the full interlock lifecycle on STFC facilities, equipment and experiments, where interlocks are employed., This includes, but is not limited to, the following functions, the: specification, design, fabrication, procurement, installation, testing, working on or near, commissioning, operation, modification, maintenance / repair, inspection, and decommissioning.

This code applies where STFC staff apply interlocks to equipment provided by STFC as part of international collaborations with third parties unless written agreement is obtained from the collaborator detailing their specific requirements, i.e. when equipment is supplied to other countries with different safety requirements. Care should, however, be taken to ensure that STFC is fulfilling all the necessary legislative requirements in the country of use as applicable.

Where third party equipment is integrated into STFC implemented interlocks, there will need to be collaboration between the supplier and STFC to ensure an appropriate system is designed and documented.

Equipment and STFC estate could also utilise the framework in this code to provide a structured approach to the implementation of the risk reduction strategy.

2.2 Exclusions

This code specifically excludes:

- Proprietary stand-alone equipment or machinery such as engineering equipment, for example, CNC milling machines or scientific equipment such as lasers that are employed as per manufacturer instructions and where the equipment safety functions are not integrated into the larger facility, i.e. an electric door with integrated collision detection is standalone, even if additional position monitoring switches are fitted as part of a wider interlock system or, a hydraulic system installation where additional e-stops are implemented into existing inputs as per the manufacturer's instructions.
- Building Fire Alarm Systems, see SHE Code 32: Fire Safety Management.

3 INTERLOCKS IMPLEMENTATION

3.1 Introduction

This SHE code sets out the STFC policy for addressing the interlock lifecycle, alongside the codes that address individual hazards. The framework of this code gives focus on the interlocks aspects and the utilisation of interlocks to help manage risks identified by SHE Code 6 (Risk Management).

Because of the range of hazards and local working practices across STFC, individual departments will need to develop their own procedures for implementing the overall framework set out in this code.

Triggers for invoking SHE Code 40 may arise from a variety of things ranging from the creation of a new facility through to a relatively minor modification to existing interlock systems. In all cases, all steps in the interlock lifecycle must be considered albeit some aspects may involve only a minor review of extant documentation to assure that there is no impact and/or that no changes are required.

3.2 Interlocks and the relationship to functional safety standards

The implementation of interlocks is a complex process that needs to ensure the system achieves adequate levels of risk reduction. Whether this is mechanical or electrical it still needs to follow an interlock lifecycle model to manage the process and ensure consistency between systems and across STFC in the management of safety.

The application of electrical interlocks is the subject of extensive and detailed guidance and standards, referred to as Functional Safety. The general benchmark of good practice is IEC 61508, Functional safety of electrical/electronic/programmable electronic safety related systems.

Functional Safety is the accepted term applied to the part of the overall safety of a system that depends on the correct functioning of electrical, electronic and programmable electronic (E/E/PE) safety related systems and other risk reduction measures[1]. This would include any mechanical interlocks that contribute to the overall safety of such a system.

IEC 61508 has been used as the basis for industry specific standards for functional safety such as:

- IEC 61511: Functional safety – Safety instrumented systems for the process industry sector
- IEC 62061: Safety of machinery – Functional safety of safety-related control systems

Other standards exist that are also commonly used and accepted as best practice in industry such as:

- ISO 13849: Safety of machinery – Safety-related parts of control systems

As an extension to the implementation of functional safety, the use of the lifecycle model for the implementation of mechanical interlocks provides additional controls and consistency across the organisation.

3.3 Risk Assessment

This code does not detail the requirements associated with risk assessment and the determination of control measures required to reduce risks to an acceptable level.

[1] IEC 61508 Part 4 section 3.1.12

SHE Code 40 assumes and requires that a Risk Assessment as per SHE Code 6 (Risk Management) has been carried out for the STFC facility/system under consideration and that the following inputs are therefore available for that facility/system:

- The Concept
- The Overall Scope Definition
- A Hazard & Risk Analysis
- Overall Safety Requirements, to reduce risk to a level acceptable by STFC

A risk assessment identifies the controls in place to mitigate the risks identified, however it does not define the level of risk reduction that an interlock system is required to achieve as part of a risk reduction strategy. A critical step in the specification of an interlock system is this identification of the level of risk reduction that the interlock system must achieve.

A determination of the required risk reduction shall be carried out to identify the requirement for, and level of risk reduction required by, the interlock system.

