RioTinto

HSE-B-31

Norme du Groupe

D7 – Sécurité fonctionnelle

<table>
<tr><td rowspan="4">Norme du Groupe</td><td colspan="4">Titre : Sécurité fonctionnelle</td></tr>
<tr><td colspan="4">Fonction : Santé, sécurité, environnement et sûreté</td></tr>
<tr><td colspan="4">Nombre de pages : 11</td></tr>
<tr><td>Date d'approbation :
Juillet 2019</td><td>Entrée en vigueur :
1er sept. 2019</td><td>Remplace :
S.O.</td><td>Pas d’audit avant :
1er septembre 2020</td></tr>
<tr><td colspan="2">Propriétaire :
Directeur mondial, SSES</td><td colspan="2">Approuvé par :
Comité exécutif</td><td>Public cible :
Tous les employés et les prestataires de services de Rio Tinto et chaque unité d’affaires et fonction de Rio Tinto effectuant du travail sur les systèmes liés à la sécurité</td></tr>
<tr><td colspan="5">Liens directs avec d’autres politiques, normes, procédures ou notes d’orientation pertinentes :

Norme du système de gestion de Rio Tinto
Norme de gestion des actifs du Groupe
Norme de gestion des risques du Groupe
Procédure du Groupe pour la sécurité de l’information et la cybersécurité
Norme d’approvisionnement du Groupe</td></tr>
<tr><td colspan="5">Objectif du document :

• Appuyer la mise en œuvre de la politique SSEC du Groupe.
• Ce document précise les exigences minimales qui doivent être respectées pour appuyer la mise en œuvre de la Norme du système de gestion de Rio Tinto relativement à la mise en place de systèmes techniques caractérisés par une sécurité fonctionnelle rigoureuse.</td></tr>
</table>

Champ d’application et objectifs

La présente norme s’applique à toutes les unités d’affaires ainsi qu’à tous les projets et à tous les établissements gérés de Rio Tinto (y compris la chaîne d’approvisionnement).

Le but de cette norme est de décrire les exigences minimales de gestion efficace de la sécurité fonctionnelle au sein de Rio Tinto et de faire en sorte que, là où nous avons des contrôles d’ingénierie applicables à la sécurité, nous mettions l’accent sur la sécurité technique et fonctionnelle, ainsi que sur la sécurité personnelle.

La sécurité fonctionnelle est le cadre utilisé pour fournir des fonctions de sécurité cruciales dans nos systèmes techniques et pour en maintenir l’efficacité. L’application des principes de sécurité fonctionnelle dans cette norme permet à Rio Tinto d’avoir la certitude que les systèmes techniques offrent des mesures de protection efficaces et contrôlent les risques.

La sécurité fonctionnelle est un concept applicable à tous les secteurs industriels. Elle est fondamentale pour la mise en place des systèmes techniques complexes utilisés pour les systèmes liés à la sécurité. Elle offre l’assurance que les systèmes liés à la sécurité permettront la réduction des risques nécessaire.

Les exigences de cette norme doivent être appliquées à tous les systèmes techniques pouvant provoquer des événements menant à des accidents mortels ou à des blessures importantes, afin que l’entreprise puisse mettre en place et exploiter des systèmes correspondant à un niveau tolérable de risque.

Cette norme doit être appliquée à la gestion des risques significatifs pour la santé et l’environnement ainsi que pour la sécurité, là où des contrôles techniques sont utilisés.

Exigences de contrôle

Les exigences de gestion précises énoncées dans cette norme s’appliquent en sus des exigences définies dans la Norme du système de gestion de Rio Tinto.

1 Gestion de la sécurité fonctionnelle

1.1 Les sites ou les projets doivent choisir une norme (ou plusieurs normes) reconnue et courante qui représente une bonne pratique dans le secteur auquel la sécurité fonctionnelle doit s'appliquer (voir les exemples à l'annexe A). La justification du caractère approprié de la norme choisie doit être indiquée. Cette justification doit comprendre une recension des lois applicables et des documents publiés par les organismes de réglementation au sujet de la sécurité fonctionnelle.

