AN003657

ANNEXE A

Travailleur accidenté

ACCIDENTÉ

Nom, prénom	**:**	[redacted]
Sexe	:	Masculin
Âge	:	42 ans
Fonction habituelle	:	Opérateur du broyeur à bois
Fonction lors de l'accident	:	Opérateur du broyeur à bois
Expérience dans cette fonction	:	21 mois
Ancienneté chez l'employeur	:	21 mois
Syndicat	:	Non
Numéro d'indemnisation	:	[redacted]

ANNEXE B

Schéma

Schéma

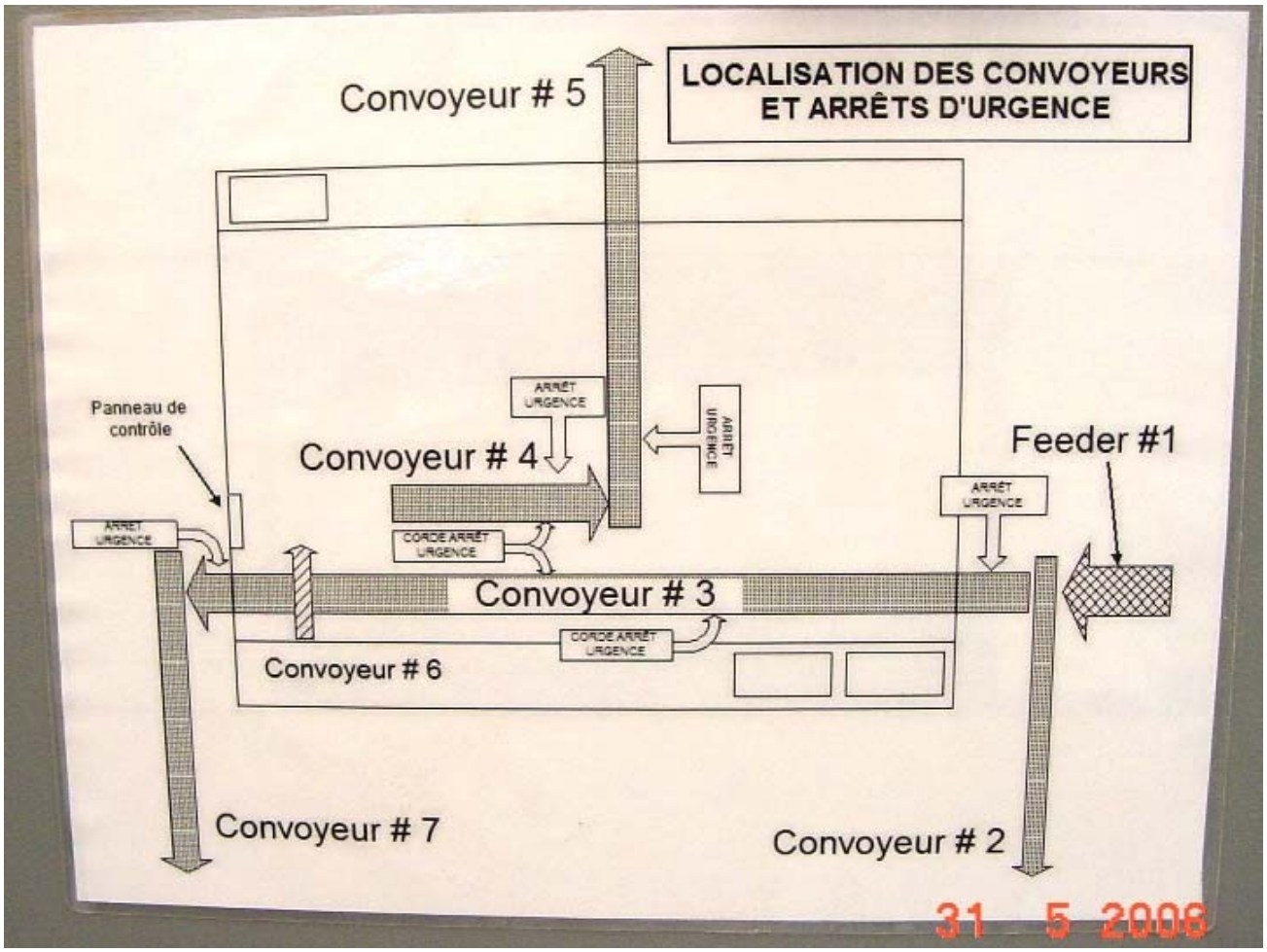


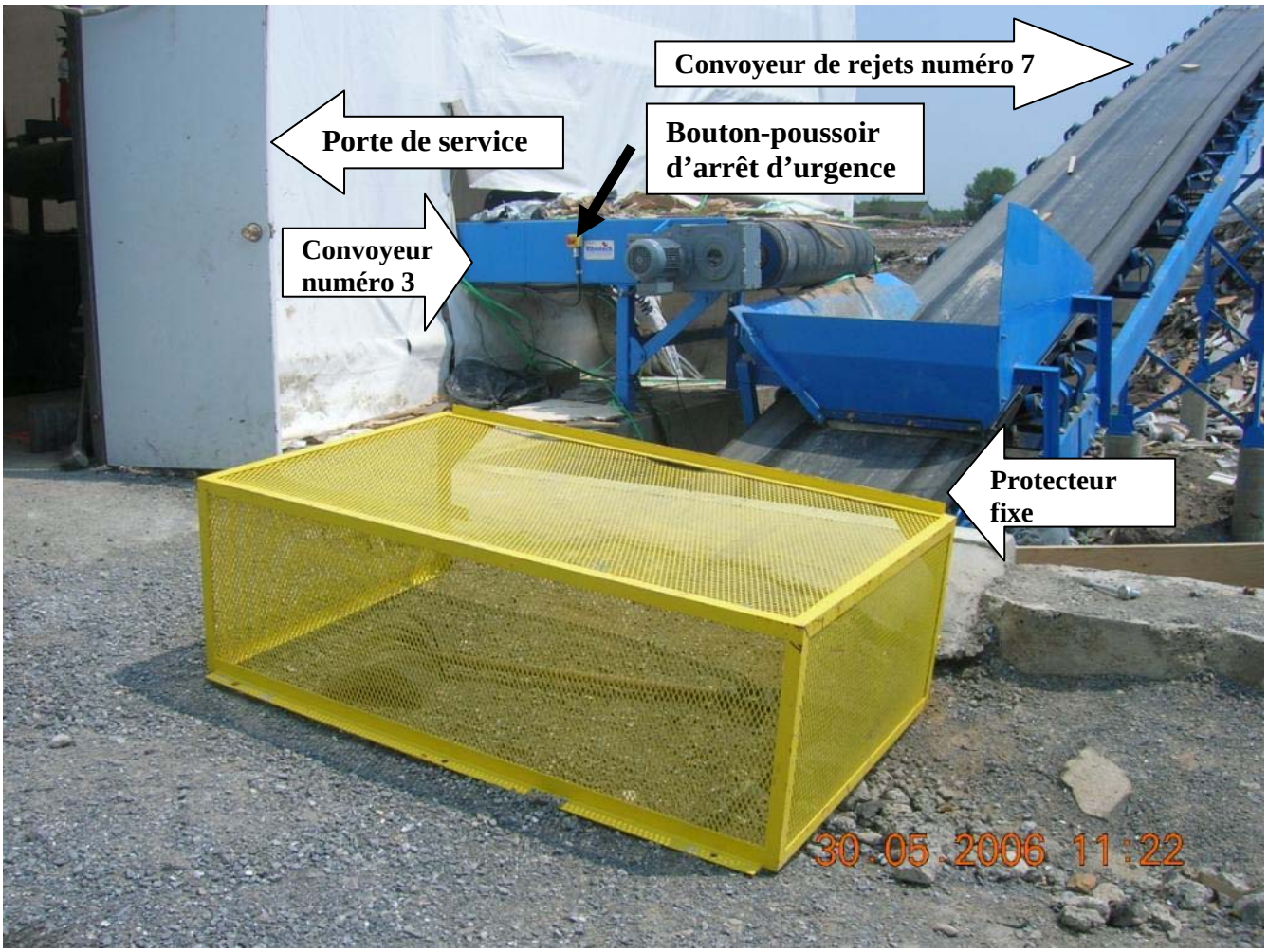
Schéma illustrant la localisation des convoyeurs du centre de tri et des dispositifs d'arrêt d'urgence. Ce schéma est affiché sur le panneau électrique principal