There are a number of methods available to perform this. The chosen method will depend on the specifics of the system being assessed. Examples of methods are:

- Risk Graph (commonly used in ISO 13849)
- Matrix Assignment (commonly used in IEC 62061)
- Layer of Protection Analysis (commonly used in IEC 61511)

3.4 Interlocks Implementation

The implementation of interlocks requires consideration and planning of many aspects, covering a range of areas that are applicable throughout the lifecycle.

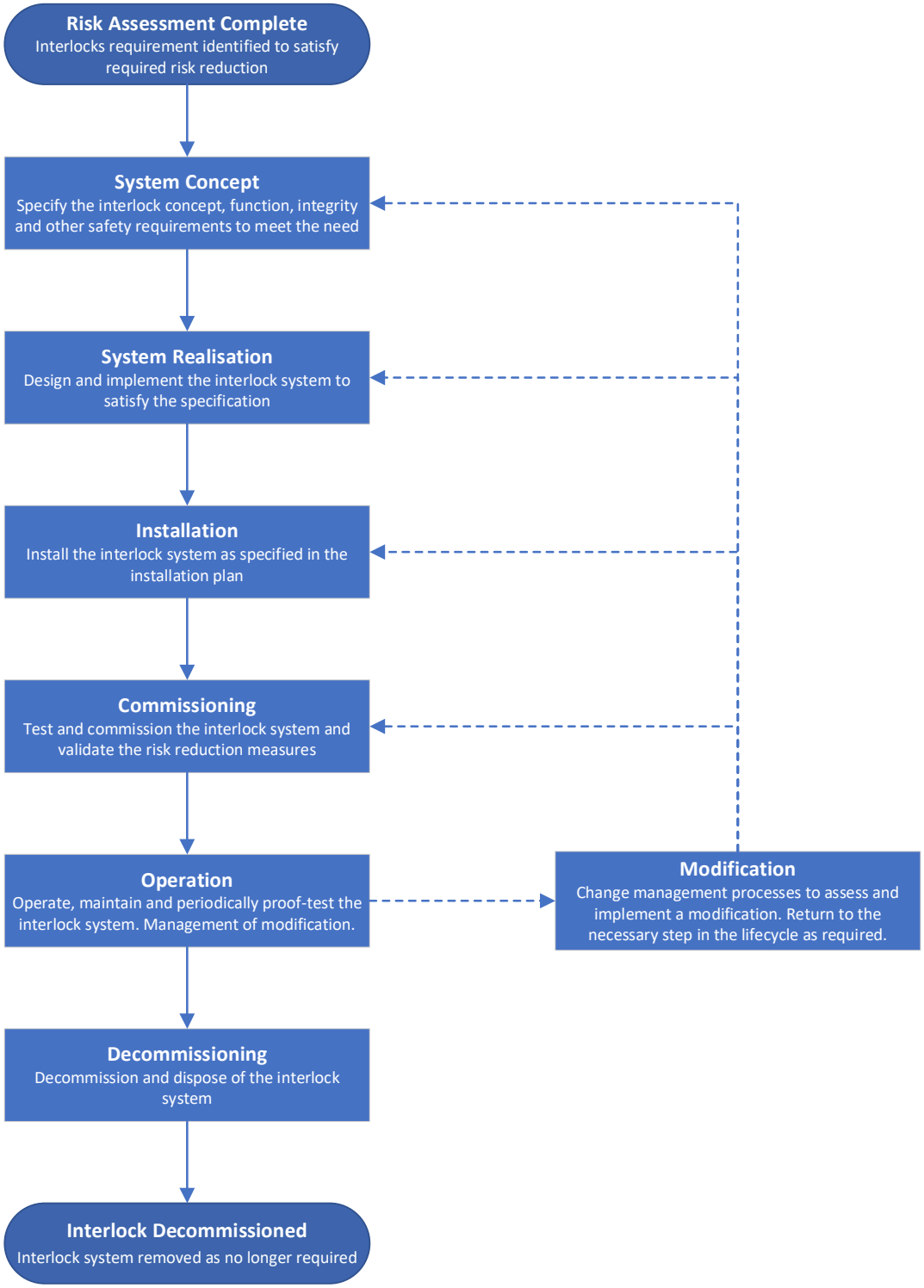
There are two ways to address the requirements for implementation of interlocks within STFC and therefore compliance with this code, either:

1. a suitable recognised international standard that covers the lifecycle phases associated with, as a minimum, safety requirements allocation through to decommissioning:
    a. IEC 61508 (or sub-standards, i.e. IEC 62061, IEC 61511, etc.)
    b. ISO 13849 (With the addition of an Interlock Management Plan (IMP), see section 3.5)
2. A process that affords equivalent to or better protection than that detailed within the recognised international standards applicable to interlocks lifecycle implementation.

