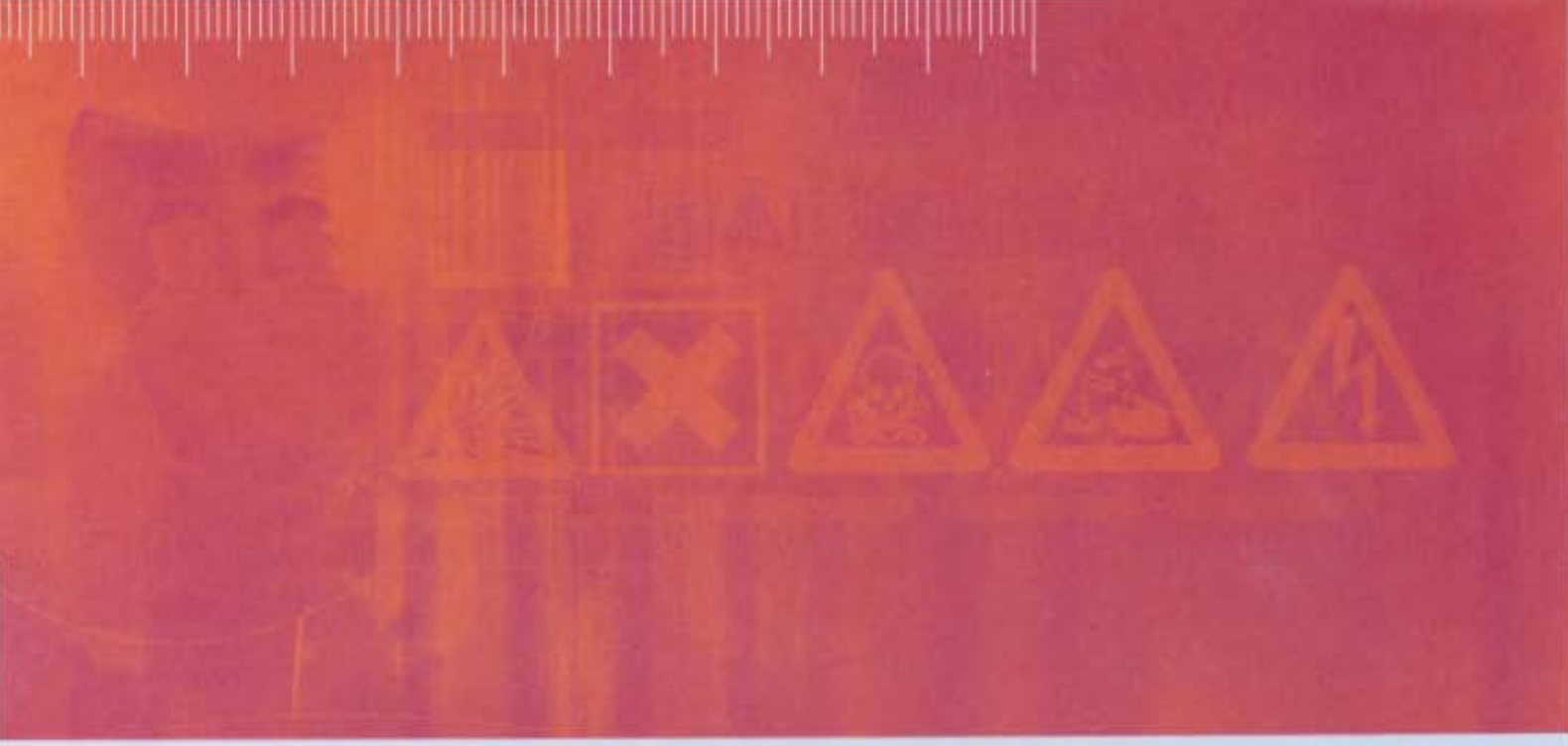


Document de synthèse relatif à une Barrière à Action Manuelle de Sécurité (BAMS)

ACTIONNEMENT D'UN BOUTON DE MISE EN SÉCURITÉ (TYPE « ARRET D'URGENCE »)

N° DRA-18-172833-07285B
03 AVRIL 2019

INERIS
maîtriser le risque
pour un développement durable

Document de synthèse relatif à une Barrière à Action Manuelle de Sécurité (BAMS)

Type d'installation : Tout type d'installation

Nom du dispositif : Actionnement d'un Bouton de mise en sécurité (type « Arrêt d'Urgence »)

Document élaboré par : l'INERIS

Liste des personnes ayant participé à l'étude : Ahmed Adjadj, Ludovic Moulin, Franck Prats

PRÉAMBULE

Les documents de synthèse relatifs à une barrière de sécurité sont la propriété de l'INERIS. Il n'est accordé aux utilisateurs qu'un droit d'utilisation n'impliquant aucun transfert de propriété.

Le présent rapport a été établi sur la base des informations fournies à l'INERIS, des données (scientifiques ou techniques) disponibles et objectives et de la réglementation en vigueur, ainsi que des pratiques et méthodologies développées par l'INERIS. Bien que l'INERIS s'efforce de fournir un contenu fiable, il ne garantit pas l'absence d'erreurs ou d'omissions.

Ce rapport est destiné à des utilisateurs disposant de compétences professionnelles spécifiques dans le domaine des risques accidentels. Les informations qu'il contient n'ont aucune valeur légale ou réglementaire. Ce sont des informations générales. Elles ne peuvent, en aucun cas, répondre aux besoins spécifiques de chaque utilisateur. Ces derniers seront donc seuls responsables de l'utilisation et de l'interprétation qu'ils feront des rapports. De même, toute modification et tout transfert de ces documents se feront sous leur seule responsabilité.

La responsabilité de l'INERIS ne pourra, en aucun cas, être engagée à ce titre.

	Rédaction		Vérification	Approbation
Nom	Ludovic Moulin	Ahmed Adjadj	François Massé	Sylvain Chaumette
Qualité	Responsable de l'unité HUGO (Facteurs Humains et Gouvernance des Organisations) Direction des Risques Accidentels	Ingénieur d'études et de recherche Direction des Risques Accidentels	Responsable de l'unité QRIB (Quantification des RIsques et performance des Barrières) Direction des Risques Accidentels	Responsable du pôle AGIR (Analyse et Gestion Intégrées des Risques) Direction des Risques Accidentels
Visa				

TABLE DES MATIÈRES

1 FONCTION DE SÉCURITÉ

La fonction traitée dans ce document est le maillon d'une chaine de mise en sécurité permettant de mettre en sécurité un équipement, un système ou une installation par l'actionnement d'un Bouton d'Arrêt d'Urgence (BAU) et la commande associée.

L'actionnement d'un BAU provoque une mise en sécurité par la coupure des énergies (électrique, pneumatique…) et l'arrêt immédiat ou contrôlé de tout processus en cours (arrêt d'un équipement, d'un système ou d'une installation (par exemple par la fermeture/ouverture de vanne)) avec éventuellement le démarrage de systèmes de sécurité (extinction incendie, rideau d'eau, extracteur…).

L'actionnement d'un BAU présente la particularité de nécessiter une intervention humaine pour son activation. La performance de ce dispositif nécessite de considérer à la fois le bon fonctionnement de la chaine de commande du BAU et la capacité de l'opérateur à détecter, diagnostiquer la situation et activer le BAU. L'évaluation de sa performance (par exemple dans le cadre d'une étude de dangers) nécessite de prendre en compte à la fois sa composante technique et sa composante humaine et organisationnelle. Cette évaluation peut reposer sur l'utilisation des approches Oméga 10[1] et Oméga 20[2], telles que présentées dans ce document.

La performance de la fonction de sécurité activée par l'actionnement d'un bouton d'Arrêt d'Urgence dépendra également de la performance de la détection (quand réalisée par un ou des détecteurs), et des actions de sécurité des actionneurs commandés par une chaîne d'AU. L'évaluation de la performance des détecteurs et des actionneurs n'est pas traitée dans cette fiche.

2 REGLEMENTATION OU TEXTES NORMATIFS APPLICABLES

Un système d'arrêt d'urgence provoque, après actionnement du BAU, une mise en sécurité via un circuit de commande qui permet de traiter l'ordre d'arrêt d'urgence et de commander les moyens d'arrêt.

Les éléments du circuit de commande des fonctions de sécurité (relais, modules logiques de sécurité, etc.) et les moyens d'arrêts (relais, contacteurs, distributeurs électropneumatiques, etc.) sont réglementés en Europe par la directive Machines 2006/42/CE[3] dont les exigences pourraient être appliquées, totalement ou partiellement, aux système d'arrêt d'urgence équipant les installations industrielles.