1.2 Pour l'exécution d'un projet, un plan de gestion de la sécurité fonctionnelle doit être élaboré pendant ou avant l'étape de faisabilité. Ce plan doit correspondre à la nature et à la portée des risques pour la sécurité fonctionnelle. Il doit répondre aux exigences des lois pertinentes et à celles de la présente norme de sécurité fonctionnelle.

1.3 Lorsqu'un projet consiste à mettre en place un système ayant une exigence importante de performance en matière de sécurité (par exemple, qui respecte un niveau d'intégrité de sécurité (SIL), une catégorie de sécurité ou un niveau de performance (PL)), l'équipe du projet doit s'assurer que le fournisseur et l'intégrateur de système dressent aussi un plan de gestion de la sécurité fonctionnelle.

1.4 Les sites qui exploitent des technologies ou des systèmes liés à la sécurité doivent avoir un plan de gestion de la sécurité fonctionnelle qui sert à assurer la performance continue de ces systèmes pendant l'exploitation et la maintenance.

1.5 Le plan de gestion de la sécurité fonctionnelle doit être approuvé par le chef de projet, dans le cas des projets, et par la haute direction du site, dans le cas des sites d'exploitation.

1.6 Un processus d'audit doit être développé et mis en œuvre pour le plan de gestion de la sécurité fonctionnelle.

1.7 Lorsque des systèmes ou des technologies liés à la sécurité sont mis en œuvre ou modifiés, des niveaux appropriés d'indépendance par rapport à l'équipe d'exécution doivent être définis pour les rôles de gouvernance, d'audit et d'évaluation conformément aux normes reconnues adoptées.

Gouvernance

1.8 Un processus de gouvernance de la sécurité fonctionnelle doit être en place avant le début du travail de conception de la solution.

1.9 La gouvernance doit être maintenue pour la phase d'exploitation et de maintenance du cycle de vie afin que la performance en matière de sécurité soit obtenue et soutenue et que les changements d'ordre technique ou les changements des processus de soutien liés aux systèmes de sécurité tiennent compte des exigences de sécurité et des nouveaux dangers identifiés.

Ressources

1.10 Les sites et les projets doivent mettre en place un processus pour déterminer les principaux rôles et responsabilités relatifs à la sécurité fonctionnelle et pour les consigner dans le plan de gestion de la sécurité fonctionnelle.

1.11 Les compétences doivent être démontrées, vérifiées et inscrites pour chaque phase pertinente du cycle de la sécurité fonctionnelle. Lorsqu'un système est considéré comme critique pour la sécurité (c'est-à-dire avec un niveau d'intégrité de sécurité (SIL) de 1 ou plus ou avec une catégorie ou un PL équivalent), ces compétences doivent être documentées dans le processus d'assurance.

1.12 Les ressources doivent être indiquées pour le processus de gouvernance en ce qui concerne l'approbation de la mise en place des systèmes liés à la sécurité. Le niveau de gouvernance doit être proportionnel au risque (ou à la gravité des conséquences), à la nouveauté et à la complexité.

2 Compréhension du risque pour la sécurité fonctionnelle

2.1 Pendant l'étape de préfaisabilité d'un projet et avant l'élaboration du plan de gestion de la sécurité fonctionnelle, le contexte et la portée doivent être définis et présenter les éléments suivants :

- environnement d'exploitation;
- lois applicables, documents d'orientation des organismes de réglementation nationaux, normes nationales et locales;
- concept d'exploitation et/ou objectif d'affaires.

2.2 Les techniques d'identification des dangers et d'analyse des risques doivent être indiquées pendant la phase de planification afin de permettre d'analyser les risques de façon rigoureuse et systématique. Une évaluation des risques de niveau 2 de Rio Tinto n'est pas suffisante en soi et il faut donc effectuer aussi une analyse quantifiée (niveau 3). Lorsque la quantification n'est pas possible en raison de la nature du système, une justification documentée doit être effectuée.

