RioTinto

HSE-B-31

Group Standard

D7 – Functional Safety

<table>
<tr><td rowspan="4">Group standard</td><td colspan="4">Title: Functional Safety</td></tr>
<tr><td colspan="4">Function: Health, Safety, Environment and Security</td></tr>
<tr><td colspan="4">No. of Pages: 9</td></tr>
<tr><td>Approved :
July 2019</td><td>Effective:
1st Sept 2019</td><td>Supersedes:
N/A</td><td>Auditable From:
1st Sept 2020</td></tr>
<tr><td colspan="2">Owner:
Global head of HSES</td><td colspan="2">Approver:
Executive Committee</td><td>Target Audience:
All Rio Tinto employees and contractors and each Rio Tinto Group business and function, performing work related to safety related systems</td></tr>
<tr><td colspan="5">Direct Linkages to other relevant Policies, Standards, Procedures or Guidance notes:

Rio Tinto Management System standard
Group Asset Management standard
Group Risk Standard
Group Procedure for Information and Cybersecurity
Group Procurement Standard</td></tr>
<tr><td colspan="5">Document purpose:

• To support implementation of the Group HSEC policy.
• It defines the minimum requirements to support implementation of the Rio Tinto management system standard in terms of delivering technical systems with robust functional safety</td></tr>
</table>

D7 – Functional Safety

Intent and scope

This standard is applicable to all Rio Tinto business units and managed operations (including supply chain) and projects.

The intent of this standard is to set minimum requirements for effective functional safety management within Rio Tinto and to ensure that where we have engineering safety controls, we address technical and functional safety, as well as personal safety.

Functional safety is the framework used to deliver and maintain the effectiveness of critical safety functions in our technical systems. Applying functional safety principles within this standard enables Rio Tinto to have confidence that technical systems deliver effective protection measures and control the risk.

Functional safety is a concept applicable across all industry sectors. It is fundamental to the enabling of complex technical systems used for safety related systems. It provides the assurance that the safety-related systems will offer the necessary risk reduction required to achieve safety of the equipment.

All technical systems with potential events that lead to fatalities or significant injury must apply the requirements of this standard to enable the business to deliver and operate systems that meet a tolerable level of risk.

This standard is to be applied for managing significant health and environmental risks as well as safety where technical controls are used.

Control requirements

Specific management requirements in this standard apply in addition to any requirements defined in the Rio Tinto Management System.

Managing Functional Safety

1.1 Sites or projects must select a recognised and current good practice standard(s) in the relevant sector with which to apply functional safety (see examples in Appendix A). The rationale as to why the standard chosen is appropriate must be documented. This must include a review of any applicable legislation and regulators' published documents related to functional safety.

1.2 For delivery of a project a functional safety management plan must be developed during the feasibility stage or earlier. The plan shall be commensurate with the nature and extent of the functional safety risks. It must meet relevant legislative requirements and the requirements of the functional safety standard.

1.3 Where a project is delivering a system with a significant safety performance requirement, (for example that meets a Safety Integrity Level (SIL), Category or Performance Level (PL) threshold) the project must ensure the supplier(s) and system integrator(s) also develop a functional safety management plan.

1.4 Sites that are operating safety related systems or technology, must have a functional safety management plan that is used to ensure ongoing effective performance of these systems during operation and maintenance.

1.5 The functional safety management plan must be approved by the Project Manager for projects and site senior leadership for operational sites.

1.6 An audit process must be developed and implemented for the functional safety management plan.

1.7 When safety related systems or technology are implemented or changed, appropriate levels of independence from the delivery team must be defined for governance, audit and assessment roles in line with recognised standards adopted.

Governance

1.8 A functional safety governance process must be in place before work is commenced on design of the solution.

1.9 Governance must be maintained for the operations and maintenance phase of the lifecycle to ensure the safety performance is achieved and is sustained; and that any technical changes or changes to supporting processes related to safety systems consider the safety requirements and any new hazards identified.

Resources

1.10 Sites and projects must have a process in place for identifying key roles and responsibilities related to functional safety and document them within the functional safety management plan.

1.11 Competencies must be demonstrated, verified and recorded for each relevant phase of the functional safety lifecycle. Where a system is considered to be safety critical (i.e. has a Safety Integrity Level of 1 or greater or equivalent Category or PL) then these competencies must be documented as part of the assurance process.

1.12 Resources must be identified for the governance process for endorsing delivery of the safety related systems. The level of governance must be commensurate with the risk (or consequence severity), novelty and complexity.

Understanding Functional Safety risk

2.1 During a pre-feasibility stage of a project and prior to developing the functional safety management plan the context and scope must be developed and documented that outlines the:

- Operating environment
- Relevant legislation, regulator guidance, national and local standards
- Concept of operations and/ or business objective

2.2 Hazard identification and risk analysis techniques must be identified during the planning phase that enable the risks to be robustly and systematically analysed. A Rio Tinto Level 2 risk assessment will not be adequate on its own and a quantified analysis (Level 3) must also be completed. Where quantification is not feasible due to the nature of the system a documented rationale must be recorded.