(Source : *AD-Tech Électrique inc.*, photo prise par la CSST)

ANNEXE C

Photos

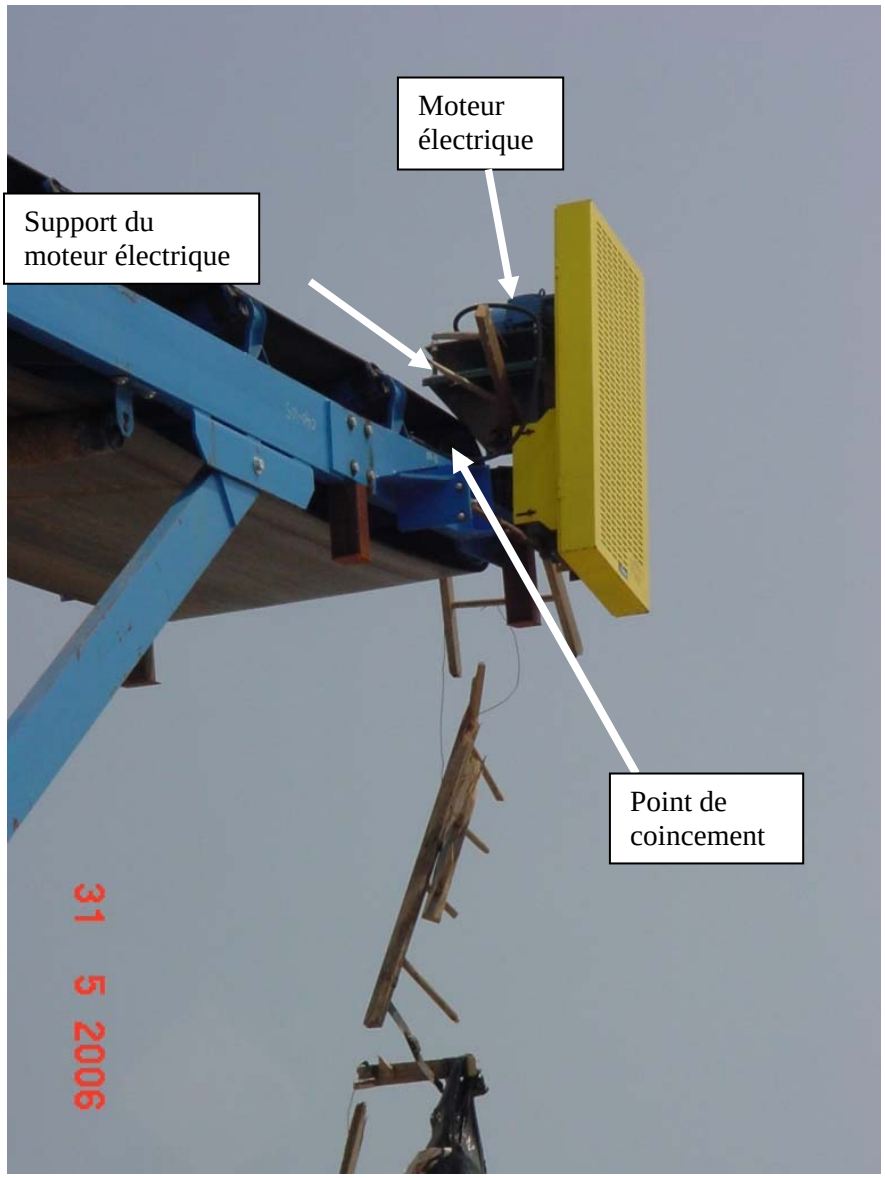
Photo 1



Lieu de l'accident

(Source : CSST)

Photo 2



Position du moteur et du système de transmission du convoyeur 7

(Source : CSST)

Photo 3

Position des employés lors de l'accident

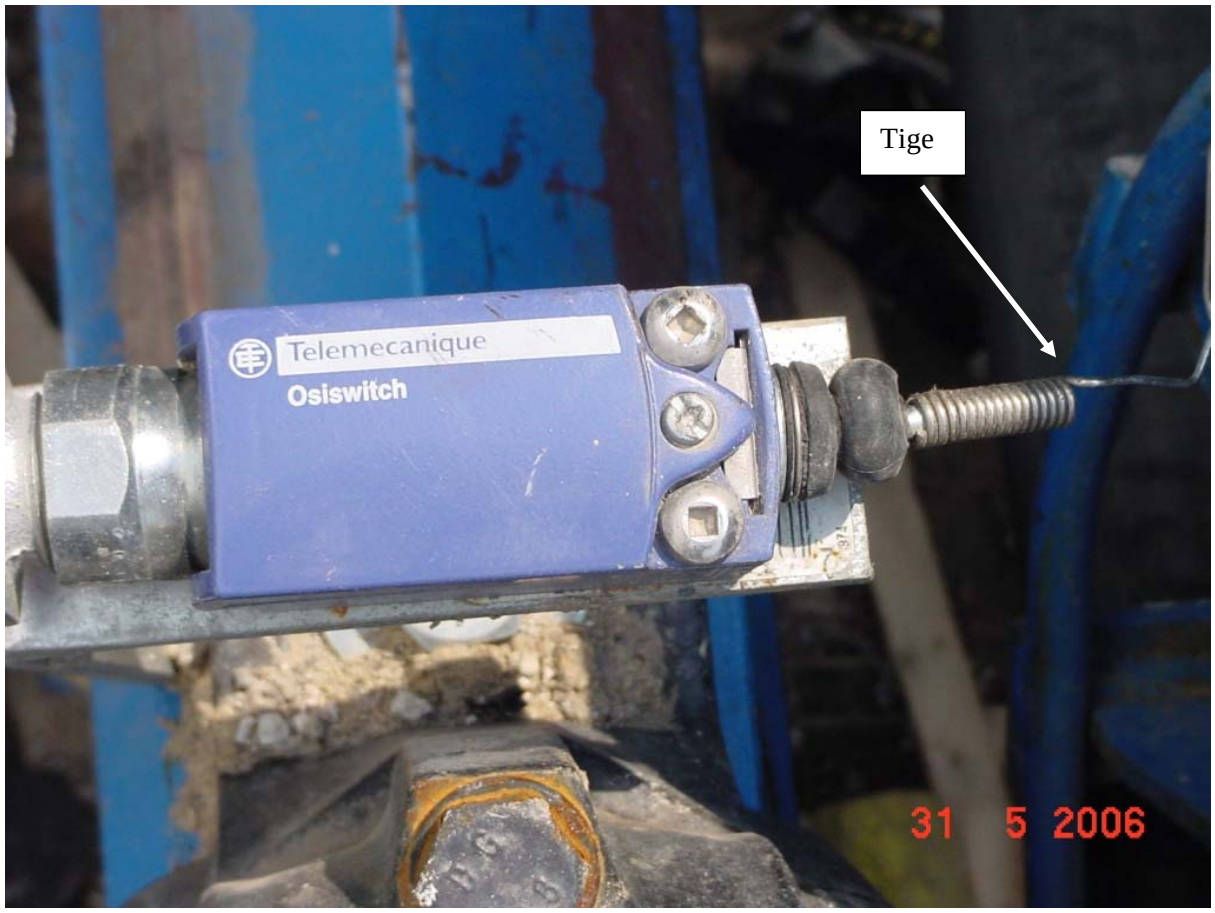
(Source : CSST)

Photo 4

Boulon soudé sur le tambour de queue

(Source : CSST)