2.3 Un registre des dangers, des causes et des contrôles doit être tenu pendant toute la vie du système afin d'orienter les modifications futures et la mise hors service. Ce registre doit être revu et mis à jour périodiquement en fonction de l'analyse des dangers et des évaluations des risques durant la phase d'analyse et de réalisation du projet, ainsi qu'en fonction des données d'exploitation et de maintenance recueillies pendant la phase d'exploitation et de maintenance.

2.4 Il doit être prouvé que les contrôles et la gestion des risques réduisent le risque au « niveau le plus bas que l'on peut raisonnablement atteindre » (ALARP).

2.5 Les exigences de sécurité doivent provenir de l'analyse des dangers et des risques et y être documentées, et doivent servir de base à la définition des exigences globales des systèmes en vue de l'exécution du projet. Les exigences de sécurité doivent décrire en détail la fonction à accomplir et la performance exigée de la fonction.

2.6 Une spécification des exigences de sécurité pour le système lié à la sécurité doit être maintenue tout au long de la vie du système.

3 Approvisionnement

3.1 Lorsqu'une équipe de projet a mis en place un contrat portant sur des systèmes liés à la sécurité, le contrat doit préciser la norme ou les normes de sécurité fonctionnelle à appliquer.

3.2 Toutes les composantes de la solution du système de sécurité doivent être gérées de manière à ce qu'il ne soit pas possible de les commander ou d'y apporter différentes modifications sans qu'une évaluation de l'impact sur le système de sécurité fonctionnelle soit menée et consignée dans le cadre d'un processus de gestion du changement approuvé.

4 Conception et mise en œuvre

4.1 Une nouvelle conception qui comprend des fonctions de sécurité doit appliquer le cadre correspondant aux normes reconnues (comme la norme IEC 61508 ou les exemples mentionnés à l'annexe A, ou leur équivalent courant).

4.2 La décision sur la norme ou les normes à appliquer doit être approuvée par les représentants de Rio Tinto de l'unité d'affaires responsable de l'exécution du projet ainsi que de l'unité d'affaires responsable de l'exploitation et de la maintenance qui recevra le système lors du transfert.

4.3 Le développement de tout système qui comprend des fonctions de sécurité soumises à une exigence de performance en matière de sécurité doit être effectué au moyen d'un système d'assurance qualité conforme aux exigences de la norme ISO 9001 ou d'une norme équivalente.

4.4 Des évaluations indépendantes de la sécurité fonctionnelle doivent être menées conformément aux exigences de performance en matière de sécurité et à la norme choisie, avant la mise en service du système.

4.5 Une évaluation indépendante des processus de sécurité fonctionnelle du fournisseur doit être effectuée afin de fournir l'assurance que le travail est effectué de manière appropriée. Cette évaluation doit avoir lieu aux phases du cycle de vie pendant lesquelles il est possible de résoudre les problèmes éventuels, afin de réduire le plus possible les répercussions sur l'obtention de la sécurité fonctionnelle.

4.6 Lorsqu'un système lié à la sécurité est développé pour être appliqué à un projet ou un site en particulier, la conformité du système à la norme doit être auditée avant l'acceptation du système au nom de Rio Tinto. Cet audit doit porter sur l'assurance qualité du matériel et du logiciel ainsi que sur l'application des processus de sécurité fonctionnelle indiqués dans le plan de gestion de la sécurité fonctionnelle concerné.

4.7 Les résultats de la vérification doivent être enregistrés pour chaque phase du cycle de la sécurité pour les systèmes liés à la sécurité.

4.8 Il faut vérifier si le système lié à la sécurité a été installé conformément aux conceptions et spécifications approuvées.

4.9 Un plan de validation doit être élaboré pour indiquer qui entreprendra la validation, les exigences d'indépendance et la méthode de validation.

5 Acceptation

5.1 Un processus défini doit préciser comment le système lié à la sécurité sera mis en service et quels intrants doivent être fournis avant que l'acceptation puisse avoir lieu.

5.2 Les sites et les projets doivent définir les critères d'acceptation selon lesquels l'acceptation doit être documentée au minimum par le propriétaire de l'actif, le responsable de la maintenance de l'actif et l'exploitant de l'actif.