The implementation of the interlock design lifecycle is addressed in the relevant international standards which are considered industry best practice. The departmental implementations of SC40 should be maintained in line with updates to the applicable international standards as new versions are released for use.

Any alternative approach is to be clearly defined and justified as to how it meets the requirement to point 2 above and will require the director of the department who owns and operates the equipment to sign off this implementation.

The key steps in the interlock lifecycle are:



Within the overall implementation there are some key areas that need to be addressed as detailed in sections 3.5 to 3.10 below.

3.5 Interlock Management Plan

Key to the implementation of a consistent approach to interlocks is the generation of an interlock management plan (IMP), more commonly referred to as a Functional Safety Management Plan (FSMP). An IMP shall be produced to cover any work carried out on interlocks covered by this code through its lifecycle.

The purpose of an IMP is to ensure a clear and shared understanding of the approach to be used to achieve the required safety risk reduction using an interlock system. It does not need to exist as a separate document; for example it could be included in wider safety management plans or engineering management plans. The IMP should be produced by drawing on standard organisational/department practices/procedures where available, e.g. Safety Management System.

The IMP should be updated at a frequency agreed by key stakeholders, but it would be unusual if the IMP were not reviewed at least on major project events, e.g. Major life-cycle phase reviews.

Some key elements that must be included are:

- The activities to be carried out as part of the lifecycle and the persons responsible for carrying out and reviewing these
- The overall policy, strategy, procedures and resources that will ensure the functional safety requirements can be fulfilled and relevant information recorded and maintained
- The strategy for configuration management and management of change
- The verification and validation plan throughout the lifecycle

Refer to the IEC 61508 suite of standards for a clear definition of the full content requirements of the IMP.

3.6 Change Management

Given the lifespan of facilities within the STFC, changes to the systems providing risk reduction are inevitable and need to be managed effectively and efficiently to provide a level of risk that remains acceptable.

The management of change to interlocks should follow STFC standards where available. There is nothing unique to interlocks in this respect. However, where STFC Standards do not exist, Departments should develop and follow their own procedures for implementing Change Management.

3.7 Legacy Interlocks

It has been accepted that, with the adoption of SHE Code 40, all new interlock installations from concept to disposal will comply with the new code.

It is key however that all systems to which this code would apply are known and managed appropriately. Departments shall hold a record of all such systems that are within their control.

Existing (‘legacy’) installations will benefit from so called grandfather rights. A grandfather clause (or grandfather policy or grandfathering) is a provision in which an old rule continues to apply to some existing situations while a new rule will apply to all future cases.

This would normally continue to apply until:

1. A risk assessment under SHE Code 6 (Risk Management) identifies a risk that needs to be further reduced to become acceptable, or to conform to good practice, and the chosen method of risk control includes E/E/PE equipment; or

2. Existing/legacy installations where survey/assessment shows significant dependence on E/E/PE for personnel protection – to be applied on a priority call and in timescale dictated by STFC and Departmental review.

Frequently, the exemption is limited; it may extend for a set time, or it may be lost under certain circumstances.

Legacy systems are to be defined as systems that have a completed design finalised for installation, and are within the installation, commissioning, operational or decommissioning phases of their project lifecycle by 31st January 2026. Systems still within the design phase after this time will not be considered legacy and shall comply with this code.

By 31st January 2026 these legacy systems shall be identified, and a suitable and sufficient assessment will have been carried out for each system to justify its continued use. Additional guidance on the expectations of the grandfather rights risk assessment (GRRA) can be found in Appendix B.

There is no prescribed time that will apply to grandfather rights for legacy interlocks. It will be up to department directors to decide if any grandfather rights shall be time limited.

Circumstances that may result in the loss of grandfather rights would include, for example, modification of the interlocks to change its functionality. This may be influenced by the degree of changes being made. It will be up to departments to determine the criteria that will result in the loss of grandfather rights. Additional guidance providing some of the expected criteria that would trigger an upgrade can be found in Appendix B.