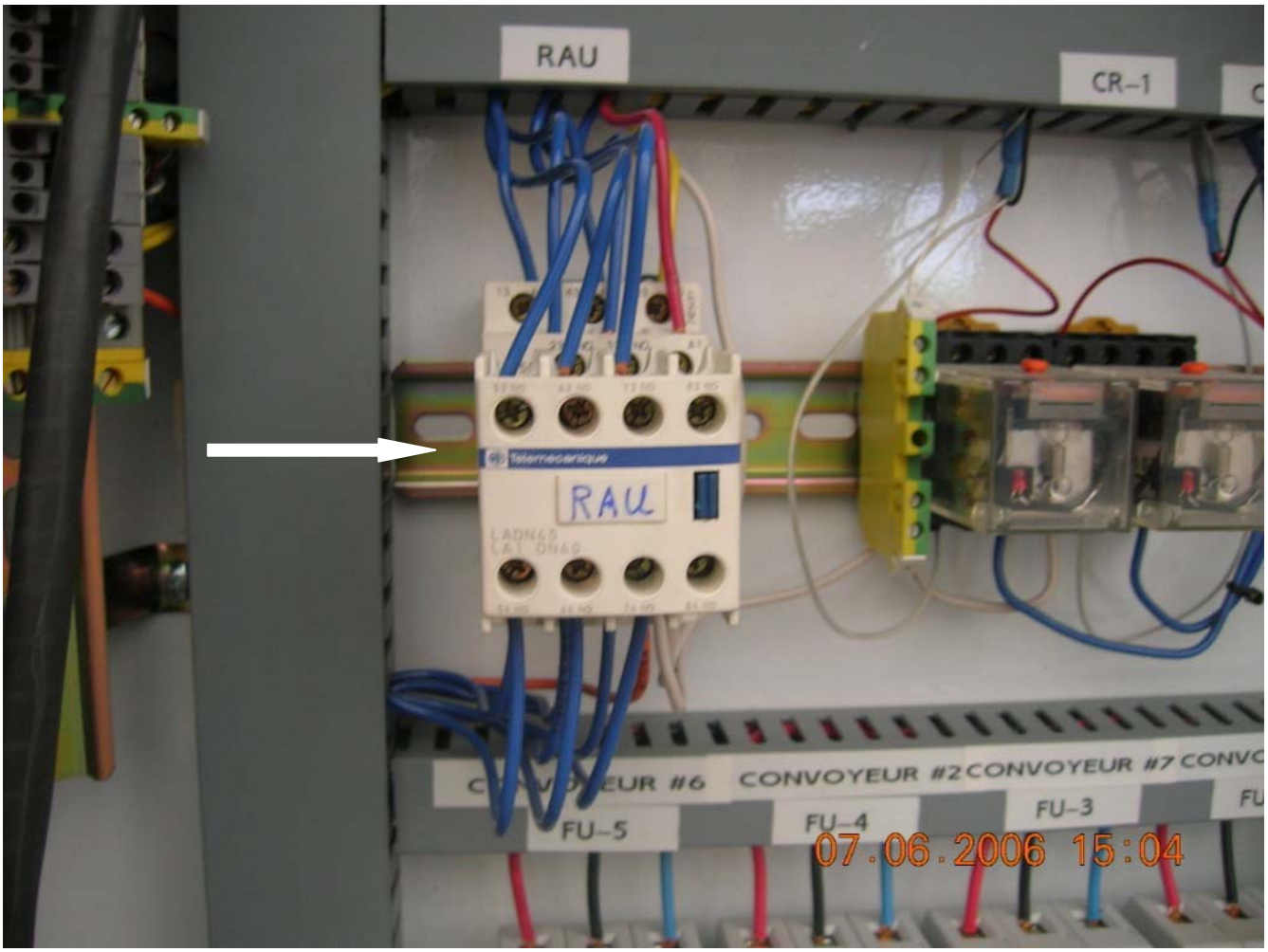
Photo 5



Interrupteur de position

(Source : CSST)

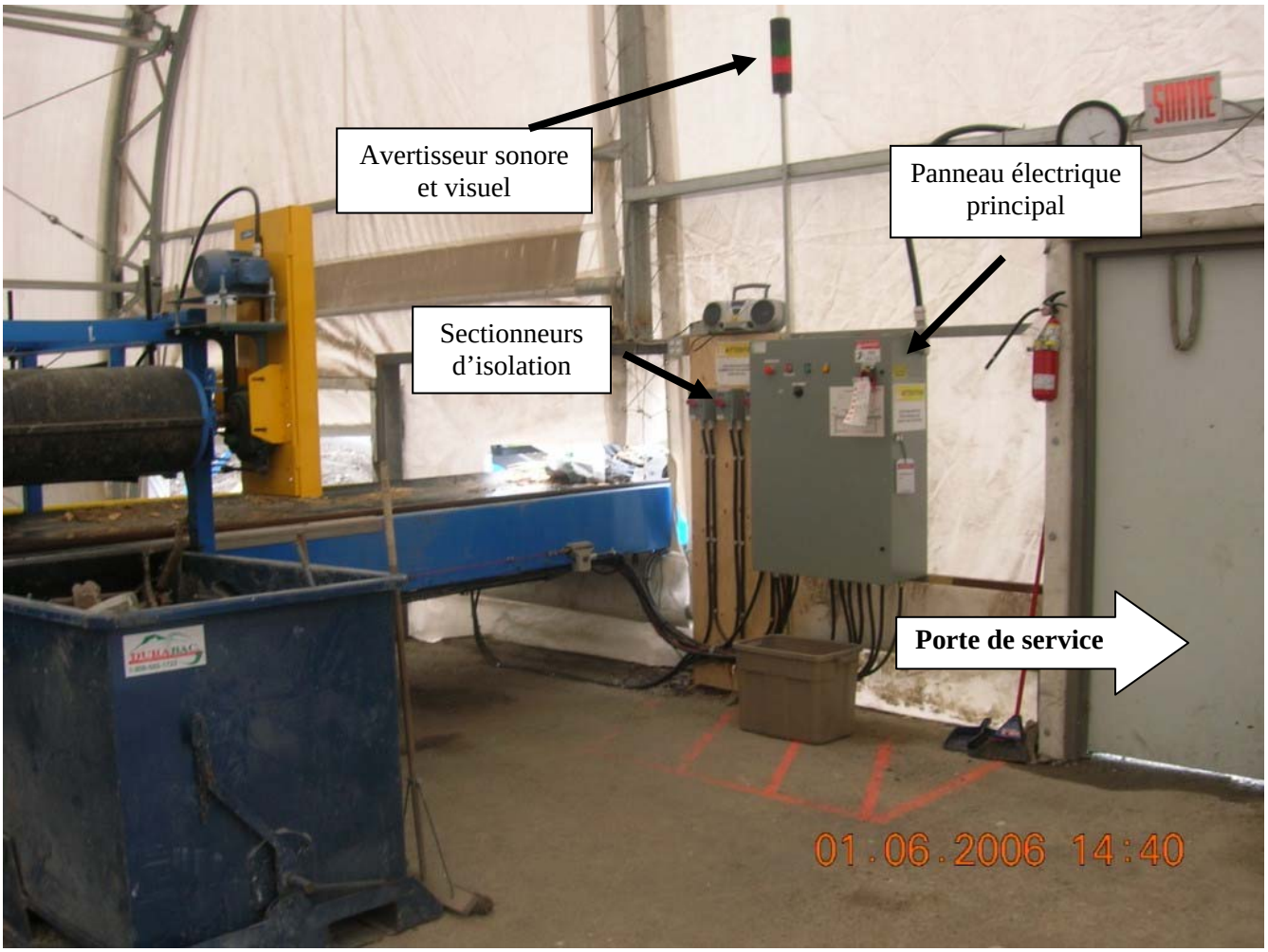
Photo 6



Relais de sécurité à l'intérieur du panneau électrique principal

(Source : CSST)