Parmi les normes dont les éléments du circuit de commande et d'arrêts doivent faire l'objet d'une conformité, nous pouvons citer :

- NF EN ISO 13850[4],
- ISO EN 13849-1[5],
- IEC 62061[6],
- NF EN 60947-5-5/A2[7],
- NF EN IEC 60947-4-1[8],
- IEC 60204-1 [9],
- EN ISO 12100[10],
- NF EN IEC 61511[11],
- NF EN IEC 61508[17].

Pour l'actionnement du BAU suite une alarme, les normes IEC 62682[12] et IEC 62603-1[13] peuvent être citées, entre autres référentiels, pour les aspects gestion des alarmes dans les process industriels.

Pour la conception d'interface humain / machine, plusieurs normes décrivent les exigences ergonomiques pour faciliter la perception de l'information sur un écran informatique. Voici quelques exemples pertinents dans le cas d'une interface d'alarme(s) pour un BAU :

- La norme ISO 9241-210[14],
- La norme ISO 9241-12[15],
- La norme ISO 9241-125[16].

Une présentation de ces normes est donnée en Annexe A.

3 PRINCIPE DE FONCTIONNEMENT

Un système d'arrêt d'urgence déclenche, à la suite de la détection d'une situation dégradée, une mise en sécurité :

- par la coupure des énergies (électrique, pneumatique…) et l'arrêt immédiat ou contrôlé de tout processus en cours (arrêt d'un équipement, d'un système ou d'une installation),
- et/ou par le déclenchement/démarrage de systèmes de sécurité (extinction incendie, rideau d'eau, extracteur…).

Il est composé en général d'un (ou de plusieurs) boutons poussoirs de coupure ou de démarrage (BAU), lesquels assurent une mise en sécurité via un circuit de commande. De façon générale, un système d'arrêt d'urgence est décomposé en quatre parties :

1. la partie intervention d'un opérateur pour détecter une situation dangereuse (par des alarmes…), diagnostiquer la situation et activer le BAU,
2. la partie organe de commande (le BAU) : appareil de commande manœuvrable manuellement et utilisé pour initier la fonction d'arrêt d'urgence. Cet organe de commande engendre l'ordre d'arrêt ou démarrage lorsqu'il est actionné,
3. la partie circuit de commande : système de commande permettant de traiter l'ordre d'arrêt ou de démarrage (relais, module logique de sécurité, automate),
4. la partie moyens de mise en sécurité (d'arrêt ou de démarrage) qui peuvent prendre différentes formes :
    a. appareils de commutation de puissance (contacteurs, distributeurs électropneumatiques, variateurs de vitesse, etc.) qui arrêtent ou démarrent les actionneurs finaux (moteur, vanne…),
    b. moyens de déconnexion mécanique (embrayage, etc.),
    c. freins utilisés pour accomplir la fonction d'arrêt d'urgence.

Cette décomposition d'un système d'arrêt d'urgence est présentée dans le tableau 1 suivant.

Tableau 1 : Composition d'un système d'arrêt/démarrage d'urgence

<table>
<tr><th colspan="4">Les quatre parties d'un système d'arrêt/démarrage d'urgence</th></tr>
<tr><th>1</th><th>2</th><th colspan="2">3</th><th>4</th></tr>
<tr><th>Intervention d'un opérateur</th><th>Organe de commande (BAU)</th><th colspan="2">Circuit de commande</th><th>Moyens de mise en sécurité</th></tr>
<tr><td rowspan="4">  </td><td rowspan="4"> 
 
  </td><td rowspan="2">Commande directe</td><td>Relais  </td><td></td></tr>
<tr><td>Contacteurs  </td><td></td></tr>
<tr><td rowspan="2">Commande et surveillance par un module logique de sécurité ou un APS</td><td>Module logique de sécurité  </td><td>Variateurs de vitesse  </td></tr>
<tr><td>Automate  </td><td>Distributeurs électropneumatiques 
…</td></tr>
</table>

Cette fiche barrière ne traite que des trois premières parties et elles sont décrites dans les paragraphes qui suivent :

- Paragraphe 3.1 pour la partie intervention d'un opérateur pour détecter, diagnostiquer la situation et activer le BAU,
- Paragraphe 3.2 pour la partie organe de commande (le BAU),
- Paragraphe 3.3 pour la partie circuit de commande.

L'actionnement du BAU par un opérateur est la réaction à une situation dangereuse. La détection de celle-ci par les opérateurs peut être le résultat :

- soit d'un déclenchement automatique d'un signal d'alarme (lumineux et/ou sonore),
- soit de la détection d'une situation anormale (valeur anormale d'un paramètre, incendie, fuite d'un produit…).

3.1 L'INTERVENTION D'UN OPÉRATEUR

L'intervention de l'opérateur est le maillon décisionnel de la chaine de sécurité associée au BAU. Cette chaine de sécurité est une barrière de rattrapage de dérive car elle permet de détecter une dérive et d'en limiter les conséquences.

Selon les sites, les contraintes ou exigences techniques, les moyens et ressources d'une entreprise, la mise en place d'un système dit Bouton d'Arrêt d'Urgence va pouvoir prendre plusieurs formes. Ce chapitre propose de se focaliser sur quatre configurations génériques selon l'endroit de la détection d'un problème, et l'endroit de l'actionnement du BAU

Ces configurations technico-organisationnelles retenues et décrites dans le paragraphe 3.1.1 sont :

1. Détection du problème et actionnement du BAU en salle de conduite,
2. Détection du problème sur le terrain, actionnement du BAU en salle de conduite,
3. Détection du problème en salle de conduite, actionnement du BAU sur le terrain,
4. Détection du problème et actionnement du BAU sur le terrain.

Les actions associées à ces configurations peuvent être conditionnées par une « étape de levée de doute ».

Pour compléter cette description contextuelle de la mise en place d'un BAU, un paragraphe propose de faire le point sur les champs d'actions possibles d'un BAU sur une installation. Ces champs d'actions décrits au paragraphe 3.1.2 sont :

1. Le BAU arrêt général,
2. Le BAU arrêt local (chaine de production),
3. Le BAU arrêt machine (équipement).

Pour chacune des quatre configurations présentées ci-dessous, des photos décrivent de manière simple la configuration de la barrière « BAU ».

Ces quatre configurations et la description des trois champs d'action (général, local, machine) serviront de référence pour comprendre les éléments à prendre en compte pour l'évaluation de la performance du BAU en tant que barrière de sécurité.

3.1.1 CONFIGURATION TECHNICO-ORGANISATIONNELLE D'UN BAU

3.1.1.1 DÉTECTION ET ACTIONNEMENT DU BAU EN SALLE DE CONDUITE

Dans cette configuration, un ou des capteurs envoient des informations dans un système électrique et informatique. Quand un seuil est dépassé, ou une configuration de données atteintes, une alarme peut apparaitre sur une interface (écran en salle de conduite) et/ou retentir de manière sonore et/ou visuelle dans les locaux.








L'actionnement du BAU se fait par l'opérateur en salle de conduite, potentiellement après une levée de doute, et déclenche les actions de sécurité.

3.1.1.2 DÉTECTION SUR LE TERRAIN ET ACTIONNEMENT DU BAU EN SALLE DE CONDUITE

Dans cette configuration, un opérateur sur le terrain détecte une anomalie (par exemple au cours d'une ronde, lors d'une opération de consignation ou de maintenance, …). Cet opérateur informe la salle de commande (téléphone de service, talkie-walkie, …).





L'actionnement du BAU se fait par l'opérateur en salle de conduite, potentiellement après une levée de doute, et déclenche les actions de sécurité.

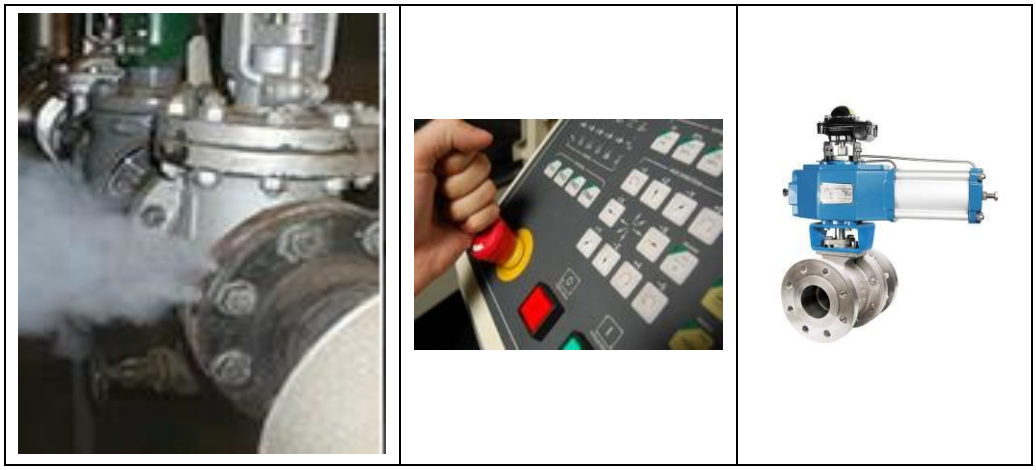
3.1.1.3 DÉTECTION EN SALLE DE CONDUITE, ACTIONNEMENT DU BAU SUR LE TERRAIN

Dans cette configuration, un ou des capteurs envoient des informations dans un système électrique et informatique. Quand un seuil est dépassé, ou une configuration de données atteintes, une alarme peut apparaitre sur une interface (écran en salle de conduite), et/ou retentir de manière sonore et/ou visuelle dans les locaux.