Existing (legacy) interlocks may not be fully documented as required by SHE Code 40. In these cases, where the need for review or change has been triggered, it would be necessary to identify, log and review the available information. This could include not only formal written records but also the informal knowledge of those involved in the development and operation of the interlock system. This understanding should be explicitly documented and subjected to appropriate review as part of a formal Change Management process.

3.8 Mechanical Interlocks

General Approach

The implementation of mechanical interlocking systems either standalone or as part of a functional safety system, referring primarily to trapped key based systems, e.g. Castell or Fortress keys, shall follow the implementation approach detailed within this code. Although the application of a trapped key interlocking philosophy is not covered by the functional safety standards unless it forms a layer of protection in a wider E/E/PE based implementation, this best practice is considered appropriate.

As part of this approach the applicable documentation, reviews and change management should be implemented.

Key Register

A register of all trapped key reference numbers for STFC sites is held by the SHE Group, accessed via the SHE website. This is to ensure that duplicate key references are not utilised by a single STFC department.

All new proposed key references/numbers should be registered with SHE Group **PRIOR** to being ordered to ensure that they are unique to that department and recorded.

Failure to ensure that all keys on a site are unique could result in a safety system being compromised by the use of a duplicate key.

The key register is located at https://stfc365.sharepoint.com/sites/SHEGroupHub/STFC-Key-Database.

Additional Information

There is additional information on the design and application of trapped key interlocking devices in ISO/TS 19837:2018

4 RESPONSIBILITES

4.1 Introduction

The competencies and level of experience required to undertake these roles within the interlock's lifecycle will vary and will depend on the nature of the hazards, operational environment and complexity of the risk control measures required. It is the responsibility of the department to tailor the competency required of these roles to be appropriate to the situation at hand.

Persons carrying out roles within the Interlocks lifecycle are expected to be competent and appropriately trained for the role. Refer to Appendix A for training requirements.

The management process employed within this code is a Matrix management approach, where the persons who manage competence are not necessarily the same as those that manage systems or permit work on such systems. This approach is proposed to maintain a simple and scalable implementation.

Note that these roles may not map directly to existing STFC jobs.

4.2 Directors whose operations include equipment/facilities employing interlock systems shall:

Approve in writing any deviations from the application of international standards (as per point 2 in Section 3.4) for their department and ensure that this decision is reviewed on a periodic basis.

Approve in writing the continued operation of any legacy systems as part of a grandfather rights methodology for the department (see Appendix B for additional guidance).

Ensure that the specification, design, fabrication, procurement, installation, testing, commissioning, operation, modification, maintenance / repair, inspection and decommissioning of interlock systems meet requirements of this code throughout the interlock system lifecycle, see section 3.

Ensure a sufficient number of competent people are identified and that sufficient resource and facilities are available to them to implement the requirement of this code throughout the interlock system lifecycle, see section 3. See Appendix A for training and competence requirements. Where necessary, collaborate with or share such specialist personnel with other Departments.

Ensure the exact extent of the interlock systems and installations for which a person working on interlock systems is responsible is identified and documented, maintaining clear demarcation between areas.

Ensure that all reported SHE incidents involving interlocks within their area of responsibility are investigated. Where learning points can be derived, identify suitable persons to work with SHE Group to ensure that the learning is cascaded to persons working on interlock systems and to the wider STFC interlocks community.

4.3 Managers of equipment/facilities employing interlock systems, including Contract Supervising Officers shall:

Be accountable for the safe operation of their equipment and ensuring that only competent persons are permitted to work on the interlock systems that they manage.

Ensure appropriate implementation, administration and monitoring of the application of this SHE code is carried out for the systems for which they are responsible.

Prior to allowing work on their equipment/facilities that contain interlocks as a control measure ensure that a risk assessment and method statement for the work planned has been established, see SHE Code 6 (Risk Management) based on the advice of competent individuals, see Appendix A for training and competence requirements, on all aspects of the interlock system lifecycle.

Where such work is undertaken by STFC staff, or contractors working on their behalf, the competence of all individuals working on or near interlock systems must be approved before undertaking work or tests, see Appendix A for training and competence requirements. Maintain appropriate records to show that personnel carrying out work on interlock system are competent and appropriately trained.

Ensure all Persons working with/on Interlock systems are made aware of any relevant safety information, defect report or operational restriction on the functional systems or equipment on which they are working as soon as is reasonably practicable, providing appropriate advice to prevent injury.

Consult with the competent individuals prior to purchasing or embarking on a new project in which interlock may be required as a risk reduction measure.