5.3 Un rapport de validation doit être documenté et publié comme intrant de l'acceptation officielle d'un système lié à la sécurité mis en service.

5.4 La validation doit consister à s'assurer que le système de sécurité installé et mis en service remplit les fonctions et affiche la performance énoncée dans les exigences de sécurité.

5.5 L'acceptation doit déterminer si le système a atteint efficacement les réductions de risque proposées, si le niveau de risque est tolérable et s'il est nécessaire de démontrer que le risque a été réduit au « niveau le plus bas que l'on peut raisonnablement atteindre » (ALARP).

6 Exploitation

6.1 Des processus opérationnels documentés qui soutiennent la performance d'un système lié à la sécurité doivent être en place avant qu'il soit prévu d'exploiter le système; les opérateurs doivent recevoir une formation sur ces processus.

6.2 Les contraintes ou les hypothèses formulées pendant le développement d'un système appuyant la sécurité fonctionnelle et relatives à l'exploitation et à la maintenance doivent être intégrées dans les processus pertinents du site, et les liens justifiant la gestion du changement future doivent être enregistrés.

6.3 Lorsque l'introduction d'un système lié à la sécurité peut influer sur une intervention d'urgence en cas d'incident (par exemple, l'accès à un système automatisé), il faut s'assurer continuellement de la façon dont cela est communiqué et adopté par l'organisation d'intervention d'urgence.

6.4 Les contrôles qui ont été identifiés et consignés au cours de la phase d'identification des dangers et d'évaluation des risques et qui sont pertinents pour l'intervention d'urgence doivent figurer dans les processus d'intervention d'urgence et dans la formation, y compris l'utilisation d'arrêts d'urgence, les opérations d'isolation et les processus de communication, à l'intention des opérateurs du système de commande.

7 Maintenance

7.1 Des processus de maintenance documentés qui soutiennent la performance d'un système lié à la sécurité doivent être en place avant qu'il soit prévu d'exploiter le système.

7.2 Des processus documentés pour les essais de sûreté et les inspections doivent être en place avant l'acceptation d'un système lié à la sécurité.

7.3 L'équipe de maintenance doit disposer de systèmes garantissant que les essais de sûreté sont exécutés dans les intervalles requis déterminés durant la conception des systèmes et doit remettre des rapports sur les essais de sûreté non effectués à l'intérieur de ces intervalles.

7.4 Un processus doit être en place pour gérer et approuver l'exploitation de systèmes comportant des composants défectueux ou de systèmes qui n'ont pas respecté l'intervalle entre essais de sûreté permettant de garantir que les systèmes restent sûrs.

7.5 Une gestion de la configuration doit être en place pour la maintenance d'un système lié à la sécurité, et les responsabilités de gestion efficace doivent être clairement définies.

7.6 Lorsque la gestion de la configuration est effectuée par un fournisseur ou un prestataire de services, il faut s'assurer adéquatement de l'efficacité de cette étape.

7.7 Des outils appropriés pour les activités de maintenance, y compris la gestion de la configuration, doivent être utilisés et des ressources de maintenance de ces outils doivent être désignées.

7.8 Le personnel de maintenance doit recevoir une formation sur :

- les processus de maintenance;
- la criticité des essais de sûreté;
- les exigences de gestion de la configuration des composants matériels et logiciels.

8 Performance et surveillance

8.1 Lorsqu'une enquête sur un incident est effectuée pour un système lié à la sécurité, des ressources possédant une compétence technique appropriée doivent participer à l'enquête pour évaluer le fonctionnement actuel et la conception initiale (y compris toute modification).

8.2 Des indicateurs précurseurs et retardés doivent être définis pour le système lié à la sécurité et un processus d'extraction des données requises doit être documenté.

8.3 Un programme de surveillance, de mesure et de revue des indicateurs doit être mis au point et appliqué afin de s'assurer que la spécification du système lié à la sécurité était correcte, que les hypothèses de performance étaient correctes et que la performance en matière de sécurité s'est maintenue au niveau défini.