2.3 A register of hazards, causes and controls must be maintained throughout the life of the system to inform future modifications and decommissioning. This must be periodically reviewed and updated based on hazard analysis and risk assessments during the project analysis and realisation phase and the operational and maintenance data captured during the operations and maintenance phase.

2.4 The risk controls and management must be demonstrated to reduce the risk to As Low As Reasonably Practicable (ALARP).

2.5 Safety requirements must be derived and documented from the hazard and risk analysis and provided as an input to the development of overall system requirements for delivery. Safety requirements must include detail of the function to be achieved and the performance requirement of the function.

2.6 A safety requirement specification for the safety related system must be maintained through the life of the system.

Procurement

3.1 Where a project has a contract in place for the delivery of safety related systems the contract must state the functional safety standard(s) to be applied.

3.2 All components that form part of the safety system solution must be managed so that they cannot be ordered, or changed for different modifications, without an assessment of the impact on the functional safety system being completed and documented as part of an approved management of change.

Design and Implementation

4.1 Delivery of a new design that includes safety functions must apply the framework within recognised standards (such as IEC 61508 or those examples referred to in Appendix A, or their current equivalent).

4.2 The decision of the standard(s) to apply must be endorsed by Rio Tinto representatives from both the project delivery business unit and the operator and maintainer business unit that will receive the system at handover.

4.3 Development of any system that includes safety functions that have a safety performance requirement must be delivered using a quality assurance system that meets the requirement of ISO 9001 or equivalent.

4.4 Independent functional safety assessments must be undertaken in line with the safety performance requirements and the chosen standard before the system is commissioned.

4.5 An independent assessment must be undertaken of the supplier's functional safety processes that gives assurance that the work is undertaken appropriately. This should be undertaken at appropriate lifecycle phases that enable any issues to be resolved, in order to minimise the impact to the delivery of functional safety.

4.6 For a safety related system that is developed for a specific project or site application, the system must be audited for compliance with the standard before acceptance of the system on behalf of Rio Tinto. This must include a focus on quality assurance of hardware and software and application of functional safety processes identified within the appropriate functional safety management plan.

4.7 Verification results must be recorded for each phase of the safety lifecycle for safety related systems.

4.8 The safety related system must have been verified to have been installed to the approved designs and specifications.

4.9 There must be a plan to complete validation which identifies who shall undertake this, any independence requirements and the method of validation.

Acceptance

5.1 There must be a defined process that states how the safety related system will be accepted into service and what inputs are expected to be provided before acceptance can be achieved.

5.2 Sites and projects must define acceptance criteria that require documented acceptance at a minimum by the asset owner, asset maintainer and asset operator.

5.3 A validation report must be documented and issued as an input to formal acceptance of a safety related system into service.

5.4 The validation must ensure that the installed and commissioned safety system achieves the functions and performance stated in the safety requirements.

5.5 Acceptance must consider whether the system has delivered the proposed risk reductions effectively, that they are considered to have reduced the level of risk to a tolerable level and support the need to demonstrate the risk has been reduced As Low As reasonably Practicable (ALARP).

Operating

6.1 Documented operating processes that support the performance of a safety related system must be in place before a system is expected to be operated, and the operators must be trained in these processes.

6.2 Constraints or assumptions made during development of a system supporting functional safety that relate to operations and maintenance must have been integrated into relevant site processes and the linkages recorded to support future change management.

6.3 Where the introduction of a safety related system may impact on emergency response from an incident (such as access to an automated system) assurance must be maintained as to how this has been communicated and adopted by the emergency response organisation.

6.4 Controls identified and captured as part of the hazard identification and risk assessment phase that are relevant to emergency response must be shown to have been captured in emergency response processes and training, including the use of emergency stops, isolations and communication processes to control system operators.

Maintenance

7.1 Documented maintenance processes that support the performance of a safety related system must be in place before a system is expected to be operated.

7.2 Documented processes for performing proof tests and inspections must be in place prior to a safety related system being accepted.

7.3 The maintenance team must have systems that ensure proof testing is performed in line with required intervals determined during system design and provide reports on any proof testing not undertaken within these intervals.

7.4 A process must be in place to manage and approve the operation of systems with failed components or systems which have not achieved a proof test interval to ensure the system remains safe.

7.5 Configuration management must be in place for the maintenance of a safety related system and the responsibilities clearly defined to manage this effectively.

7.6 Where configuration management is undertaken by a supplier or contractor appropriate assurance must be undertaken that this is effective.

7.7 Appropriate tools for maintenance activities including configuration management must be used and resources identified to maintain these tools.

7.8 Maintenance personnel must be trained in:

- the maintenance processes
- criticality of any proof tests
- configuration management requirements of hardware and software components

Performance and Monitoring

8.1 Where an incident investigation is undertaken for a safety related system, resources with appropriate technical competence must be involved in the investigation to assess current operation and original design (including any modifications).

8.2 Lead and lag indicators must be developed and defined for the safety related system and a process for extracting the required data is to be documented.

8.3 A programme to monitor, measure and review indicators must be developed and applied that ensures the safety related system was specified correctly, assumptions around the performance were correct and that the safety performance is maintained at its defined level.