Instigate the change management process when required and ensure that appropriate persons are carrying out the required modifications to systems under their control.

When dismantling/decommissioning/disposing of equipment that has interlocks they must consult competent individuals.

Ensure that when facility users/visitors bring their own, non-proprietary, equipment into the STFC sites/facilities containing interlocks they must consult competent individuals for assurance that such equipment meets the requirements of this SHE Code.

Ensure that all incidents, near misses, hazardous conditions, dangerous occurrences or failures of safe systems of work for staff and others working on or using interlocks, including contractors, are reported through Evotix Assure following SHE Code 5 (Incident Reporting and Investigation).

4.4 Staff, tenants, contractors, facility users or visitors shall:

Report all interlock incidents or near misses to the Equipment Manager as soon as is practicable, and in Evotix Assure following SHE Code 5 (Incident Reporting and Investigation).

Only use interlock systems on which they have been suitably trained and deemed competent.

Use interlock systems as demonstrated and instructed, and as per any supplied manuals. Where there is ambiguity or uncertainly then a competent person should be sort to clarity these items before continuing operation of the interlock system.

4.5 SHE Group shall:

Ensure STFC subscribes to suitable industry fora where serious interlock incidents, equipment faults/failures and manufacturers advisory notices are published sharing relevant information across STFC in a timely manner.

Ensure that learning from interlock SHE incidents and good practices are shared across STFC.

Manage the trapped key interlock database.

4.6 Line managers/managers of persons working on interlock systems shall:

Identify and maintain, in writing and record, the completed training and competence for the relevant lifecycle phases (see Appendix A), of persons under their management working on interlock systems.

Review the training and competence of persons working on interlock systems at least every 5 years or more frequently depending on performance and if necessary suspend their involvement in interlock activities documenting the reasons why. The equipment manager is to be advised of such action and the corrective action recommended, in collaboration with a competent person, ensuring the continued safe operation of the safety related systems and installations.

Ensure that all incidents, near misses, hazardous conditions, dangerous occurrences or failures of safe systems of work are promptly reported by the relevant example Persons working on interlock systems and others undertaking interlock related work, including contractors through Evotix Assure following SHE Code 5 (Incident Reporting and Investigation).

4.7 Personnel involved in the interlock lifecycle

The Interlock lifecycle can be significant durations (>30 years), span an extremely large scope, and roles and responsibilities within it will vary between and within both departments and projects.

These roles and responsibilities, and named individuals assigned to these, shall be documented by departments as part of the IMP for the facility, project or equipment as applicable.

Roles and responsibilities within the interlock lifecycle shall include the following:

- System Manager/Owner - responsibilities such as co-ordinating effort to establish the overarching needs of the system and ensuring formal documentation is generated as required, including the generation and maintaining of the IMP. Responsible for the instigation of the change management procedure during the operational phase of the interlock system. The responsibilities of this person/role will potentially change during the lifecycle of the project depending on the lifecycle phase requirements.
- Design – covers all levels of design from concept through to detailed design. Responsible for producing system requirements & specifications, functional design of the system including (if applicable) software, wiring, etc. and all relevant documentation as dictated by the IMP.
- Testing and Commissioning - responsible for commissioning and testing of the functional safety as well as physical testing of the overall installation against the initial aims and requirements of the system.
- Operation – the user of the system who is responsible for using it in a safe and appropriate manner. Such users may have responsibility for training and supervising others in the use of the system.
- Maintenance and Repair - responsible for the ongoing maintenance and repair of systems, ensuring no work is undertaken without authorisation of the manager/system owner.

Where roles within the lifecycle are undertaken by committees, memberships of such shall be clearly defined in the IMP.

Regardless of their role personnel involved in the interlock lifecycle shall:

Be responsible for the practical implementation and operation of this SHE Code for the tasks and activities for which they are responsible.

Ensure that the interlock systems under their responsibility have all required accurate documentation available, including drawings / schematics, so that the interlock system can be operated, modified, maintained and decommissioned safely. All changes to the interlock system shall be recorded.

Ensure that all incidents, near misses, hazardous conditions, dangerous occurrences or failures of safe systems of work are promptly reported by the relevant example Persons working on interlock systems and others undertaking work in the interlock lifecycle, including contractors through Evotix Assure following SHE Code 5 (Incident Reporting and Investigation).

Instruct persons required to operate interlock system equipment under their control in the safe use of that equipment and advise on the hazards arising from improper operation.