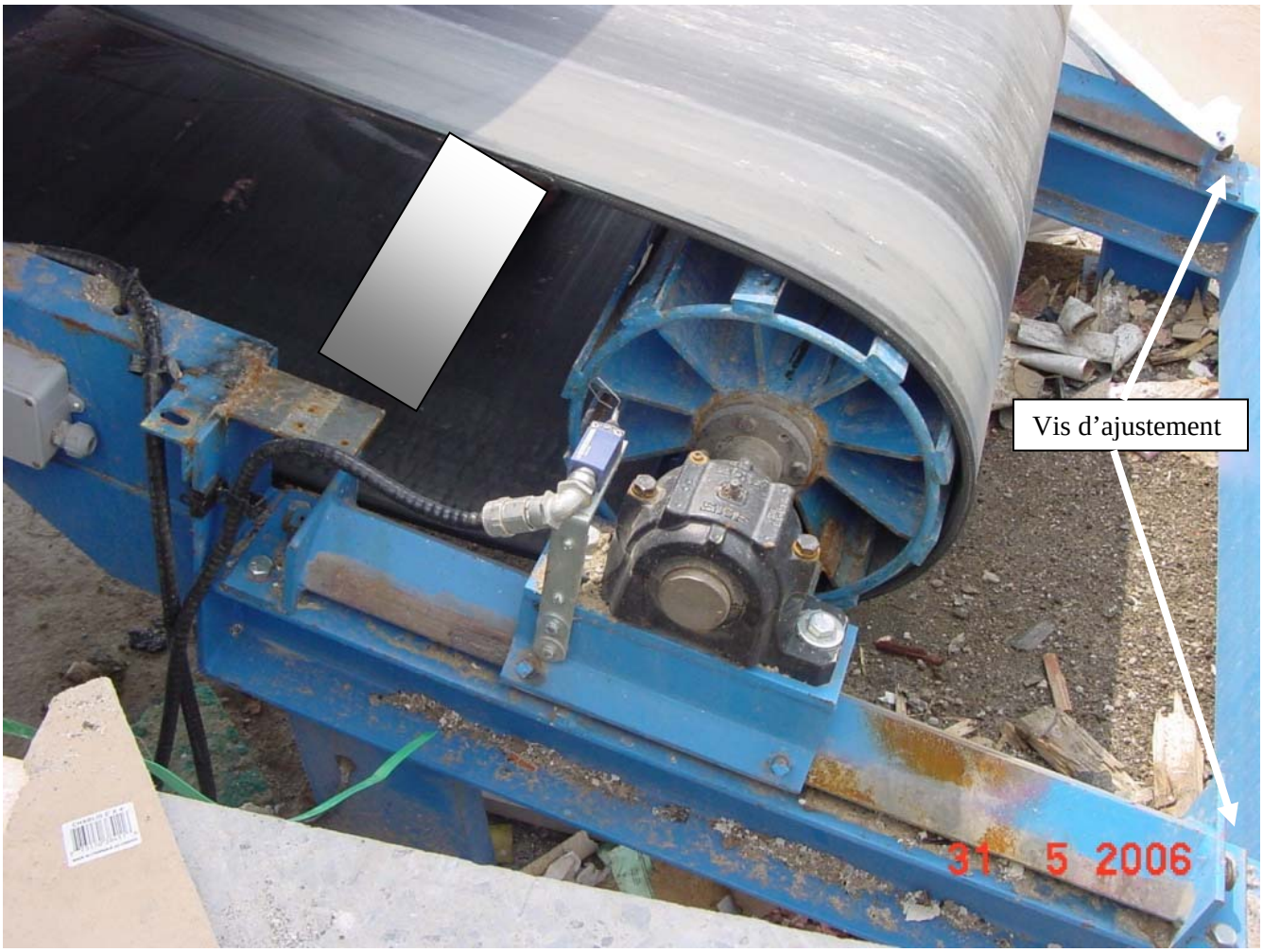
Photo 7



Avertisseur sonore et visuel du système de convoyeurs et position des sectionneurs d'isolation

(Source : CSST)

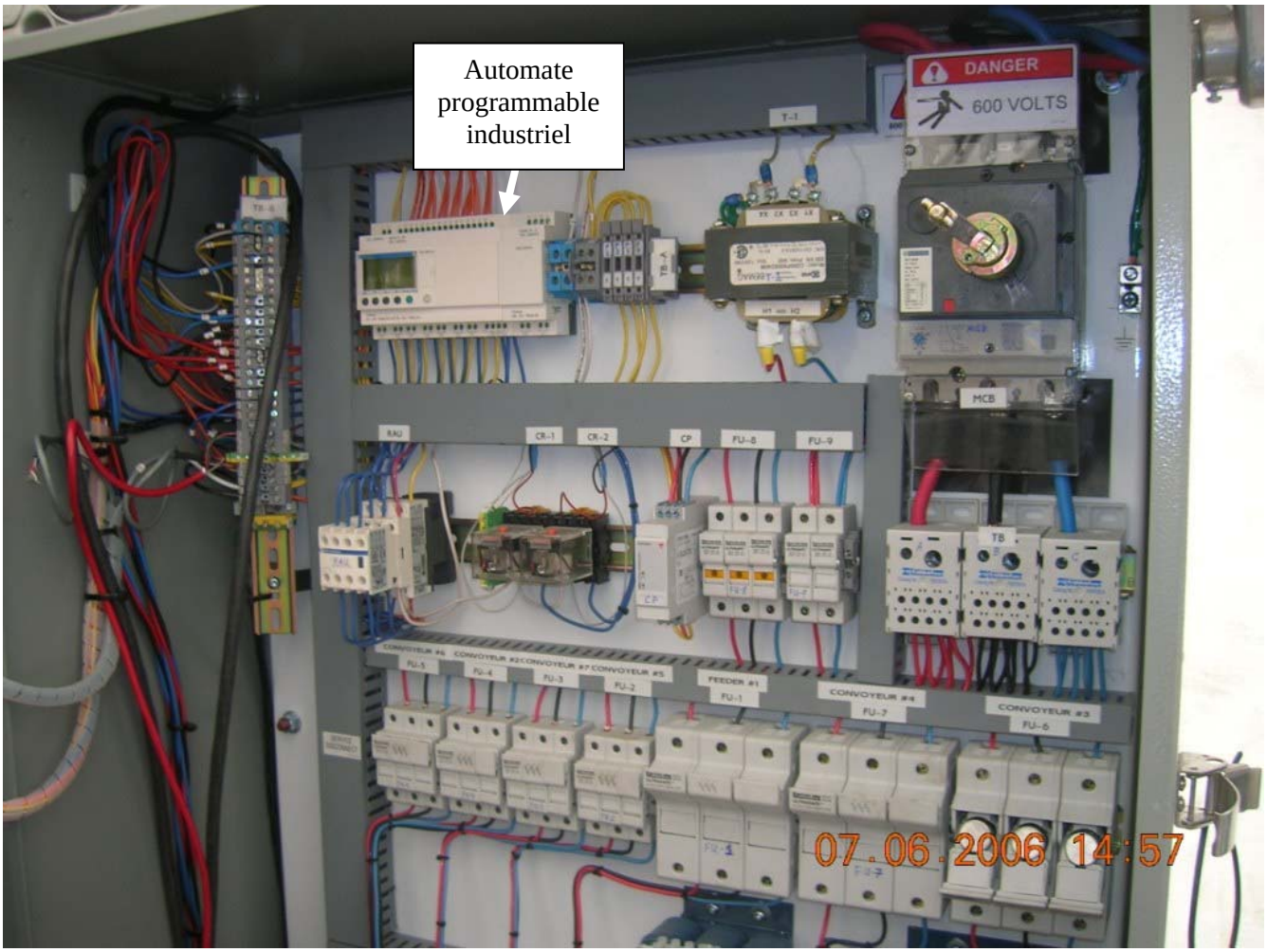
Photo 8



Tambour de queue du convoyeur numéro 7

(Source : CSST)