8.4 A programme of assurance must be defined as part of a plan to maintain the performance of the safety related system.

Cybersecurity

9.1 The security of the system must have demonstrated that the risks related to the safety functions have been managed in accordance with the company standards and cybersecurity frameworks.

9.2 The safety requirements must include cybersecurity controls with associated verification and validation activities.

Change Management

10.1 Any change management that affects the delivery of functional safety must review the original hazard and risk analysis using the hazard or risk register developed.

10.2 Organisational change that includes roles or management of roles that includes functional safety must include a review of the specific responsibilities and ensure these remain effective.

Modifications

11.1 Modifications to any safety related system must be properly planned reviewed and approved prior to undertaking the modification and change.

11.2 The safety performance of the safety system and functions being modified must be demonstrated to have been maintained at the level required.

Legacy Systems

12.1 An evaluation of the performance of legacy safety related systems, other than those considered low complexity (i.e. systems, sub-systems and components whose failure modes are well defined and understood and where the system behaviour under all fault conditions can be completely understood) must be undertaken. Where a significant shortfall is identified with the level of risk reduction expected or required, a programme to manage the risk effectively through maintenance, regular testing and operational controls must be developed with a documented rationale to support the schedule and scope to address the gaps.

12.2 Identified safety systems delivering safety functions that are considered legacy must have a functional safety management plan.

Appendix A – International Functional Safety Standards

Projects should consider using one or a combination of the following standards:

Reference	Application
IEC 61508	Generic to Electronic, Electrical and Programmable Electronic Systems. Especially useful for developing new systems
IEC 61511 / ISA 84.01	Safety Instrumented Systems for the Process Industry Sector
IEC 62061	Safety of machinery -- Functional safety of safety-related control systems
IEC 62278 IEC 62279 IEC 62425	Systematic safety management process in the railway sector
ISO 13849	Safety of machinery -- Safety-related parts of control systems

Note that the above needs to be considered with consideration of local legislation and practice required by a national regulator and the highest standard (i.e. local law vs international standards) is to be applied. It is often appropriate to supplement the above standards with specific technical standards such as ISO Type B and C standards.

Appendix B – Definitions

Legacy safety related systems	All systems that are operational or in the design and implementation stage prior to the effective date of this standard.
Low complexity systems	Systems that satisfy these conditions: • The failure modes of the system, sub-systems and components are well defined and understood • The system behaviour under all fault conditions can be completely understood
Safety Integrity Level (SIL) (in some standards defined similarly as Category or Performance Levels)	Discrete level corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest. Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the safety-related systems. A safety integrity level (SIL) is not a property of a system, subsystem, element or component.
Safety related systems	Within this standard this is any system whose correct operation is necessary for ensuring or maintaining safety and protects events that may lead to fatalities (or significant environment or asset damage). In process safety this may be instrumented protective systems, in rail and mine automation safety related or safety critical systems
Supply Chain	Any Rio Tinto assets or infrastructure that enables transport of products to clients such as a rail network or port infrastructure.
Verification	IEC 61508 definition “confirmation by examination and provision of objective evidence that the requirements have been fulfilled”

Validation	IEC 61508 definition “confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled”

Appendix C – Accountabilities

Section	Implementation requirements		
	Projects	Sites / Assets	Operational Readiness
1. Managing Functional Safety	Yes	Yes	
2. Understanding Functional Safety risk	Yes		
3. Procurement	Yes	Yes	
4. Design and Implementation	Yes		
5. Acceptance	Yes	Yes	
6. Operating		Yes	Yes
7. Maintenance		Yes	Yes
8. Performance and Monitoring		Yes	Yes
9. Cybersecurity	Yes	Yes	Yes
10. Change Management	Yes	Yes	
11. Modifications		Yes	
12. Legacy Systems		Yes	

Appendix D – Competencies

For a person to be competent, they need qualifications, experience, and qualities appropriate to their duties. These include:

- such training as would ensure the necessary knowledge of the field for the tasks that they are required to perform
- appropriate knowledge of the hazards and failures of the equipment for which they are responsible so that they can understand the risks arising from those hazards
- knowledge and understanding of the working practices used in the organisation for which they work
- an appreciation of their own limitations and constraints, whether of knowledge, experience, facilities, resources, etc.

An example of aspects requiring competencies required to support a safety-related system is provided below

Functional safety engineering knowledge, training and experience appropriate to the lifecycle phase, for example:

- hazard and risk analysis
- safety requirements specification and allocation
- safety performance
- human factors
- architectural design
- hardware realisation
- software realisation
- installation and commissioning

- validation
- operation and maintenance
- modification

Functional safety engineering knowledge, training and experience appropriate to the technology used, for example

- sensors
- logic system
- proprietary programming or configuration language
- communications protocol
- final elements

Functional safety management knowledge, training and experience appropriate to the project and/or site, for example

- lifecycle planning
- safety management (e.g. safety culture, incident learning, managing competence)
- safety assurance
- independent safety assessment
- Application domain knowledge
- Knowledge of the legal and safety regulatory requirements