L'actionnement du BAU se fait par l'opérateur sur le terrain, potentiellement après une levée de doute, et déclenche les actions de sécurité.

3.1.1.4 DÉTECTION ET ACTIONNEMENT DU BAU SUR LE TERRAIN

Dans cette configuration, un opérateur sur le terrain détecte une anomalie.



L'actionnement du BAU se fait par l'opérateur sur le terrain et déclenche les actions de sécurité.

3.1.2 LES CHAMPS D'ACTION D'UN BAU

Selon des choix de conception de l'installation, un BAU pourra avoir un impact sur tout ou partie de l'installation. C'est l'analyse des risques qui devra éclairer les choix de conception entre les trois champs d'action d'un BAU, car certains scénarios d'accident nécessiteront des champs d'action différents de la part d'un BAU.

Dans tous les cas, il s'agira d'informer les opérateurs et leurs manageurs de la portée de chaque BAU, et des conditions d'activation qui leurs sont propres. Les points particuliers liés à ces champs d'action sont décrits dans les paragraphes qui suivent.

En conception, le choix entre les différents types de BAU doit faire l'objet d'une analyse particulière pour identifier tous les éléments techniques et organisationnels pertinents à considérer et à prendre en compte. Grace à cette analyse, une procédure d'aide à la décision doit être élaborée. Le processus d'élaboration et de test de la procédure devra mobiliser des opérateurs en charge de la mettre en œuvre.

Dans le cas des configurations présentées au 3.1.1.2 et 3.1.1.3, une relation de subordination, et une procédure claire de décision devra permettre de trancher entre l'arrêt local et général.

3.1.2.1 LE GÉNÉRAL : ARRÊT INSTALLATION (SHUT DOWN)

Une première catégorie de BAU a pour fonction d'arrêter l'ensemble des process ou lignes de production d'une installation industrielle. L'avantage d'un tel système général est de prévenir tout risque de propagation d'un incident local sur l'ensemble d'une installation.

L'inconvénient d'un BAU général est le risque de ne jamais être utilisé car l'opérateur sera toujours réticent à stopper totalement la production. Il risque alors soit de perdre du temps en recherchant une autre solution, soit de privilégier une solution moins radicale, et donc moins efficace.

Comme précisé dans le paragraphe 4.3.2, la prise de décision dépendra du contexte général d'intervention de l'opérateur.

Dans les configurations présentées aux paragraphes 3.1.1.1 et 3.1.1.4, dans lesquelles l'opérateur peut être seul à prendre la décision (soit en salle de commande soit sur le terrain), le risque pour qu'un tel arrêt général ne soit jamais utilisé est important (Cf. paragraphe 4).

Dans les configurations présentées aux paragraphes 3.1.1.2 et 3.1.1.3, ce type d'arrêt permet de minimiser les risques d'une décision isolée. La décision fait l'objet d'une discussion entre l'opérateur sur le terrain et celui de la salle de commande.

3.1.2.2 LE LOCAL : ARRÊT D'UNE UNITÉ DE PRODUCTION

Un arrêt d'urgence local a l'avantage de n'arrêter qu'une partie d'une installation, et donc de préserver une partie de la production. Comme précisé dans le paragraphe 4.3.2, la prise de décision dépendra également du contexte général d'intervention. Néanmoins, il devrait être plus facilement actionnable par un opérateur isolé en comparaison à un arrêt général.

A priori, bien qu'il reste difficile de prendre une décision qui va stopper la production, la crainte de faire une erreur de jugement est moindre car les conséquences, notamment économiques sont plus limitées (contrairement à l'arrêt d'urgence général).

3.1.2.3 LE MACHINE : ARRÊT D'UN ÉQUIPEMENT

Un arrêt d'urgence sur un équipement est le BAU le plus facilement actionnable par un opérateur isolé (configurations 3.1.1.1 et 3.1.1.4). Il concerne l'équipement dont il a la charge, et pour lequel il a développé une certaine expertise qui le rend apte à décider de la nécessité d'une mise à l'arrêt selon les circonstances.

L'impact de cette décision ne devrait affecter qu'une petite partie de la production.

D'un point de vue maitrise des risques, ce type d'arrêt peut s'avérer suffisant pour certains scénarios d'accident, mais insuffisant pour d'autres.

3.2 LE BOUTON D'ARRÊT D'URGENCE

De façon générale dans l'industrie, le BAU est constitué d'un bouton poussoir rouge et rond sur un fond jaune, facilement discernable et accessible pour l'actionnement (appelé bouton "coup de poing") et d'un jeu de contacts (bloc de contacts) ; le tout intégré dans un boîtier. Le jeu de contacts se compose d'un contact normalement ouvert et d'un contact normalement fermé pour ouvrir ou fermer le circuit électrique.

Le BAU peut être recouvert d'un couvercle ou d'un système empêchant une poussée intempestive sur le bouton.

Dans le cas d'un arrêt d'urgence, le BAU avec verrouillage brusque provoque instantanément l'arrêt des processus dangereux. Lorsque le bouton est relâché, le redémarrage ne devant pas se faire automatiquement pour un maintien en sécurité, l'état de commutation doit rester inchangé. Il assure un verrouillage par accrochage mécanique (via une bague de verrouillage). Pour ramener le bouton et le jeu de contacts en position initiale, il nécessite donc un déverrouillage manuel pour pouvoir redémarrer. Ce déverrouillage peut se faire de trois façons différentes :

- Déverrouillage en tirant
- Déverrouillage en tournant
- Déverrouillage à clé

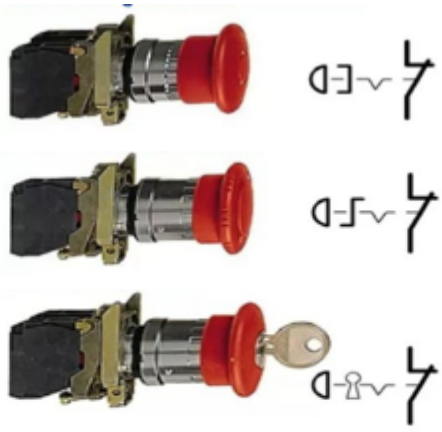


Figure 1 : Type de déverrouillage

Le choix du type de déverrouillage dépendra du contexte (en particulier la prise en compte des exigences de sécurité) et des contraintes organisationnelles de l'entreprise. Le déverrouillage du BAU doit obligatoirement faire l'objet d'une procédure adapté.

Il existe également des boutons d'arrêt d'urgence électroniques pour branchement (de type Plug & Play) sur réseau de terrain.

Figure 2 : Exemple de BAU électronique

3.3 LE CIRCUIT DE COMMANDE

La mise en œuvre d'une fonction d'arrêt/démarrage d'urgence est basée sur un circuit de commande. Ce circuit (relais, module logique de sécurité, automate) permet de traiter l'ordre d'arrêt/démarrage d'urgence et de commander les moyens pour la mise en sécurité.

Cette commande (telle que présentée dans le Tableau 1) peut se faire :

- directement (sans relayage intermédiaire),
- avec une commande et une surveillance par l'intermédiaire d'un module logique de sécurité,
- avec une commande et une surveillance par l'intermédiaire d'un automate programmable de sécurité.

3.3.1 COMMANDE DIRECTE SANS RELAYAGE INTERMÉDIAIRE

La commande des moyens d'arrêt d'urgence sans relayage intermédiaire consiste à commander directement les moyens d'arrêt (relais / contacteurs, distributeurs électropneumatiques, variateurs de vitesse).

Un relais/contacteur (électromécanique ou statique) est un organe électrique permettant :

- d'une part, d'assurer l'ouverture et la fermeture (commutation) d'un circuit électrique,
- et d'autre part, de dissocier et isoler (par une isolation galvanique[1]) la partie puissance de la partie commande du circuit électrique.

Un relais électromécanique est composé principalement d'un électroaimant (bobine) qui, lorsqu'il est alimenté, transmet une force pour commuter mécaniquement les contacts électriques. Dans les circuits mettant en œuvre une certaine puissance, le relais est désigné "contacteur".

L'alimentation de la bobine est obtenue par l'intermédiaire d'un transistor. Le champ magnétique ainsi créé ouvre ou ferme le contact, suivant sa position de repos maintenue par un ressort de rappel.