Photo 9



Panneau électrique et de contrôle principal pour le système de convoyeurs

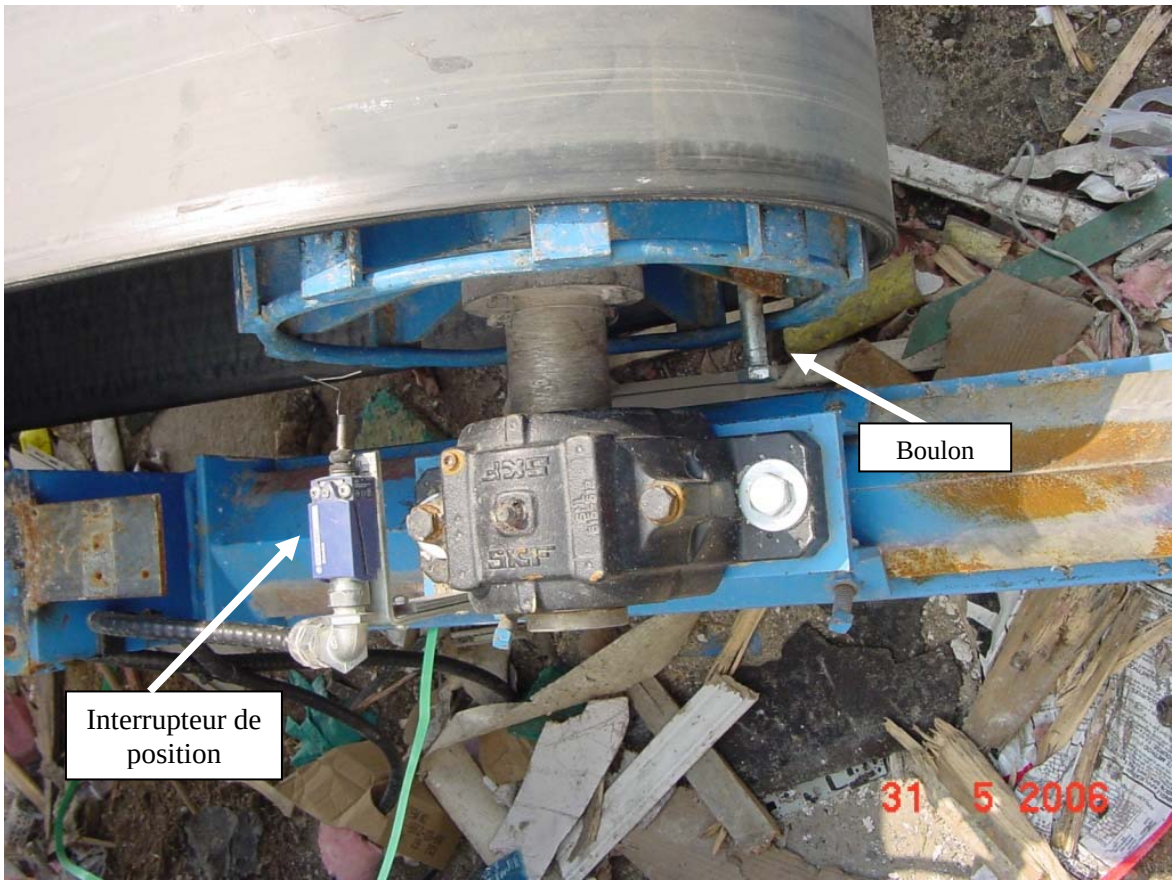
(Source : CSST)

Photo 10

Affiche sur le panneau électrique principal

(Source : CSST)

Photo 11



Présence de débris autour du tambour de queue

(Source : CSST)

Photo 12

Sectionneur d'isolation du convoyeur numéro 7 mis en position ouverte (*« off »*)

(Source : CSST)

Photo 13

Bouton d'arrêt normal sur le panneau électrique principal

(Source : CSST)

ANNEXE D

Liste des témoins et des autres personnes rencontrées

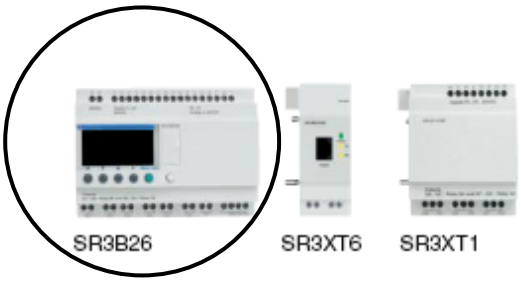
Liste des témoins et des autres personnes rencontrées

- Monsieur [redacted] de Transformation de matières recyclables T.M.R. inc.
- Monsieur [redacted] chez Transformation de matières recyclables T.M.R. inc.
- Monsieur [redacted] chez Transformation de matières recyclables T.M.R. inc.
- Madame [redacted] chez Transformation de matières recyclables T.M.R. inc.
- Monsieur [redacted] chez Transformation de matières recyclables T.M.R. inc.
- Monsieur [redacted] chez Transformation de matières recyclables T.M.R. inc.

ANNEXE E

Description de l'automate programmable industriel

Description de l'automate programmable industriel



Modules compacts ou modulaires

■ **Zelio Logic Compact**, une solution optimisée pour des automatismes simples de 10 à 20 E/S :
□ 3 modèles monoblocs de 10, 12, 20 E/S : versions avec ou sans afficheur et touches.
■ **Zelio Logic Modulaire :**
□ 2 bases de 10 et 26 E/S extensibles jusqu'à 40 E/S
□ 3 types de modules d'extension : 6, 10, 14 E/S
□ 1 module d'extension de communication Modbus... pour de nouvelles fonctionnalités et capacités de programmation.

Extensions d'entrées/sorties
Les modules logiques Zelio Logic modulaires peuvent recevoir des extensions d'entrées/sorties si nécessaire, alimentées par le module logique :
■ 6, 10 ou 14 E/S TOR
■ 2 entrées ANA et 2 sorties ANA.

Extension de communication
Un module d'extension de communication sur réseau Modbus est proposé pour les modules logiques Zelio Logic modulaires. Il est alimenté en ⎓ 24 V, par le module logique.

SR2 PACK

Programmation
La programmation peut être effectuée :
■ de façon autonome en utilisant le clavier du module logique (langage à contacts)
■ sur PC avec le logiciel "Zelio Soft".
Sur PC, la programmation peut être réalisée soit en langage à contacts (LADDER), soit en langage blocs fonctions (FBD).

Mémoire
Le module logique Zelio Logic intègre une mémoire de sauvegarde, qui permet de dupliquer le programme dans un autre module logique (exemples : réalisation d'équipements identiques, envoi de mises à jour à distance).
Cette mémoire permet aussi d'effectuer une sauvegarde du programme en prévision d'un échange du produit.
Lorsqu'elle est associée à un module sans afficheur et sans touches, la copie du programme contenu dans la cartouche est automatiquement transférée dans le module logique à la mise sous tension.

Automate programmable industriel de marque Télémécanique, modèle SR3 B261FU

(Source : Telecatalog – Automatisme et contrôle 2006)

ANNEXE F

Rapport d'expertise

GROUPE CADEC des gens de solutions

Montréal
450.973.9111
www.groupecadec.com

Sherbrooke
819.569.1009
info@groupecadec.com

Laval, mercredi, 16 mai, 2007

À :

André Dupras, ing.
Inspecteur
CSST – Direction Régionale de St-Jean-sur-Richelieu

De :

Alain Brassard, ing.
Expert en automation et robotique
Expert en sécurité des machines

Rapport d'expertise : accident chez TMR inc

Monsieur,

Il me fait plaisir de vous soumettre ce rapport qui met en lumière les éléments techniques qui ont un lien avec l'accident mortel survenu à l'usine de TMR inc, au 503 Rg Ste-Marie à St-Sébastien le 31 mai 2006.

Les installations de TMR ont été visitées le 28 novembre 2006.

Cordialement,

Alain Brassard, ing.
Expert en Sécurité des Machines
Expert en automatisation industrielle

Table des matières

1. Prise de contact

M. André Dupras ainsi que Jean Martel, tous deux des inspecteurs de la CSST de la Régionale de St-Jean-sur-Richelieu, sont venus me rencontrer le 17 novembre dans nos bureaux de Laval. M. Dupras nous a alors expliqué les circonstances connues d'un accident survenu le 31 mai 2006 chez TMR à St-Sébastien; un travailleur est décédé suite à une intervention dans un convoyeur à courroie. J'étais accompagné de Serge Danis, ing., membre du Groupe Cadec lors de cet entretien.

Nous avons visualisé les photos qui ont été prises suite à l'événement. Le procédé à l'usine de traitement de matières recyclables chez TMR est contrôlé à l'aide d'un automate programmable industriel (API) de marque Télémécanique (SR3B261FU). M. Dupras nous a ensuite remis le programme informatique qui gère les états de cet API. Selon M. Dupras, cette version du programme était celle qui contrôlait le système le jour de l'accident. M. Dupras nous a aussi remis un logiciel (ZelioSoft 2, version 2.4) avec lequel il était possible de visualiser le programme en question. Ce logiciel nous a aussi permis de simuler le fonctionnement du programme et de visualiser les effets de certaines mises en scènes.