5 GLOSSARY OF TERMS

E/E/PE - Electrical/Electronic/Programmable Electronic – e.g. E/E/PE Safety-related system.

EUC - Equipment Under Control.

Functional Safety - Functional safety is the part of the overall safety of plant and/or equipment that depends on the correct functioning of safety related systems and other risk reduction measures including alarms, trips and interlocks.

Interlocks/Interlock System – the term used throughout SHE Code 40 to describe E/E/PE Safety-related systems in STFC.

Harm - Physical injury or damage to the health of people or damage to equipment, property or the environment.

Hazard - Potential source of harm.

Hazardous Situation - Circumstance in which people, property or the environment are exposed to one or more hazards.

Safety Integrity - A measure of the rate of unsafe failures; the likelihood of a safety-related system satisfactorily performing the required safety functions under all the stated conditions, within a stated period of time.

Risk - combination of the probability of occurrence of harm and the severity of that harm.

Residual risk - risk remaining after protective measures have been taken.

Safety - freedom from unacceptable risk.

SIL - Safety Integrity Level - A target probability of dangerous failure of a defined safety function; a discrete level (one of 4) for specifying the safety integrity requirements of safety functions.

Tolerable risk - risk which is accepted in a given context based on the current values of society or, in the context of STFC, within the Corporate Risk Appetite.

6 REFERENCES

[1] IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1 General requirements

[2] IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems

[3] IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements

[4] IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations

[5] IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels

[6] IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

[7] IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures

[8] IEC 62061:2021, Safety of machinery – Functional safety of safety-related control systems

[9] ISO 13849-1:2015, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

[10] ISO 13849-2:2012, Safety of machinery – Safety-related parts of control systems – Part 2: Validation

[11] IEC 61511-1:2016+AMD1:2017, Functional Safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements

[12] ISO/TS 19837:2018, Safety of machinery – Trapped key interlocking devices – principles for design and selection

[13] Health & Safety Executive – Functional Safety https://www.hse.gov.uk/eci/functional.htm

[14] Managing Competence for Safety-Related Systems, IET/BCS/HSE, 2007; (Part 1: Key guidance; Part 2 Supplementary material). HSE. 2007

[15] Competence criteria for safety-related system practitioners. IET. 2006

[16] Code of Practice, Competence for Safety-Related Systems Practitioners. IET. 2017

[17] TUV Training Provider List – Functional Safety https://www.tuv.com/landingpage/en/training-functional-safety-cyber-security/meta-navigation/all-providers/

Appendix A TRAINING AND COMPETANCE REQUIREMENTS

Role	Training	Training Frequency
System Manager / Owner	Training should address the following topics, or equivalent for the standard being utilised, and ideally be accredited by an appropriate certification body, i.e. TUV: • Management of functional safety • Safety Lifecycle Concepts • Compliance framework for IEC 61508 • Functional safety and the role of IEC 61508 and other related standards in achieving functional safety • The concept of risk reduction, risk reduction parameters and the concept of a tolerable risk • The concept of a safety function with respect to its functionality and its performance • The role of safety-related, other engineering measures and risk parameters in achieving a tolerable risk • Concept of Safety Integrity and Safety Integrity Level (SIL) / Performance level (PL) • SIL Determination concepts and methods	At least every 5 years
	Bitesize training for this code	At least every 5 years
	Departments must provide training based on the IMP of the specific systems being worked on.	At least every 5 years
	Competence	**Review Frequency**
	They should be able to demonstrate for the systems, installations and equipment on which they are system manager/owner: • a clear understanding of the boundary and purpose of the equipment • a clear understanding of the overall implementation of risk reduction for the hazards	Prior to commencing relevant lifecycle activity, and at least every 5 years

Role	Training	Training Frequency
Design	Training should address the following topics, or equivalent for the standard being utilised, and ideally be accredited by an appropriate certification body, i.e. TUV: • Functional safety and functional safety management • The concept of risk reduction, safety integrity levels (SIL), Performance Levels (PL) and SIL/PL determination • Safety function definition and appropriate implementation • The role of a Safety Related System, other engineered measures and risk parameters in achieving a tolerable risk	At least every 5 years

	• Design essentials for functional safety	
	Bitesize training for this code	At least every 5 years
	Departments must provide training based on the IMP of the specific systems being worked on.	At least every 5 years
	Competence	**Review Frequency**
	They should be able to demonstrate for the systems, installations and equipment on which they are designing: • a good working knowledge of appropriate control functions for the hazards • a good understanding of all the necessary safety measures to be taken to prevent injury or ill health (or to prevent damage to Equipment)	Prior to commencing relevant lifecycle activity, and at least every 5 years