[1] Isolation galvanique : deux circuits électriques ou électroniques sont isolés galvaniquement, lorsqu'il n'y a aucune liaison conductrice (fil électrique, châssis métallique, etc.) entre ces deux circuits.

Un relais/contacteur statique permet d'assurer la commutation d'un circuit électrique sans recours à des éléments mécaniques ou électromécaniques. Son fonctionnement repose sur des composants électroniques, en particulier des semi-conducteurs.

Schématiquement, les relais/contacteurs sont des interrupteurs qui, via une tension (continue ou alternative) appliquée en entrée, ferment ou ouvrent un/des contacts (commutation), pour laisser passer ou isoler un courant.

Pour une utilisation en sécurité, il faut que la position de repos du contact corresponde à l'action de sécurité (sécurité dite positive).

3.3.2 COMMANDE ET SURVEILLANCE PAR L'INTERMÉDIAIRE D'UN MODULE LOGIQUE DE SÉCURITÉ

Pour des exigences de sécurité, les circuits de commande d'une fonction d'arrêt/démarrage d'urgence sont généralement basés sur la mise en œuvre de blocs logiques de sécurité, même si l'utilisation de relayage "dit standard" reste possible. Les modules de sécurité sont des éléments indispensables pour assurer les fonctions de sécurité. Ils permettent de détecter les défauts de fonctionnement que le relayage "dit standard" ne permet pas d'éviter. Ils pilotent des contacteurs ou des relais de commande qui sont équipés de contacts liés mécaniquement. L'insertion de ces contacts dans la boucle de retour assure la détection d'un défaut sur les sorties.

Ce sont des appareils qui s'intègrent dans les circuits de commande pour assurer la fiabilité et la disponibilité des fonctions de sécurité. Leur câblage interne est réalisé en redondance et leur logique est autocontrôlée.

Ils disposent des fonctionnalités suivantes :

- des sorties de sécurité constituées soit de plusieurs contacts en série appartenant aux relais internes à contacts guidés, soit des sorties statiques,
- un contrôle de la concordance des informations d'entrée,
- un contrôle de leurs liaisons avec le bouton d'arrêt d'urgence,
- une boucle de retour permettant de contrôler l'état des contacts de recopie associés aux relais ou contacteurs commandés par les sorties du module. Cette fonction permet de surveiller l'état des relais ou contacteurs de commande externes à chaque sollicitation.

Ils effectuent à chaque cycle de fonctionnement une série de tests qui permettent de détecter toute défaillance des dispositifs de protection et des circuits associés. C'est ainsi qu'ils détectent :

- tout défaut et court-circuit sur les câblages des organes de commande,
- tout collage d'un contact électrique dans un organe de service,
- la mise en court-circuit d'un contact de bouton d'arrêt d'urgence,
- le grippage d'un bouton d'impulsion de mise en marche,
- un courant de fuite à la terre.

Ils permettent ainsi de surveiller la chaîne d'arrêt/démarrage d'urgence (autocontrôle).

L’association de la redondance et de l’autocontrôle permet d’assurer un niveau de sécurité élevé. Après un premier défaut, l’autocontrôle signale le défaut et incite au dépannage tandis que la redondance permet d’assurer la fonction de sécurité.

Après activation du BAU, les modules logiques de sécurité permettent un réarmement automatique ou manuel par le biais d’un bouton poussoir, dans le cas d’une chaine d’arrêt d’urgence.

Ces blocs ou modules logiques de sécurité font l’objet d’une conformité (et d’une certification) aux normes de sécurité fonctionnelle NF EN ISO 13849-1[5] et NF EN IEC 62061[6]. Leur mise en œuvre nécessite de se conformer aux prescriptions du constructeur, en particulier en ce qui concerne le câblage et les limites d’utilisation.

3.3.3 COMMANDE ET SURVEILLANCE PAR L’INTERMÉDIAIRE D’UN AUTOMATE PROGRAMMABLE DE SÉCURITÉ

Le traitement de l’ordre d’arrêt/démarrage d’urgence et la commande des moyens d’arrêt peuvent être réalisés par un automate programmable de sécurité. Ce type de traitement n’est pas abordé dans le cadre de cette fiche.

4 CRITÈRES D'ÉVALUATION DES PERFORMANCES D'UN BAU EN TANT QUE BARRIÈRE DE SÉCURITÉ

Dans ce paragraphe, sont considérés le couple opérateur et le système d'AU comme éléments d'une barrière de sécurité. Il s'agit d'une barrière mixte (Barrière à Action Manuelle de Sécurité), c'est-à-dire avec une composante humaine et une composante technique. L'application d'une démarche spécifique d'évaluation de la performance de cette barrière est donc requise.

L'analyse de risques permet d'identifier des scénarios d'accidents dans des conditions d'exploitation plus ou moins précises. Lors de l'analyse de risques, pour chacun des scénarios où le BAU aura été identifié comme une barrière de sécurité, la question du champ d'action nécessaire pour que le BAU soit efficace devra se poser. Les éléments présentés dans les paragraphes précédents (la configuration technico-organisationnelle, champ d'action du BAU ou lieu de détection ou d'actionnement) vont être utilisés lors de l'évaluation de la performance de la barrière de sécurité.

4.1 EFFICACITÉ

4.1.1 DÉFINITION

L'efficacité d'une fonction d'arrêt d'urgence est son aptitude à remplir la fonction de sécurité pour laquelle elle a été choisie, dans son contexte d'utilisation et pendant une durée donnée de fonctionnement. Elle est évaluée pour un scénario d'accident précis.

L'évaluation de l'efficacité repose en premier lieu sur les principes de dimensionnement adapté et de résistance aux contraintes spécifiques des éléments constituant la fonction de sécurité Arrêt d'Urgence. D'autres paramètres, comme le positionnement et l'installation peuvent également influencer l'efficacité.

4.1.2 PARAMÈTRES/CRITÈRES D'ÉVALUATION

Sur le plan technique, l'efficacité de la chaine de commande d'un BAU dépendra avant tout du bon dimensionnement des éléments, de leur installation et câblage qui doivent être en conformité avec les prescriptions du fournisseur. En particulier, pour le bloc de contact, la position de repos du contact (NF ou NO) considéré doit correspondre à l'action de sécurité. De plus, il doit permettre d'empêcher un réarmement automatique (redémarrage de l'appareil commandé).

Il faudra également s'assurer que les différents éléments de la chaine de commande d'un BAU résistent aux contraintes spécifiques liées à l'environnement où ils sont installés (humidité, poussière, CEM, vibration, …). En particulier, il faudra veiller à ce que leur Indice de Protection (IP) soit adapté.

Pour le cas du bouton d'AU (en plus de câblage), l'efficacité dépendra également de son positionnement et son accessibilité par les opérateurs.

Sur le plan humain, l'occurrence de l'événement ne doit pas impacter l'intégrité physique ou mentale des opérateurs. Le BAU doit donc se trouver à un endroit suffisamment proche et protégé pour permettre une action rapide et en sécurité pour l'opérateur. De plus, suivant le champ d'action de l'AU et sa configuration, des procédures d'actionnement et de communication doivent être mises en place.

Des informations complémentaires sont fournies ci-après sur des éléments considérés comme importants de la fonction AU.

4.1.3 PARTIE TECHNIQUE

4.1.3.1 RELAIS / CONTACTEUR

Les caractéristiques à considérer pour le bon fonctionnement d'un relais ou d'un contacteur sont les suivantes :

- la tension de sa bobine de commande (5V à 220V),
- le nombre de contacts souhaités,
- le pouvoir de coupure (ou puissance de coupure) des contacts généralement exprimé en Ampère (0,1A à 50A),
- le type de courant de sa bobine, en général du continu,
- la tension d'isolement entre la bobine et les contacts,
- l'environnement (vibrations, humidité, poussières, température).

Le pouvoir (puissance) de coupure est la capacité des contacts à couper un courant maximal sous une tension maximale. S'il n'est pas adapté, le relais ne pourra pas couper le courant (risque d'arcs électriques, problèmes d'isolation, etc…).

La commande de charges fortement selfiques comme les moteurs mais aussi de résistances de puissance (chauffage) demande un pouvoir de coupure particulièrement important et peut générer des arcs électriques (risque de destruction et d'incendie). Le contacteur permet d'assurer la même fonction que le relais mais il possède un pouvoir de coupure plus important grâce des dispositifs d'extinction de l'arc électrique.

De plus, il est important de respecter les préconisations d'installation et de câblage fixées dans la notice d'utilisation. Cette dernière présente le fonctionnement et donne des conseils pour son branchement et son utilisation en fonction du contexte d'utilisation.