Lors de cet entretien, nous avons pu effectuer quelques simulations sur le programme à l'aide du logiciel. À la fin de la rencontre les membres du Groupe Cadec ont pu déterminer qu'ils étaient en mesure de satisfaire les demandes des inspecteurs Dupras et Martel pour fournir une expertise en automatisation et en sécurité des machines.

2. Mandat d'expertise

La description originale du mandat, telle que rédigée par André Dupras, est reproduite en annexe.
Le mandat consiste à éclaircir les éléments de conception et d'utilisation des équipements automatisés chez TMR, en particulier le système de convoyeurs fourni par Vibrotech.
Le texte décrivant le mandat a été envoyé à Alain Brassard de Groupe Cadec le 14 novembre 2006 par André Dupras, inspecteur à la CSST. Voici le texte en question[1] :
…
La CSST octroie donc un mandat d'expertise afin d'éclaircir certains points de l'enquête et de vérifier si l'ensemble du système nouvellement installé est sécuritaire et si la conception de ce système a été faite selon les règles de l'art.

2.1. Description du mandat

1. *Examiner l'ensemble du système de contrôle avec automate programmable industriel (API) de l'usine*
2. *Identifier les lacunes de conception du système, s'il y a lieu*
3. *Identifier si l'interrupteur de position était le bon mécanisme pour le rôle qu'il devait jouer*
4. *Identifier si l'installation de l'interrupteur de position du convoyeur no 7 a été faite selon les règles de l'art. Est-ce que cet interrupteur a été conçu afin de permettre des interventions sur le convoyeur non-cadenassé? Si oui, son niveau de sécurité est-il suffisant?*
5. *Indiquer si la programmation de l'API aurait dû prévoir, pour l'interrupteur de position, l'activation des avertisseurs visuel et sonore pendant huit secondes comme lors de la remise en marche des convoyeurs. Est-ce qu'une période de 8 secondes est suffisante pour éliminer tout danger?*
6. *Procéder à des essais « in situ » et virtuel (par simulation) de l'interrupteur en cause pour reproduire le fonctionnement anormal de celui-ci lors de l'accident du 31 mai 2006.*

[1] Le document a été envoyé par courriel d'abord. Ce même texte a ensuite été inséré dans un document accompagnant le contrat pour la demande en question et qui a été envoyé le 24 novembre 2006.

7. *Lorsqu'une situation anormale permet à l'API d'arrêter les convoyeurs, est-ce que cet arrêt devrait être permanent jusqu'à l'intervention de l'humain (ex. : un reset à l'interrupteur)? Dans le cas présent, la reprise des opérations a causé la mort d'un travailleur et aurait pu mettre en danger la sécurité de plusieurs autres travailleurs. Est-ce que le niveau de sécurité des composantes est adéquate, le type d'API utilisé est-il adéquat?*
8. *Rédiger un rapport signé par un ingénieur, membre de l'Ordre des ingénieurs du Québec, résumant les points ci-haut mentionnés et donner son avis d'expert sur la situation présentée.*

2.2. Le mandat, point par point

2.2.1. Point 1

Le système a été examiné lors d'une visite sur le site de TMR inc. le 28 novembre 2006 en compagnie d'André Dupras et Jean Martel pour visiter les lieux, prendre connaissance du système et de son fonctionnement et effectuer quelques essais pour évaluer les réactions du système. M. E de AD-Tech Électrique nous y attendait et a assisté aux essais. Les résultats de ces essais sont discutés plus loin, au Point 6.

2.2.2. Point 2

Nous allons nous concentrer sur la conception électriques éléments électriques, les automatismes (logique et programmation), le choix des dispositifs électriques et électroniques et leur installation, les principes de sécurité des machines de même que les items touchant les applications industrielles qui me sont familières (certains choix de convoyeurs, par exemple).

Du point de vue électrique, je n'ai pas observé de lacune concernant les éléments de base comme l'utilisation de matériel prévu pour des applications industrielles, d'éléments de coupure et de protection électrique adéquates ou du calibre des conducteurs, par exemple. Bien entendue, nous ne sommes pas allés dans le détail comme le calcul des charges ou les températures d'utilisation des gaines isolantes pour les conducteurs.

En ce qui a trait à la programmation, ce point est discuté plus bas à la section 2.2.5.

Dans son ensemble, le système semble conçu adéquatement pour remplir le rôle demandé par le client, c'est-à-dire TMR. Aucune lacune évidente n'a été relevée dans la conception électrique du système.

2.2.3. Point 3

Un interrupteur a été installé près du tambour de queue du convoyeur #7. Ce détecteur avait pour but de détecter le passage d'un boulon, soudé au tambour. À chaque tour, le boulon accrochait l'actionneur de l'interrupteur qui se présentait sous la forme d'une 'moustache de chat' (cat whisker), et provoquait un changement d'état momentané du signal pour revenir à son état initial une fois le boulon passé. Techniquement, le contact (normalement) fermé de l'interrupteur s'ouvrait pour ensuite se refermer après le passage du boulon. Le signal était envoyé à l'API. Ce dernier effectuait une supervision de ce signal lorsque le convoyeur était en fonction. Si un délai trop long s'écoulait entre deux signaux, l'API réagissait en interrompant le fonctionnement du système. Le rôle de cette supervision permettait d'éviter que le moteur du convoyeur #7 ne fonctionne si le tambour était bloqué (par des débris, par exemple).

L'interrupteur qui a été choisi, devait respecter certains critères, tant au niveau de son choix que de son installation. Voir aussi, en Annexe, la section 2.4.1

L'interrupteur

L'interrupteur, fabriqué par le manufacturier Telemecanique (Schneider Électrique) correspond au numéro de commande XCKD2106N12. Il est composé d'un boîtier de métal avec contacts à ouverture brusque (NO/NF) respectant le principe d'ouverture forcée, de modèle ZDC21, associé à un actionneur en forme de moustache de chat de modèle ZCE06. Voir description technique entière en annexe.

C'est un interrupteur de position avec un organe externe de détection (actionneur) appelé 'moustache de chat' (whisker). Ce type d'interrupteur permet de détecter le passage d'un objet lorsque celui-ci entre en contact avec l'actionneur et ce, quelle que soit la direction d'approche, tant que celle-ci provoque une déflexion ou un déplacement de cet actionneur. Il importe, cependant, de s'assurer que la déflexion de l'actionneur soit suffisante pour provoquer le changement d'état des contacts électriques. Ceci dépendra de la distance entre l'interrupteur et l'objet à détecter.