Role	**Training**	**Training Frequency**
Testing and Commissioning, and Maintenance and Repair	Training should address the following topics, or equivalent for the standard being utilised, and ideally be accredited by an appropriate certification body, i.e. TUV: • Management of functional safety • Safety Lifecycle Concepts • The role of a safety-related, other engineered measures and risk parameters in achieving a tolerable risk • Documentation requirements and fault logging	At least every 5 years
	Bitesize training for this code	At least every 5 years
	Departments must provide training based on the IMP of the specific systems being worked on	At least every 5 years
	Competence	**Review Frequency**
	They should be able to demonstrate for the systems, installations and equipment on which they are working: • a good working knowledge of the layout and operation of the system • a good understanding of all the necessary safety measures to be taken to prevent injury or ill health (or to prevent damage to Equipment)	Prior to commencing relevant lifecycle activity, and at least every 5 years

Role	Training	Training Frequency
Operation	They should be trained for the systems that they are authorised to operate to ensure that they have: • a good working knowledge of the layout and operation of the functional safety system • a clear understanding of actions to take in the event of any alarms or other warning devices being active • knowledge of those responsible for operation and maintenance, including out of hours contacts, in the event of a fault with the system • a clear understanding on how to report system faults or hazardous events during operation This training will be provided by departments and will usually be bespoke for each specific system the individual is authorised to operate.	As frequently as necessary, but at least every 5 years or following a major change or a significant period of non-operation
	Competence	**Review Frequency**
	They should be able to demonstrate for the systems, installations and equipment which they operate: • a good working knowledge of the layout and operation of the system • a good understanding of all the necessary safety measures to be taken to prevent injury or ill health (or to prevent damage to Equipment)	As frequently as necessary, but at least every 5 years or following a major change or a significant period of non-operation

Appendix B GRANDFATHER RIGHTS RISK ASSESSMENT AND LEGACY SYSTEMS

This Appendix provides additional information and guidance on the assessment of existing interlock system (referred to as grandfather rights risk assessment) as well as key considerations for legacy systems that are currently in operation.

B.1 GRRA Purpose

The grandfather rights risk assessment (GRRA) needs to be carried out on existing legacy interlock systems that would be covered by SC40. It is the process that will determine whether a legacy, pre-existing, safety interlock system can continue to operate of under it's 'grandfather rights' or that it needs to be reviewed and updated to current standards of interlock design and implementation for future facility safe operation. It relies on identifying the hazards and associated controls that are implemented and assessing the reliance on interlocks systems as part of the safety risk reduction strategy. The purpose of the GRRA is to highlight where existing controls rely solely, or very heavily, on interlock systems and therefore where there is a need to provide additional layers of protection or upgrade the existing controls.

B.2 GRRA Process

The process of carrying out the GRRA needs to, as far as possible, ensure that all existing systems that would be covered by SC40 are included. The following would be key steps in this process:

1. **Identification of legacy interlock systems** – systems across the department/Site identified and their name, location, purpose and system owner identified.
2. **Carry out GRRA for each system** – keep a documented record of the GRRA for future review.
3. **Director Sign off** – director reviews the legacy systems that are still in operation and approves their continued use to assure their safe operation based on the GRRA outcomes.
4. **Periodic Review** – the continued use and assessments of legacy systems are reviewed on a periodic basis to ensure that the system is still safe for use.

B.3 GRRA Considerations

As part of the GRRA the following elements should be identified and considered when assessing the suitability of legacy systems for operation:

- **Hazards** – Identify all of the potential hazards that are present on the equipment and whether the system addresses these.
- **Level of risk** – What is the level of risk present from the equipment, how is the equipment going to be used in all of its lifecycle phases (operations, maintenance, etc.) and what tasks are going to be performed?
- **Controls** – What controls, or layers of protection, are in place to protect against the hazardous scenarios? Do the existing controls provide a suitable breadth of protection against these?
- **Amount of reliance on interlocks** – Are there limited other controls and the primary protection is the legacy interlock system? Depending on the level of risk, is this a suitable application for a legacy interlock system?
- **Level of regular testing** – Is it tested, if so how frequently should it be tested to maintain GRRA approval?