4.1.3.2 MODULES LOGIQUES DE SÉCURITÉ

Un module (ou bloc) logique de sécurité a une conception basée sur la combinaison de contacts en redondance et à guidage forcé pour la commutation de sécurité (avec des contacts liés). Il est également équipé d'un circuit de surveillance pour contrôler et surveiller la position des actionneurs, qui sont commandés par les contacts de sécurité. Il a également la capacité de détecter une défaillance dans le circuit d'entrée telle que la "soudure" d'un contact ou sur l'un des contacts de sécurité du relais de sortie (autocontrôles de ses entrées et de ses sorties).

Certains modules logiques de sécurité sont assimilés à un "mini-automate de sécurité". Leur mise en œuvre nécessite de se conformer aux prescriptions du constructeur, en particulier en ce qui concerne le câblage et les limites d'utilisation. Il est donc important de respecter les consignes de câblage préconisées par son fabricant et de tenir compte des spécificités de l'application.

4.1.4 PARTIE HUMAINE

4.1.4.1 PRÉPARATION DES OPÉRATEURS

L'actionnement du bouton d'arrêt d'urgence (avec l'étape de détection de la situation dangereuse) peut être considéré dans certains scénarios d'accident comme la première partie d'une barrière de sécurité. Cette tâche critique doit faire l'objet d'une analyse afin de s'assurer qu'elle est bien réalisable dans la situation de travail de l'opérateur. Les opérateurs doivent être formés et sensibilisés aux risques que présente leur activité, et aux conditions d'activation du BAU (général, local, équipement).

Le port d'EPI adéquats peut être une obligation pour assurer l'intégrité de l'opérateur en charge de déclencher le BAU.

Dans les configurations ou plusieurs opérateurs doivent coopérer (paragraphe 3.1.1.2 et 3.1.1.3) leur disponibilité doit également être entière. De plus, les modalités de communication doivent être précises (communication d'urgence, phraséologie). La communication entre les opérateurs en salle de conduite et sur le terrain nécessite :

- la disponibilité du matériel de communication,
- l'existence d'une procédure de communication opérationnelle laissant aucun doute sur le sens des messages (définition d'une phraséologie spécifique),
- l'exigence d'un collationnement[2] pour l'instruction,
- la confirmation une fois l'action effectuée.

4.1.4.2 ACCESSIBILITÉ

Les choix de conception doivent garantir l'accès facile au BAU : visible, identifiable, accessible (zone dégagée sans risque d'être masquée par du matériel ou un véhicule, et pas d'obstacle).

De plus les informations nécessaires pour décider d'actionner le BAU doivent être fournies aux opérateurs (par exemple lors des formations) et formalisées dans des procédures (par exemple : fiches reflexes) accessibles et lisibles.

Pour les configurations mettant en jeu une centralisation de l'alarme et/ou de l'action de sécurité (comme dans une salle de contrôle déportée par exemple), la série des normes ISO 9241-210[14], 9241-12[15] et 9241-125[16] pour la conception d'interface homme / machine décrivent les exigences ergonomiques pour faciliter la perception (détection) de l'information sur un écran informatique, tels que dans le cas d'une interface d'alarme(s) pour un BAU. Ces trois normes sont présentées en Annexe A.

[2] Collationnement : répétition de l'instruction par l'opérateur recevant pour vérifier sa bonne compréhension

4.2 TEMPS DE RÉPONSE

4.2.1 DÉFINITION

Le temps de réponse correspond à l'intervalle de temps entre le moment où une barrière de sécurité, dans un contexte d'utilisation, est sollicitée et le moment où la fonction assurée par cette barrière de sécurité est réalisée dans son intégralité. Le temps de réponse de la barrière doit être en adéquation avec la cinétique du scénario qu'elle doit maîtriser, c'est-à-dire qu'il doit être inférieur à la cinétique du scénario à traiter.

Le temps de réponse intègre :

- le temps nécessaire à la détection,
- le temps nécessaire à la transmission et au traitement de l'information jusqu'aux éléments devant remplir l'action de sécurité,
- le temps nécessaire à la réalisation de l'action de sécurité.

Pour la fonction traitée dans ce document (actionnement d'un Bouton d'Arrêt d'Urgence) et la commande associée, le temps de réponse intègre :

- le temps nécessaire à la détection de la situation à risque par l'opérateur (partie humaine),
- le temps nécessaire pour appuyer sur le BAU (partie humaine),
- le temps d'activation des éléments de commande (partie technique).

4.2.2 TEMPS DE RÉPONSE DE LA PARTIE TECHNIQUE

Le temps de réponse des éléments d'une boucle d'arrêt d'urgence est lié à leur temps de commutation et est de l'ordre de la dizaine de millisecondes.

Par exemple :

- 10 ms pour un relais,
- 30 ms pour un contacteur,
- 20 à 40 ms pour un modules logiques de sécurité.

Dans le cas où une temporisation est ajoutée à ces éléments, il faudra ajouter celle-ci au temps de commutation.

Par ailleurs, dans le cas où la détection est reportée sur un pupitre d'opérateur, le temps de traitement de la chaine de détection (du détecteur jusqu'au déclenchement de l'alarme) est à prendre en compte.

4.2.3 TEMPS DE RÉPONSE DE LA PARTIE HUMAINE

Le temps de réponse correspondra au temps d'activation par un opérateur et sera notamment dépendant des conditions de détection et de prise de décision d'enclenchement.

La rapidité de la détection dépendra des moyens développés en termes d'alarmes visuelle (ergonomie) et sonore (distinguable et plus fort que le bruit ambiant). Il est indispensable que l'alarme soit différenciée par rapport à toutes les autres alarmes via une visualisation et un son spécifiques.

Le temps de décision dépendra :

- d'une part, de la complexité de la situation,
- et d'autre part, de la formation et de l'entrainement de l'opérateur sur les modalités d'actionnement du BAU et de la connaissance des conséquences de l'actionnement (machine, local, général).

En cas de détection de circonstance appelant à actionner le BAU, l'opérateur doit pouvoir actionner le bouton rapidement. La localisation, les conditions d'accès (avec une attention particulière à la coactivité pouvant générer de l'encombrement ou du masquage) et les conditions de la situation (incendie, fuite…), doivent permettre une activation rapide. Les opérateurs peuvent ne pas intervenir dans des zones qui ne garantissent pas un accès au BAU rapide et/ou sécurisé.

Il conviendra de s'interroger sur les risques d'hésitation de l'opérateur entre l'activation du BAU et une solution alternative qui peut apparaitre comme moins impactante (notamment pour un BAU général ou unité, cf. paragraphe 3.1.2). Ce dilemme peut faire perdre du temps. Il est donc nécessaire que les opérateurs disposent d'instructions ou de procédures claires (§ 3.1.2.4) et qu'ils soient formés et entrainés (test, essais, exercices périodiques).

4.3 NIVEAU DE CONFIANCE

4.3.1 NC PARTIE TECHNIQUE

En règle générale, les éléments techniques d'une boucle d'arrêt d'urgence rencontrés sur le marché sont certifiés suivant les normes de sécurité fonctionnelle NF EN IEC 61508[17], NF EN ISO 13849-1[5] et NF EN IEC 62061[6]. Ces normes classent les parties de système de commande relatives à la sécurité en niveaux, de 1 à 4, 4 étant la plus élevée. Le niveau de confiance qu'on leur accordera sera équivalent à leur niveau de sécurité si les exigences d'efficacité (en particulier dimensionnement et installation) et de temps de réponse sont remplies et s'ils font l'objet d'une politique de tests et de maintenance adaptée.

En revanche, lorsque qu'ils ne sont pas certifiés selon ces normes, une évaluation conformément au référentiel Oméga 10[1] permettra de préciser le NC. Si les exigences d'efficacité et de temps de réponse sont remplies et s'ils font l'objet d'une politique de tests et de maintenance adaptée, un NC minimal de 1 peut être retenu.

4.3.2 NIVEAU DE CONFIANCE DE LA PARTIE HUMAINE

Trois éléments de la tâche sont à prendre en compte pour évaluer le niveau de confiance d'une barrière humaine de sécurité (cf. Omega 20[2]) :

- La détection (possibilité de percevoir le signal, l'information qu'il se passe quelque chose de grave),
- Le diagnostic (compréhension de la situation),

- L’action (localisation, accessibilité physique du BAU).

Grace à ces trois éléments, un BAU en tant que Barrière de Sécurité et en application de l’Omega 20[2], va pouvoir se voir attribuer un niveau de confiance (NC) de 2, 1 ou 0.

L’évaluation du NC nécessitant de se référer à la situation réelle de travail, il est impossible de le fixer a priori. Ce calcul peut être fait en se référant à l’Oméga 20 (Evaluation des barrières humaines de sécurité). Il est toutefois possible de donner quelques éléments d’appréciation générale pour faciliter cette analyse.

4.3.2.1 CONDITION D’OBTENTION DU NC2

Un Niveau de Confiance de 2 pourrait être attribué si les conditions suivantes sont vérifiées pour chacune des trois parties de la tâche.