8.4 Un programme d'assurance doit être défini dans le cadre d'un plan afin de maintenir la performance du système lié à la sécurité.

9 Cybersécurité

9.1 La sécurité du système doit démontrer que les risques relatifs aux fonctions de sécurité ont été gérés conformément aux normes de l'entreprise et aux cadres de cybersécurité.

9.2 Les exigences de sécurité doivent comprendre des contrôles de la cybersécurité ainsi que les activités de vérification et de validation connexes.

10 Gestion du changement

10.1 Lorsque la gestion d'un changement a un effet sur l'obtention de la sécurité fonctionnelle, on doit revoir l'analyse des dangers et des risques initiale à partir du registre des dangers ou des risques constitué.

10.2 Lorsqu'un changement organisationnel comprend des rôles ou la gestion des rôles concernant la sécurité fonctionnelle, on doit revoir les responsabilités spécifiques et s'assurer qu'elles demeurent effectives.

11 Modifications

11.1 Des modifications d'un système lié à la sécurité doivent être convenablement planifiées, examinées et approuvées avant d'être mises en place.

11.2 Il doit être prouvé que la performance en matière de sécurité du système et des fonctions modifiées a été maintenue au niveau requis.

12 Anciens systèmes

12.1 Une évaluation de la performance des anciens systèmes liés à la sécurité, autres que ceux qui sont considérés comme des systèmes de faible complexité (systèmes, sous-systèmes et composants dont les modes de défaillance sont bien définis et compris et dont le comportement dans toutes les conditions de défaut peut être parfaitement compris) doit être effectuée. Lorsqu'une lacune importante est repérée relativement au niveau de réduction des risques attendu ou requis, un programme ayant pour but de gérer les risques efficacement au moyen de la maintenance, d'essais périodiques et de contrôles opérationnels doit être mis au point et accompagné d'une justification documentée de l'échéancier et de la portée des travaux nécessaires pour corriger la lacune en question.

12.2 Les systèmes de sécurité remplissant des fonctions de sécurité et considérés comme d'anciens systèmes doivent faire l'objet d'un plan de gestion de la sécurité fonctionnelle.

Annexe A – Normes de sécurité fonctionnelle internationales

Les projets devraient envisager d'utiliser une des normes suivantes ou une combinaison de ces normes :

Référence	Application
IEC 61508	Norme générique pour les systèmes électriques, électroniques et électroniques programmables. Particulièrement utile pour le développement de nouveaux systèmes.
IEC 61511 / ISA 84.01	Systèmes instrumentés de sécurité pour le secteur des industries de transformation
IEC 62061	Sécurité des machines – Sécurité fonctionnelle des systèmes de commande relatifs à la sécurité
IEC 62278 IEC 62279 IEC 62425	Processus de gestion systématique de la sécurité dans le secteur ferroviaire
ISO 13849	Sécurité des machines – Parties des systèmes de commande relatives à la sécurité

Il est à noter que ces normes doivent être envisagées compte tenu des lois et pratiques locales exigées par un organisme de réglementation national et que la norme la plus élevée (loi locale ou norme internationale) doit être appliquée. Il convient souvent de compléter les normes ci-dessus par des normes techniques précises comme les normes ISO de type B et C.