B.4 People Involved

The GRRA process should involve a range of competent personnel involved in the full lifecycle of the equipment. This should include:

- System Owner (Leads the GRRA)
- Operators
- Maintenance teams
- Design team.

B.5 Upgrading Legacy Systems

Although the use of legacy system is not time limited and their continued use can be justified through the use of the GRRA, there are some conditions that should be considered as triggers for upgrading legacy systems (not renewing legacy systems).

Examples of such triggers would be:

- **Major upgrade** – A significant change to a legacy system should trigger serious consideration of a full replacement.
- **Defined lifetime** – When the system was installed did it have a defined operational lifetime? If so, what are the implications of exceeding this on the reliability of the system, both as a whole and for individual components?
- **Performance** – Have there been any performance issues with the system or repeatable hazardous conditions that have identified?
- **Spares availability** – Consideration given to whether the system can be maintained going forwards or if an upgrade is required to ensure continued safe operation.
- **Documentation** – What is available? If there is limited documentation available and/or also limited expertise in the system's operation then consideration should be given to whether safe operation is possible and whether it could be maintained.
- **High reliance on operation** – Where a legacy interlock system is providing all, or a significant proportion, of the protection against the identified hazards consideration should be given to whether this is appropriate.

B.6 Director guidance

Where a director requires expert guidance, in the first instance they should approach SHE Group who can direct them to sources of in-house and external interlock expertise.

Appendix C **AUDITING**

This Appendix addresses the audit of interlock systems as defined in this SHE code - Operational Audit of interlock systems undertaken by department directors, or those with delegated responsibility.

Independent Compliance Audit of this SHE code as defined in STFC SHE Code 30 (SHE auditing and Inspection) will also need to be carried out as defined in SHE Code 30.

C.1 Operational Audit of Interlock Systems

The auditor shall prepare a programme, undertake and document the findings of an audit programme of interlock systems and procedures defined in this SHE code. The frequency of such audits should not exceed 3 years. Audit findings and recommendations shall be sent to the relevant Director for consideration.

Listed below are systems and procedures to be included, as a minimum, in this audit programme.

Desk Audit:

- Interlock Management Plan(s)
- Review of a selected interlock system:
  - Interlock System Design Documentation
  - Interlock Test & Results Documentation
  - Procedures and operating instructions for Interlock Systems
  - Training records of those carrying out roles in the interlock system lifecycle
  - Ongoing periodic testing and maintenance records
- Interlock SHE Incidents
- Change management process and records.

Site Audit:

- Tour of selected interlock system:
  - Appropriate signage is present
  - Location and identification of Interlocks, warning lights and audible alarms
  - Visible condition of interlock system hardware.

C.2 Compliance Audit Checklist

Ref	Item	Rating	Comments
	Has accurate documentation for their functional safety systems (design documentation, drawings, schematics etc.) been established in controlled document management systems?		
	Are interlock installations suitably supported by relevant signage and identification?		
	Are there any instances of the over-riding of interlock systems? What written supporting documentation and record of authorisation is available?		
	Have any mechanical key interlocks (standalone or integrated) been modified or implemented? Are all keys recorded in the key database?		
	Have any systems been decommissioned? Have these been suitably documented and disposed of?		
	Has any visitor/user provided equipment with interlocks been approved for use in the department? Has its compliance with this code been suitably documented?		
	Is a suitable and sufficient change management process in place?		
	Where changes or modifications to an interlock system have been undertaken are there documented records of subsequent testing and commissioning and signoff of the system before it is returned to operation?		
	Is the change management process followed and all documentation in place to enable effective management of change?		
	Interlock incidents within the area of responsibility have been investigated.		
	Are there any examples of instances where functional defects have been reported? Have these been followed up and investigated?		
	Is there evidence of a mechanism for communicating relevant commercial interlock equipment information, for example defects, recalls etc.		
	Are interlock incidents reported to department directors by SHE Group?		

Appendix D **DOCUMENT RETENTION POLICY**

Records established	Minimum retention period	Responsible record keeper	location of records	Example Documents may include:
All components of the Interlock Management Plan	Lifetime of interlock system	Departments	Local records system	Interlock Management Plan Verification and Validation Plan
All interlock system documentation	Lifetime of interlock system	Departments	Local records system	Risk Assessment and risk reduction determination. Safety Requirements. Design Documentation (drawings, specifications, technical file). Verification Calculations. Test and Commissioning Records. Periodic Test Records.