1. **Partie Détection :**

Détection active (recherche volontaire de l’information) avec identification simple et directe du problème, et disponibilité entière de l’opérateur. La tâche est planifiée en cohérence avec le reste des tâches, et l’opérateur connait l’importance de cette tâche (formation).

Détection passive (l’opérateur est en charge d’autres tâches que la détection de cette alarme) : Information disponible de façon hiérarchisée (par exemple : alarme dédiée visuelle et sonore clairement distincte des autres types d’alarmes) donnant l'état du système, quelles que soient les conditions environnementales (nuit, brouillard, …) qui seraient susceptibles d’empêcher ou de gêner la perception de ces informations. L’opérateur est présent à l’endroit où l’information est présente, et ses autres activités peuvent être interrompues à tout moment.

2. **Partie Diagnostic :**

Ce diagnostic va dépendre de la facilité d’interprétation du phénomène détecté et de facilitation de la décision à prendre (clarté et simplicité des choix d’actions, comme par exemple n’avoir qu’une 1 seule option BAU possible en fonction de la nature du problème détecté). En cas d’existence de plusieurs BAU avec des champs d’actions différents, le choix d’activation du BAU approprié est sans équivoque (importance de l’existence d’une formation avec mise en situation). C’est à ce niveau que le dilemme entre sécurité et production peut influencer le niveau de confiance. Il faut donc avoir préalablement pensé les interfaces et les procédures pour faciliter (bien guider) le diagnostic.

3. **Partie Action :**

L’accessibilité et la proximité permettent un temps d’intervention rapide vis-à-vis de la cinétique de l’événement à récupérer, avec une action simple (sans enchainement complexe).

Dans les configurations présentées aux paragraphes 3.1.1.2 et 3.1.1.3, ce type d’arrêt permet de minimiser les risques d’une décision isolée. La décision fait l’objet d’une discussion entre l’opérateur sur le terrain et celui de la salle de commande.

Ainsi la pertinence d'un arrêt général est discutée et la responsabilité peut être partagée. Toutefois, ici encore, une procédure non équivoque, des informations claires et précises, et des entrainements sont requis, afin de limiter la pression de production.

4.3.2.2 CONDITIONS DE DÉCOTE POUR TOMBER À NC1 OU NC0

Pour chacune des trois parties de la tâche, les éléments de décote qui pourraient faire tomber le Niveau de Confiance à 1 voire 0 sont les suivantes.

1. Partie Détection :

Détection active : ce critère pourra faire l'objet d'une décote de 1 ou 2 points, selon les difficultés d'obtention de l'information (efforts intellectuels ou physique demandés : ronde, levée de doute, ergonomie des IHM,), les conditions d'accès à l'information, selon les marges de manœuvre laissées à l'opérateur pour réaliser cette tâche, et selon le contenu de la formation suivie par l'opérateur pour le sensibiliser à l'importance de cette tâche dans la maitrise des risques.

Détection passive : ce critère pourra faire l'objet d'une décote de 1 à 2 points selon la qualité de présentation de l'information (sa saillance parmi les autres données à utiliser dans le travail), et selon la fréquence et la disponibilité de l'opérateur sur le lieu où se trouve l'information.

2. Partie Diagnostic / Décision :

Diagnostic : ce critère pourra faire l'objet d'une décote de 1 ou 2 points, si l'interprétation du phénomène observé peut demander du temps ou si plusieurs options d'actions sont possibles et donc demande une analyse du problème qui peut reporter de manière critique la décision d'activer le BAU.

Dans les configurations présentées aux paragraphes 3.1.1.1 et 3.1.1.4, dans lesquelles l'opérateur peut être seul à prendre la décision (soit en salle de commande soit sur le terrain), le risque pour un arrêt général est de ne jamais être utilisé. En effet, un opérateur peut avoir des difficultés à prendre la responsabilité d'arrêter toute une installation (et ce, même si une procédure l'y autorise), et pourrait privilégier d'autres solutions moins radicales.

La prise de décision dépendra bien sûr du contexte qui peut amener à une décote du NC de 1 voire de 2 :

- Type d'installation (process, dépotage, …),
- Type de process (continu ou batch),
- Des conséquences d'un arrêt sur la sécurité des personnes et des biens et sur l'environnement,
- Du coût d'exploitation,
- De la difficulté de remise en service,
- Les caractéristiques de l'opérateur (ancienneté, l'expérience, rapport aux risques…),
- Les caractéristiques de l'organisation (formation, type management, contexte des travail…),
- Etc…

Pour éviter ce dilemme entre sécurité et production, et limiter la décote, il faut aider la prise de décision avec une procédure non équivoque, des informations claires et précises sur l'état du système (hiérarchisation des alarmes par exemple), et des entrainements avec mise en situation.

3. Partie Action :

Action : ce critère pourra faire l'objet d'une décote de 1 point, si le BAU n'est pas facilement accessible (distance importante par rapport au lieu de détection sans possibilité fiable de communication à un opérateur plus proche, salle indépendante, risque d'obstacle par du matériel, ...).

5 TESTS ET MAINTENANCE

5.1 GÉNÉRALITÉS

Les dispositifs de sécurité doivent faire l'objet d'une politique de test et de maintenance. La définition de cette politique de maintenance peut reposer sur :

1. Des exigences normatives et règlementaires,
2. Des standards internes,
3. Des exigences du fournisseur,
4. Un retour d'expérience interne ou externe.

Tous les éléments d'une barrière de sécurité ne demandent pas les mêmes opérations de test et de maintenance ni la même fréquence et doivent être adaptées à la configuration du site industriel. Dans tous les cas, il est nécessaire de contrôler l'ensemble des éléments constituant la chaine de sécurité.

Il est important d'avoir une gestion adaptée pour maintenir la performance dans le temps des différents éléments constituants la fonction d'arrêt d'urgence. Cette gestion (via par exemple une GMAO, SGS, SMS[3], etc.) doit prendre en compte les aspects suivants :

- le test des procédures par les opérateurs,
- des ressources techniques (moyens et outils adaptés et étalonnés),
- la gestion des compétences des opérateurs (entrainement aux situations d'urgence),
- des pièces de rechanges disponibles,
- la traçabilité (enregistrement des preuves) des vérifications et des tests réalisés,
- l'enregistrement des résultats : les défaillances doivent être enregistrées et analysées pour améliorer la fonction de sécurité (optimisation de la fréquence des tests, définition de la fiabilité, …),
- la gestion des modifications (réalisation d'une analyse d'impact, circuit d'autorisation, mise en place d'un moyen compensatoire, …),
- des vérifications ou évaluations du système de gestion.

Les opérations de test et de maintenance doivent être réalisées en respectant le ou les modes opératoires spécifiques prévus par le constructeur. Ces opérations nécessitent une structure minimale dans laquelle les personnels intervenants, tant internes qu'externes, doivent disposer des compétences nécessaires.

---

[3] GMAO : Gestion de la Maintenance Assistée par Ordinateur.

Système de gestion de la Sécurité : ensemble de moyens (support, processus) permettant de s'assurer que les exigences identifiées dans l'analyse de risque sont suivies et maitrisées. Obligation réglementaire pour les ICPE SEVESO Seuil Haut.

SMS : Système de Management de la Sécurité.

5.2 POINTS SPÉCIFIQUES AUX ÉLÉMENTS TECHNIQUES

Les principaux types de défaillance des éléments de commutation, type relais ou contacteurs, sont les suivants :

- Une résistance de contact trop élevée due généralement soit à un mauvais alignement, soit à la contamination des contacts (trace de résine silicone par exemple), soit à la perte de résilience des ressorts ou à la présence de particules isolantes à l'intérieur du boîtier.
- Une usure prématurée des contacts due aux forts courants ou aux arcs créés à l'ouverture ou à la fermeture d'un circuit. De forts courants d'appel peuvent se produire à la commutation de charge telle que moteurs, lampes, filtres avec entrée capacitive, etc... et des surtensions importantes peuvent se produire à la coupure de circuits comportant des inductances.
- Une variation des seuils d'enclenchement et de déclenchement due soit au déplacement du moteur (suite à des chocs mécaniques), soit à l'usure des pièces mécaniques ou à l'érosion des contacts.
- Un arrêt fonctionnel dû à une rupture du fil de la bobine, à une rupture de pièces mécaniques ou d'un assemblage ou à la présence d'une particule coinçant le mécanisme.
- Etc...

De plus, les éléments de commutations ont une durée de vie liée au nombre de manœuvres (par exemple : 50 000 pour un BAU, 2 000 000 pour un contacteur, …).

Les éléments techniques avec diagnostics embarqués permettent de détecter un certain nombre de défaillances : alimentation, communication, électronique, … Généralement, certains diagnostics sont exécutés automatiquement à la mise en marche et d'autres suivant une périodicité fixée dans l'équipement (voir fiche technique de l'équipement). Ces séquences de diagnostics ne dispensent pas d'effectuer les vérifications régulières.