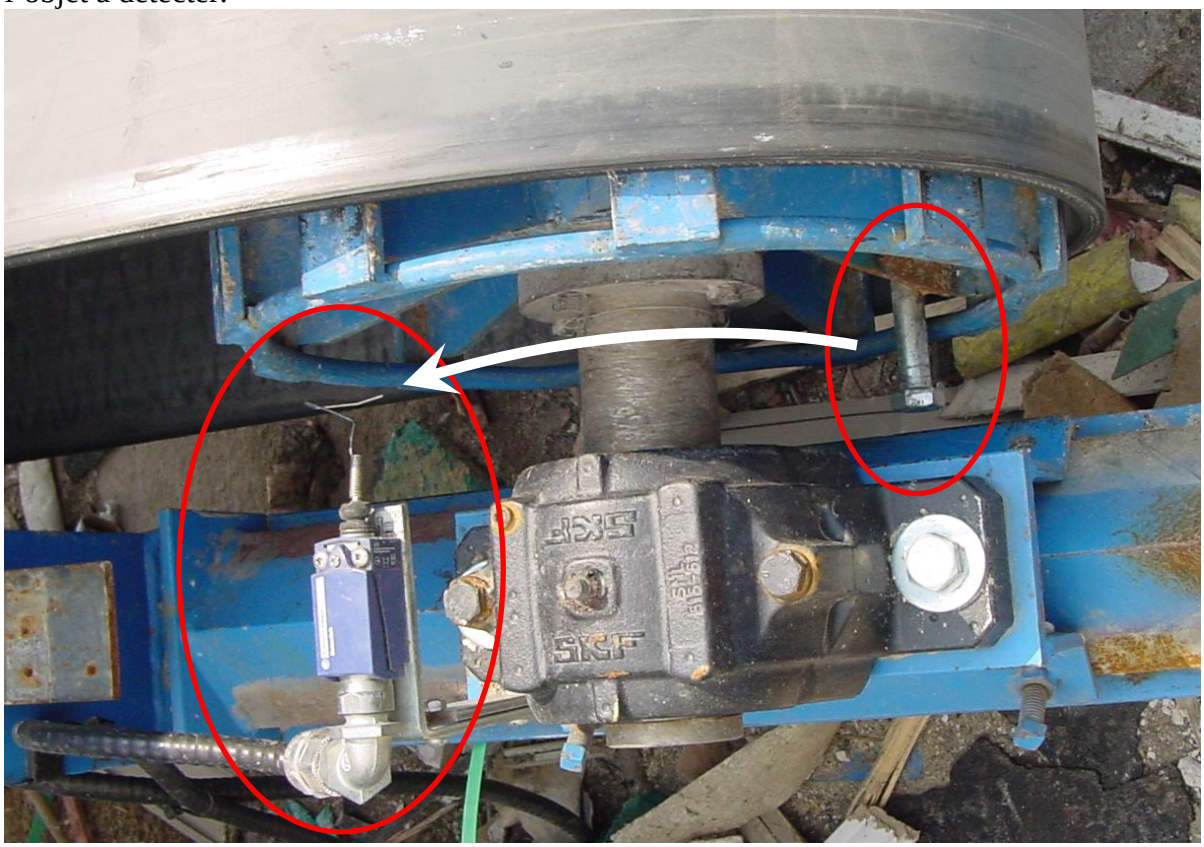


Figure 1: Interrupteur et boulon. Photo fournie par la CSST

L'interrupteur devait être en mesure de résister aux influences du milieu dans lequel il devait être utilisé. Les influences attendues sont, entre autre : température d'utilisation (-40°C à + 40 °C, environ), vibrations, chocs, humidité / pluie, fréquence des changements d'état (environ 2 fois par seconde). Or, suite aux informations obtenues du fabricant, la plupart des caractéristiques étaient rencontrées. Seule la température d'opération de l'interrupteur pouvait devenir un problème durant les moments les plus froids de l'année. En effet, le manufacturier nous garanti un bon fonctionnement de l'interrupteur à l'intérieur d'un intervalle de -25 à 70°C.

À la lumière des caractéristiques attendues, nous pouvons convenir que l'interrupteur pouvait remplir le rôle pour lequel il a été choisi, dans la plupart des situations raisonnablement envisageables. Un mauvais fonctionnement est par contre prévisible lors de conditions climatiques extrêmes, si des mesures de protection du dispositif ou du système ne sont pas prises lors de l'installation. Une intervention pour nettoyer, dégager ou déglacer l'appareil était donc prévisible à différents moments de l'année. Aucune mesure ni instruction précise n'a été prévue par les fournisseurs du système (AD Tech et Vibrotech) pour réaliser cette intervention.

Outre les caractéristiques de résistance face aux éléments environnementaux (climat, débris, etc.), il faut aussi considérer qu'une moustache de chat est un organe très flexible et relativement fragile. C'est le genre de choix qu'il convient de faire dans un environnement bien contrôlé : trajectoire régulière de l'objet à détecter, déflexion suffisante à chaque fois de la tige de l'organe de commande, fixation solide, contrôle des détections parasites. Bref, le choix de ce moyen de détection aurait dû être accompagné de mesures supplémentaires pour en assurer le bon fonctionnement comme un couvercle, par exemple.

Étant données les difficultés accompagnant son installation, qui sont aussi liées à l'environnement, il aurait été préférable de choisir un interrupteur avec un organe de détection qui soit moins vulnérable aux influences du milieux.

L'installation

Même si l'interrupteur choisi peut résister aux exigences climatiques et d'humidité, il convient que pour éviter toute défaillance, il est important de le protéger adéquatement. Ainsi, il est préférable d'éviter de l'exposer directement aux intempéries.

Il est possible que certains défauts apparaissent durant une utilisation prolongée, causés par la présence de glace, de poussière, de boue, empêchent l'interrupteur de changer d'état ou de bien fonctionner. Il est aussi possible que des débris se retrouvent dans la zone d'opération du capteur et entravent son bon fonctionnement. Ce type de défaut aurait exigé une intervention de nettoyage ou de dégagement de l'interrupteur.

Nous savons que l'interrupteur à moustache de chat remplaçait un interrupteur d'un autre type qui a été détruit durant son utilisation. En effet, selon M. Desrochers, le tambour se déplace le long de son axe. Pour cette raison, le premier dispositif qui a été utilisé, qui étaient un interrupteur de proximité (avec un champ de détection en général relativement court allant de 2 à 12mm) a été remplacé. Il est donc important de s'assurer que l'interrupteur n'est pas affecté par ces mouvements; il doit toujours être en position de détecter, il ne doit jamais être frappé par le tambour ou le boulon.

Comme nous pouvons le constater sur la photo de la Figure 1, l'interrupteur était installé dans l'axe du tambour et non pas perpendiculaire à celui-ci. Les mouvements du tambour le long de son axe étaient connus, alors la collision entre le boulon et l'interrupteur était à prévoir. De plus, d'après la même photo, la forme pliée de la moustache de chat était prédisposée à être accrochée et emportée par la tête du boulon.

Le bris de l'interrupteur pourrait avoir été causé par n'importe laquelle des deux événements. Voir le résultat à la Figure 2.

Figure 2: Interrupteur endommagé. Photo fournie par la CSST

La fonction de l'interrupteur avait été désactivée dans le programme de l'API à la suite de l'accident du 31 mai 2006, mais avait été laissé en place. Nous savons que l'actionneur de l'interrupteur a finalement été détruit quelques semaines plus tard mais cela n'a pas provoqué d'arrêt.

Il est donc clair que l'installation était déficiente; soit l'interrupteur n'était pas installé (et protégé) correctement, soit les mouvements de l'arbre du tambour n'ont pas été limités suffisamment.

Il est à noter que l'installation d'un interrupteur jouant ce rôle constituait une addition au système original. Voir à ce sujet, en Annexe, les sections 2.4.1 et 2.5.2. En effet, il n'était pas prévu par le manufacturier qu'un moyen allait être utilisé pour superviser le bon fonctionnement du convoyeur #7. Il convient de mentionner que cet ajout était tout à fait indiqué pour prévenir des bris de la machine ou une usure prématurée. Ces bris ou cette usure auraient nécessité une intervention de la part des personnes assignées à l'entretien de la machine. Cette intervention constitue une exposition à différents risques.

En clair, moins une machine nécessite d'entretien, moins les gens sont exposés aux différents risques associés à ces tâches. Il est donc intéressant de noter que les efforts visant à fiabiliser un équipement ont aussi une influence sur les risques qu'il représente.

2.2.4. Point 4

L'installation de l'interrupteur n'a pas été faite dans les règles de l'art (voir le Point 3).

L'interrupteur n'a pas été conçu à des fins de sécurité. Il n'a pas été installé non plus dans un optique de protection. Cet interrupteur n'offrait aucune protection contre les risques associés à la machine. Il a été conçu à des fins de procédé, et installé pour protéger la machine et seulement la machine. Il est vrai cependant qu'en évitant des bris, des blocages ou des déversements, nous évitons que des travailleurs s'exposent à des risques en régularisant la situation.

Toute intervention qui met un ou des individus en contact avec les zones dangereuses de la machine doit se faire à la suite d'une consignation (cadenassage) des sources d'énergie dangereuses en bonne et due forme.

Un sectionneur d'isolation avec une poignée cadenassable pour le moteur du convoyeur #7 est installé à l'intérieur du bâtiment à proximité de l'armoire électrique principale (voir la Figure 3). Ce sectionneur doit être cadenassé en position Hors (OFF) durant toute la durée de l'intervention et par chaque individu exposé par l'intervention.

Figure 3: Sectionneurs d'isolation. Photo fournie par la CSST.

Il est clair que cet interrupteur qui a été ajouté à la conception originale a été choisi et installé dans le but unique de protéger la machine et non (directement) les travailleurs.