Annexe B – Définitions

Anciens systèmes liés à la sécurité	Tous les systèmes qui sont en exploitation ou à l'étape de conception et de mise en œuvre avant la date d'entrée en vigueur de la présente norme.
Systèmes de faible complexité	Systèmes qui remplissent les conditions suivantes : • Systèmes, sous-systèmes et composants dont les modes de défaillance sont bien définis et compris • Systèmes dont le comportement dans toutes les conditions de défaut peut être parfaitement compris
Niveau d'intégrité de sécurité (SIL) (défini dans certaines normes de la même façon que la catégorie ou le niveau de performance)	Niveau discret correspondant à une plage de valeurs d'intégrité de sécurité, le SIL 4 représentant le plus haut niveau d'intégrité de sécurité et le SIL 1 le plus bas niveau. Les niveaux d'intégrité de sécurité servent à préciser les exigences d'intégrité des fonctions de sécurité à allouer aux systèmes liés à la sécurité. Un niveau d'intégrité de sécurité (SIL) n'est pas une propriété d'un système, d'un sous-système, d'un élément ou d'un composant.
Systèmes liés à la sécurité	Dans cette norme, il s'agit de tout système dont le fonctionnement correct est nécessaire pour assurer ou maintenir la sécurité et qui empêche des événements de mener à des accidents mortels ou à des dommages importants causés à l'environnement ou aux actifs. Dans le domaine de la sécurité des procédés, il peut s'agir de systèmes de protection instrumentés; dans le domaine de la sécurité de l'automatisation des activités ferroviaires et minières, il peut s'agir de systèmes liés à la sécurité ou critiques pour la sécurité.
Chaîne d'approvisionnement	Les actifs ou les infrastructures de Rio Tinto qui permettent d'acheminer les produits aux clients, par exemple un réseau de chemin de fer ou une

	infrastructure portuaire.
Vérification	Définition de la norme IEC 61508 : confirmation, appuyée sur un examen et des preuves tangibles, que les exigences ont été respectées.
Validation	Définition de la norme IEC 61508 : confirmation, appuyée sur un examen et des preuves tangibles, que les exigences particulières pour un usage spécifié prévu ont été respectées.

Annexe C – Responsabilités

Section	Exigences de mise en œuvre		
	Projets	Sites / Actifs	Préparation opérationnelle
1. Gestion de la sécurité fonctionnelle	Oui	Oui	
2. Compréhension du risque pour la sécurité fonctionnelle	Oui		
3. Approvisionnement	Oui	Oui	
4. Conception et mise en œuvre	Oui		
5. Acceptation	Oui	Oui	
6. Exploitation		Oui	Oui
7. Maintenance		Oui	Oui
8. Performance et surveillance		Oui	Oui
9. Cybersécurité	Oui	Oui	Oui
10. Gestion du changement	Oui	Oui	
11. Modifications		Oui	
12. Anciens systèmes		Oui	

Annexe D – Compétences

Pour qu'une personne soit compétente, elle doit avoir des qualifications, de l'expérience et des qualités appropriées à ses tâches. Par exemple :

- une formation qui procure la connaissance nécessaire du domaine pour les tâches que la personne doit exécuter;
- une connaissance appropriée des dangers et des défaillances de l'équipement dont elle a la responsabilité afin qu'elle puisse comprendre les risques découlant de ces dangers;
- une connaissance et une compréhension des pratiques de travail utilisées dans l'organisation pour laquelle elle travaille;
- une reconnaissance de ses propres limitations et contraintes sur le plan des connaissances, de l'expérience, des installations, des ressources, etc.

Des exemples d'aspects exigeant des compétences pour s'occuper d'un système lié à la sécurité sont indiqués ci-dessous :

Connaissances, formation et expérience en ingénierie de la sécurité fonctionnelle qui sont appropriées pour la phase du cycle de vie, par exemple :

- analyse des dangers et des risques
- spécification et allocation des exigences de sécurité
- performance en matière de sécurité
- facteurs humains
- conception architecturale
- réalisation du matériel
- réalisation du logiciel
- installation et mise en service
- validation
- exploitation et maintenance
- modification

Connaissances, formation et expérience en ingénierie de la sécurité fonctionnelle qui sont appropriées pour la technologie utilisée, par exemple :

- capteurs
- système logique
- langage de programmation ou de configuration exclusif
- protocole de communications
- éléments finaux

Connaissances, formation et expérience en ingénierie de la sécurité fonctionnelle qui sont appropriées pour le projet ou le site, par exemple :

- planification du cycle de vie
- gestion de la sécurité (p. ex. culture de sécurité, apprentissage à partir des incidents, gestion des compétences)
- assurance de la sécurité
- évaluation indépendante de la sécurité
- connaissance du domaine d'application
- connaissance des exigences des lois et des règlements en matière de sécurité