Il est donc nécessaire de tester périodiquement la boucle d'AU pour s'assurer de son bon fonctionnement global. En général un test annuel de la fonction AU est préconisé.

Ces opérations de maintenance et de tests périodiques doivent inclure :

- un contrôle visuel de l'état des différents éléments,
- la vérification du câblage et des connectiques,
- le test des circuits électriques,
- la vérification du bon fonctionnement par activation du BAU,
- Etc…

5.3 POINTS SPÉCIFIQUES SUR LES ASPECTS HUMAINS ET ORGANISATIONNELS

Les 4 configurations technico-organisationnelle décrites au paragraphe 3.1 impliquent différents contextes de mise en place d'un BAU, et suggèrent une analyse des exigences qui en découlent. En effet, pour s'assurer que la barrière de sécurité « BAU » est opérationnelle et que sa performance est maintenue dans le temps, un certain nombre de tâches vont devoir être accomplies.

Ces tâches vont dépendre de certains choix techniques (nature de l'équipement choisi, sa fiabilité) et organisationnels (ressources disponibles, sous-traitance, planification de la maintenance, habilitation, formation, entrainement…). Sur les ICPE (Installation Classée pour la Protection de l'Environnement), la bonne réalisation de ces tâches est garantie par la mise en place d'un système de gestion de la sécurité[4] (SGS).

Pour ce qui concerne la formation et l'entrainement à détecter, diagnostiquer et décider de l'actionnement ou non du BAU selon les situations opérationnelles, des sessions annuelles avec mises en situation des opérateurs sont recommandées, notamment en s'appuyant sur le retour d'expérience.

Au regard des considérations exposées dans les chapitres précédents, il est important de réduire les risques de dilemmes production/sécurité au moment de l'actionnement des BAU par l'opérateur. Ainsi, des tests et entrainements réguliers, s'appuyant sur le retour d'expérience, sont à réaliser en vue de vérifier que :

- les protocoles et moyens de communications nécessaires à la décision de déclenchement d'un BAU sont connus et applicables,
- les personnels en charge du déclenchement d'un BAU sont familiarisés à son usage potentiel,
- d'éventuelles modifications d'organisation du travail ou de procédé n'impactent pas cette barrière humaine.

[4] Exigible uniquement pour les installations SEVESO Seuil Haut

6 RÉFÉRENCES

1. Oméga 10, DRA-17-164432-10199B - Evaluation de la performance des Barrières Techniques de Sécurité
2. Oméga 20, DRA-09-103041-06026B - Démarche d'évaluation des Barrières Humaines de Sécurité
3. Directive Machines 2006/42/CE, DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL, du 17 mai 2006, relative aux machines et modifiant la directive 95/16/CE
4. NF EN ISO 13850 Décembre 2015 - Sécurité des machines - Fonction d'arrêt d'urgence - Principes de conception
5. NF EN ISO 13849-1 Mars 2016 - Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1 : principes généraux de conception
6. NF EN IEC 62061 Juillet 2005 - Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité
7. NF EN 60947-5-5/A2 Avril 2017 - Appareillage à basse tension - Partie 5-5 : appareils et éléments de commutation pour circuits de commande - Appareil d'arrêt d'urgence électrique à accrochage mécanique
8. NF EN 60947-4-1, Août 2010 - Appareillage à basse tension - Partie 4-1 : contacteurs et démarreurs de moteurs - Contacteurs et démarreurs électromécaniques
9. IEC 60204-1, Octobre 2016 - Sécurité des machines - Équipement électrique des machines - Partie 1 : Exigences générales
10. NF EN ISO 12100, Décembre 2010 - Sécurité des machines - Principes généraux de conception - Appréciation du risque et réduction du risque
11. NF EN 61511-1, Mars 2005 - Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le secteur des industries de transformation - Partie 1 : cadre, définitions, exigences pour le système, le matériel et le logiciel
12. IEC 62682, Octobre 2014, Gestion de systèmes d'alarme dans les industries de transformation
13. IEC 62603-1, Mai 2014 - Industrial process control systems - Guideline for evaluating process control systems - Part 1 : specifications
14. ISO 9241-210, mars 2010 - Ergonomie de l'interaction homme-système - Partie 210 : conception centrée sur l'opérateur humain pour les systèmes interactifs
15. ISO 9241-12, 1998 – Exigences ergonomiques pour travail de bureau avec terminaux à écrans de visualisation (TEV) -- Partie 12 : Présentation de l'information (révisée et remplacée par la norme ISO 9241-125 : 2017)
16. ISO 9241-125, 2017 - Ergonomie de l'interaction homme-système - Partie 125 : Recommandations relatives à la présentation visuelle d'informations
17. NF EN IEC 61508, 2010 - Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité
18. Directive Basse Tension 2014/35/UE[18], DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL, du 26 février 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché du matériel électrique destiné à être employé dans certaines limites de tension

7 LISTE DES ANNEXES

Repère	Désignation	Nombre de pages
Annexe A	Réglementation ou textes normatifs applicables	5

Annexe A

Réglementation ou textes normatifs applicables

Les arrêts d'urgence sont réglementés en Europe par la directive Machines 2006/42/CE[3] et, entre autres, des normes harmonisées NF EN ISO 13850[4], ISO EN 13849-1/2[5], IEC 62061[6] et NF EN 60947-5-5/A2[7].

Dans son paragraphe "1.2.4.3. Arrêt d'urgence", la directive Machines 2006/42/CE[3] fixe, entre autres, les exigences suivantes :

« La machine doit être munie d'un ou de plusieurs dispositifs d'arrêt d'urgence permettant d'éviter des situations dangereuses qui sont en train de se produire ou qui sont imminentes.

Le dispositif doit :

- *comprendre des organes de service clairement identifiables, bien visibles et rapidement accessibles,*
- *provoquer l'arrêt du processus dangereux aussi rapidement que possible, sans créer de risque supplémentaire,*
- *au besoin, déclencher ou permettre de déclencher certains mouvements de protection.*

Lorsqu'on cesse d'actionner le dispositif d'arrêt d'urgence après avoir donné un ordre d'arrêt, cet ordre doit être maintenu par un enclenchement du dispositif d'arrêt d'urgence jusqu'à ce que celui-ci soit expressément désactivé ; il ne doit pas être possible d'enclencher le dispositif sans actionner une commande d'arrêt ; la désactivation du dispositif ne doit pouvoir être obtenue que par une action appropriée et elle ne doit pas avoir pour effet de remettre la machine en marche mais seulement d'autoriser un redémarrage.

La fonction d'arrêt d'urgence doit être disponible et opérationnelle à tout moment, quel que soit le mode opératoire.

Les dispositifs d'arrêt d'urgence doivent venir à l'appui d'autres mesures de sauvegarde et non les remplacer. »

Ces exigences de la directive Machine pourraient être appliquées aux BAU équipant les installations industrielles sous certaines conditions[5].

Les normes internationales NF EN ISO 13850[4], IEC 60204-1 [9] et NF EN 60947-5-5/A2[7] spécifient les exigences fonctionnelles et les principes de conception :

- de la fonction d'arrêt d'urgence, indépendamment du type d'énergie utilisé,
- des appareils et éléments de commutation pour circuit de commande électrique (appareil d'arrêt d'urgence électrique à accrochage mécanique) utilisés afin de fournir un signal d'arrêt d'urgence.

Selon ces normes, la fonction d'arrêt d'urgence :

- est destinée à parer à des risques (séquences accidentelles et/ou phénomènes dangereux) en train d'apparaître, ou à atténuer des risques existants, pouvant porter atteinte à des personnes, à la machine ou au travail en cours,
- et est déclenchée par une action humaine unique quand la fonction d'arrêt normal ne convient pas.

Pour ces 2 normes, les risques peuvent être liés au fonctionnement normal de la machine ou à ses dysfonctionnements (pannes, dérives,...).

Ces normes précisent qu'un appareil d'arrêt d'urgence (boutons poussoirs de type champignon) est un organe de service manœuvrable manuellement et utilisé pour déclencher une fonction d'arrêt d'urgence. Il doit être conçu pour être actionné facilement par l'opérateur et les autres personnes qui ont besoin de le manœuvrer.

Ces normes fixent les exigences de sécurité suivantes :

- la fonction d'Arrêt d'urgence doit être disponible et à même de fonctionner à tout instant,
- l'Arrêt d'urgence doit fonctionner suivant le principe de l'action positive (défini dans la norme EN ISO 12100[10]),
- l'Arrêt d'urgence peut être de (Cf. IEC 60204-1 [9]) :
    - Catégorie 0 correspondant à une suppression immédiate de la puissance (arrêt non contrôlé),
    - Catégorie 1 correspondant à un arrêt contrôlé en maintenant la puissance sur les actionneurs jusqu'à l'arrêt, suivi de la coupure de la puissance quand l'arrêt est obtenu,
    - Catégorie 2 correspondant à un arrêt contrôlé par le maintien des actionneurs alimentés même après l'arrêt.

Le choix de la catégorie d'arrêt pour les fonctions d'arrêts d'urgence est basé sur une analyse du risque. La norme ISO 13850[6] concernant la fonction d'arrêt d'urgence exige que seulement une catégorie d'arrêt 0 ou 1 puisse être utilisée (catégorie 2 exclue) dans le cas d'un arrêt d'une machine dangereuse pour la protection des travailleurs.

La norme EN ISO 12100[10] est une norme fondamentale de sécurité pour la Directive Machines. Elle spécifie la terminologie de base, la représentation schématique d'une machine ainsi que les principes d'évaluation et de réduction du risque dans la conception des machines. Elle propose des méthodologies pour :

- identifier les phénomènes dangereux et évaluer les risques pour toutes les étapes du cycle de vie des machines,
- supprimer les phénomènes dangereux ou réduire les risques.

La norme IEC 60204-1[9] s'applique aux équipements et systèmes électriques, électroniques et électroniques programmables des machines et entre dans le champ d'application de la Directive Basse Tension 2014/35/UE[18] et de la Directive Machines Directive 2006/42/CE[3]. Elle définit les trois catégories d'arrêt d'urgence et également les codes des couleurs à uniformiser pour les boutons et voyants, les repères de câblage.

Un système d'arrêt d'urgence provoque, après actionnement du BAU, une mise en sécurité via un circuit de commande qui permet de traiter l'ordre d'arrêt d'urgence et de commander les moyens d'arrêt.

---

[5] Durée de l'arrêt de mouvement dangereux sur machine classique de l'ordre de 100 ms, fonctionnement de sécurité en De-Energized to Trip (DETT) c'est-à-dire mise en sécurité de la machine et arrêt du mouvement dangereux en cas de perte d'énergie selon les principes de sécurité définis dans la norme EN 12100, …

Les éléments du circuit de commande des fonctions de sécurité (relais, modules logiques de sécurité, etc.) et les moyens d'arrêts (relais, distributeurs électropneumatiques, etc.) font l'objet d'une conformité aux exigences des normes de sécurité fonctionnelle telles que NF EN IEC 61508[17], NF EN ISO 13849-1[4] et NF EN IEC 62061[5].

La norme NF EN IEC 61508 traite des aspects à prendre en considération lors de l'utilisation de systèmes électriques / électroniques / électroniques programmables (E/E/PES) pour exécuter des fonctions de sécurité. Elle fournit une méthode de développement pour réaliser la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité et fixe des exigences pour leur conception en fonction du niveau d'intégrité de sécurité.

La norme NF EN ISO 13849-1 fournit des exigences de sécurité et des conseils relatifs à la conception et à l'intégration des systèmes de commande relatifs à la sécurité des machines, indépendamment du type de technologie et d'énergie utilisée (électrique, électronique programmable, hydraulique, pneumatique mécanique, etc.). Elle spécifie le niveau de performance requis pour réaliser ces fonctions de sécurité.

La norme NF EN IEC 62061 spécifie les exigences et donne des recommandations pour la conception, l'intégration et la validation des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité pour les machines. Elle s'applique aux systèmes de commande utilisés, séparément ou en combinaison, pour assurer des fonctions de commande relatives à la sécurité de machines.

Les contacteurs font l'objet d'une conformité aux exigences de la norme NF EN IEC 60947-4-1[8]. Cette norme fixe, pour les contacteurs ainsi que les dispositifs de protection contre les surcharges et/ou contre les courts-circuits associés, les exigences pour leurs caractéristiques, leur fonctionnement et à leur tenue, leur construction…, et les essais destinés à vérifier si ces conditions sont réalisées.

Dans l'industrie de transformation, l'AU ultime n'est pas considéré comme une Fonction Instrumentée de Sécurité au sens de la norme NF EN IEC 61511[11] mais comme une prescription de construction du Système Instrumentée de Sécurité. Cette norme demande de mettre à disposition un moyen ultime pour actionner les éléments terminaux du SIS, indépendamment de la logique de traitement de l'automate de sécurité (sauf si indications contraires données par les spécifications des exigences de sécurité). En effet, elle prescrit de rajouter un moyen de commande supplémentaire des actionneurs de sécurité pour palier au risque de défaillances de modes communs à probabilités très faibles (automate en mode stop mais sorties actives, mauvais programme dans l'automate, etc.) et au risque de causes communes de défaillance (incendie, etc.). Ainsi, dans le monde du process industriel, les Arrêts d'Urgence unité et ou machine sont commandés par le SIS et les Arrêts ultimes sont commandés par du relayage (via des modules logiques de sécurité) agissant directement sur les alimentations (coupant les alimentations sur toutes les électrovannes ou autre).

L'actionnement du BAU par un opérateur est lié à deux situations :

1. L'opérateur constate une situation anormale et décide d'appuyer sur le BAU ;
2. Une alarme (sonore ou visuelle) se déclenche et l'opérateur doit appuyer sur le BAU.

Pour l'actionnement du BAU suite une alarme, les normes IEC 62682[12] et IEC 62603-1[13] peuvent être citées, entre autres référentiels, pour les aspects gestion des alarmes dans les process industriels.

La norme IEC 62682 spécifie les exigences pour la gestion des systèmes d'alarme dans les industries de transformation, à travers leur cycle de vie. Elle couvre toutes les alarmes présentées à l'opérateur, qui incluent les systèmes de commande de processus de base, les panneaux d'annonce, les systèmes instrumentés de sécurité, les systèmes incendie et gaz ainsi que les systèmes d'intervention en cas d'urgence.

Elle est un guide pour la définition et la structure d'une philosophie d'alarme appropriée. A titre d'exemple, elle impose d'identifier pour chaque alarme :

- la cause probable de l'alarme,
- l'action opérateur recommandée,
- la conséquence de l'absence d'action ou d'une action incorrecte.

La norme IEC 62603-1 constitue des recommandations pour l'élaboration des spécifications techniques d'un système de contrôle industriel. Le paragraphe 4.7.8 de cette norme traite de la gestion des alarmes. Elle fixe :

- des recommandations pour la définition du type d'alarmes, leur niveau de gravite et niveau de priorité,
- des règles pour le regroupement et l'acquittement des alarmes,
- des exigences pour la formalisation des alarmes, leur affichage dans l'interface homme-machine (IHM) et leur archivage.

Pour la conception d'interface humain / machine, plusieurs normes décrivent les exigences ergonomiques pour faciliter la perception (détection) de l'information sur un écran informatique. Voici quelques exemples pertinents dans le cas d'une interface d'alarme(s) pour un BAU :

- La norme ISO 9241-210[14] fournit des exigences et des recommandations relatives aux principes et aux activités de conception centrée sur l'opérateur humain, intervenant tout au long du cycle de vie des systèmes informatiques interactifs, comme par exemple une alarme ou un ensemble d'alarme sur un écran informatique. Cette norme est destinée à être utilisée par les responsables de la gestion des processus de conception, et traite des manières dont les composants matériels et les logiciels des systèmes interactifs permettent d'améliorer l'interaction homme-système.

- La norme ISO 9241-12[15] fournit des recommandations ergonomiques relatives à la présentation et aux propriétés particulières de l'information présentée sur des interfaces utilisateur. Les recommandations fournies visent à permettre à l'utilisateur d'exécuter des tâches de perception de manière efficace et satisfaisante. On y aborde donc l'organisation de l'information (emplacement de l'information, adéquation des fenêtres, zones d'information, zones d'entrée/sortie, groupes d'informations, listes, tableaux, labels, champs, etc.), les objets graphiques (curseurs et pointeurs, etc.), et les techniques de codage de l'information (codage alphanumérique, abréviations des codes alphanumériques, codage graphique, codage par couleur, marqueurs, etc.).

- La norme ISO 9241-125[16] est un guide pour la présentation visuelle d'informations sous le contrôle d'un logiciel, indépendamment du support. Il inclut des propriétés spécifiques telles que les aspects syntaxiques ou sémantiques des informations, par exemple les techniques de codage, et fournit des dispositions relatives à l'organisation des informations en tenant compte des capacités humaines de perception et de mémorisation. Ne sont pas concernés les détails spécifiques des tableaux, des graphiques ou ceux de la visualisation des informations.

INERIS

maîtriser le risque
pour un développement durable

Institut national de l'environnement industriel et des risques

Parc Technologique Alata
BP 2 - 60550 Verneuil-en-Halatte

Tél. : +33 (0)3 44 55 66 77 - Fax : +33 (0)3 44 55 66 99

E-mail : ineris@ineris.fr - **Internet :** http://www.ineris.fr