2.2.5. Point 5

Le système de convoyeurs est conçu pour démarrer après que l'opérateur ait appuyé sur le bouton marche.
La question du point 5 sous-entend que le redémarrage du système, suite à la manipulation de l'interrupteur, aurait dû respecter les séquences de démarrage usuelles.
En vérité, le redémarrage suite à ces manipulations constitue une faille dans le programme de l'API. Une faute de cette nature aurait dû générer un arrêt 'maintenu' du système. Ce qui signifie que seul un réarmement du système par l'entremise d'une commande volontaire aurait pu effacer la faute pour permettre au système de redémarrer à l'aide du bouton Marche.

Non, le système ne devait pas prévoir de séquence de démarrage suite à la manipulation du capteur. Le système n'aurait pas dû se remettre en marche. Le programme n'aurait pas du permettre au système de redémarrer.

Comme il est décrit à la section 2.5.3 de l'Annexe, certaines techniques ou moyens existent pour réduire les possibilités qu'une erreur de programmation n'entraîne un comportement indésirable de la part de la machine.

Cependant, si un tel comportement indésirable peut entraîner une situation dangereuse pour les opérateurs, ceci signifie que certains risques subsistent à l'intérieur du système. Si un tel risque subsiste, il est essentiel que les concepteurs ou les utilisateurs fassent en sorte que ce risque soit réduit en appliquant les principes de réduction des risques décrits dans la norme ISO 12100-1 et 2.

Le programme de l'API du système des convoyeurs chez TMR ne fait pas partie de des commandes relatives à la sécurité. En conséquence, les exigences de fonctionnalité sont moins grandes comme on peut lire à la section 2.5.2.1 de l'Annexe.

L'avertissement lors de chaque démarrage de système constitue un bon moyen pour augmenter la possibilité d'évitement d'un phénomène dangereux. De même, il permet de diminuer la probabilité qu'un incident dangereux lié aux fonctions (démarrage) du système en question ne survienne. Pour ce qui est de la durée de l'avertissement lors du démarrage, je crois que 8 secondes, est suffisant pour atteindre ces objectifs. Si l'avertissement est trop long, ceci peut induire une hésitation néfaste pour les intervenants; comme par exemple lorsque deux automobilistes se présentent en même temps à une intersection et qu'aucun d'eux ne sait si c'est à son tour d'y aller!

L'utilisation d'un avertissement n'éliminera pas tous les dangers. Ce moyen de réduction des risques doit être combiné à d'autres moyens si les risques visés sont importants. Les normes ISO 12100-1 et ISO 14121 dressent un tableau des différents moyens à considérer lors de l'élaboration des mesures de réduction des risques d'un équipement ainsi que leur efficacité relative.

2.2.6. Point 6

Durant la visite de MM Dupras et Martel, nous avons eu l'occasion de faire des essais simulés grâce au logiciel ZelioSoft 2. Nous avons pu, lors de ces tests, reproduire le comportement du système, tel qu'il était au moment de l'accident.

Le programme de l'API qui était présent au moment de la visite n'était pas le même que lorsque l'accident est arrivé. En effet, TMR avait demandé à E de AD Tech d'apporter quelques modifications pour ne plus tenir compte du capteur de détection de mouvement du tambour. E et moi avons procédé à la modification du programme résident pour qu'il devienne identique à celui lors de l'accident. Nous avons pu comparer le programme ainsi modifié avec la version remise à Groupe Cadec le 17 novembre 2006 et confirmer qu'ils étaient identiques.

Nous avons utilisé le capteur qui était installé lors de l'accident. Bien qu'il ait été endommagé par la suite (l'actionneur en forme de moustache de chat a été arraché), la fonction d'ouverture et de fermeture des contacts était toujours intacte. Nous avons relié le contact normalement fermé (NF) du capteur sur l'entrée d'API, là où il était originalement branché, en utilisant un câble électrique provenant d'une extension.

Nous avons ensuite fait fonctionner le système et procédé à quelques essais sur le système des convoyeurs (voir les résultats des essais à la section 5 de l'Annexe). Durant ces essais, j'ai dû actionner manuellement le capteur pour simuler le passage du boulon qui est soudé au tambour de queue.

5.2.1.1 Essai #1 : Marche et Arrêt normaux

Nous avons appuyé sur le bouton Marche, sur panneau de commande. Lors de la commande de démarrage, une alarme sonore s'est faite entendre durant une période de 8 secondes au terme de quoi le système s'est mis en route en cascade, en commençant par le convoyeur 7, tel que décrit à la section 1 de l'Annexe. Durant toute la durée de l'essai, j'ai dû faire bouger l'actionneur de l'interrupteur pour simuler le passage du boulon. Il est à noter que durant une période de 8 secondes, lors du démarrage du convoyeur 7, la faute provoquée par un délai trop long du passage du boulon n'est pas surveillée par l'API pour permettre au convoyeur de prendre sa vitesse sans causer d'arrêt.

Une fois que tout le système fut en marche, nous avons ensuite appuyé sur le bouton Arrêt, et le système s'est arrêté en cascade, conformément à la description donnée à la section1 de l'Annexe.

Cet essai nous a montré que le système démarre et s'arrête en cascade.

5.2.1.2 Essai #2 : Marche normale et Arrêt suite à la détection de blocage

Nous avons démarré le système comme à l'Essai #1. Durant toute la durée de l'essai, j'ai fait bouger l'actionneur de l'interrupteur. Une fois que tout le système fut en marche, j'ai cessé de bouger l'actionneur. Au bout de 4 secondes, le système entier s'est arrêté. Cette commande touche tous les moteurs du système en même temps; il n'y a pas d'arrêt en cascades suite à cette faute. La lumière rouge indiquant une faute s'est mise à clignoter au moment de l'apparition de la faute.

Suite à l'apparition de la faute (et à l'arrêt des convoyeurs), nous avons tenté de redémarrer le système en appuyant sur le bouton Marche, mais rien n'a bougé; la faute empêchait le redémarrage. Nous avons finalement redémarré le tout en appuyant d'abord sur le bouton de Remise À Zéro (RAZ) qui sert aussi de bouton d'arrêt. Cette action a éliminé la faute.

Cet essai nous a confirmé que la faute de blocage provoquait bel et bien un arrêt immédiat du système.

5.2.1.3 Essai #3 : Redémarrage du système par la manipulation de l'interrupteur de détection de blocage

Nous avons ensuite appuyé sur le bouton Marche et le système s'est activé tel que prévu. J'ai fait bouger l'actionneur de l'interrupteur jusqu'à ce que tout le système soit en marche à nouveau.

Une fois le système en marche, j'ai cessé de bouger l'actionneur. Au bout de 4 secondes, le système entier s'est arrêté à nouveau.
J'ai recommencé à bouger l'actionneur de l'interrupteur. Au bout de quelques secondes, le système s'est remis à bouger, en cascade. Une faille dans la programmation a permis au système de redémarrer sans que le bouton Marche ne soit appuyé. Fait à noter, l'alarme sonore ne s'est pas faite entendre au moment du redémarrage.

5.2.1.3.1 Explication de la réaction du système lors de l'essai #3 :

En étudiant le programme de l'API, nous avons pu déterminer quels étaient les mouvements de l'actionneur à accomplir ainsi que les délais à respecter pour permettre au système de se remettre en marche :

Le capteur était branché à l'entrée de l'API via son contact normalement fermé. En tenant l'actionneur pour le soustraire au passage du boulon, le travailleur a changé l'état du contact en position ouverte. À partir de cette position, il faut bouger l'interrupteur pour faire fermer, ouvrir et fermer à nouveau le contact à l'intérieur d'un intervalle de 4 secondes.

Il y a 2 temporisations qui sont à l'œuvre dans cette faille du programme. La première (TD) calcule le délai entre deux fermetures du contact et produit une faute si le temps (alors configuré à 4 secondes) expire. La seconde temporisation (T9) calcule un délai minimum (fixé à 4 secondes à ce moment) avant de permettre le démarrage du convoyeur #7, une fois toutes les conditions rencontrée. Lors de la fermeture du contact, les temporisations TD et T9 se mettent à compter en même temps. Voir le diagramme temporel à la Figure 4. Une version agrandie est représentée en Annexe

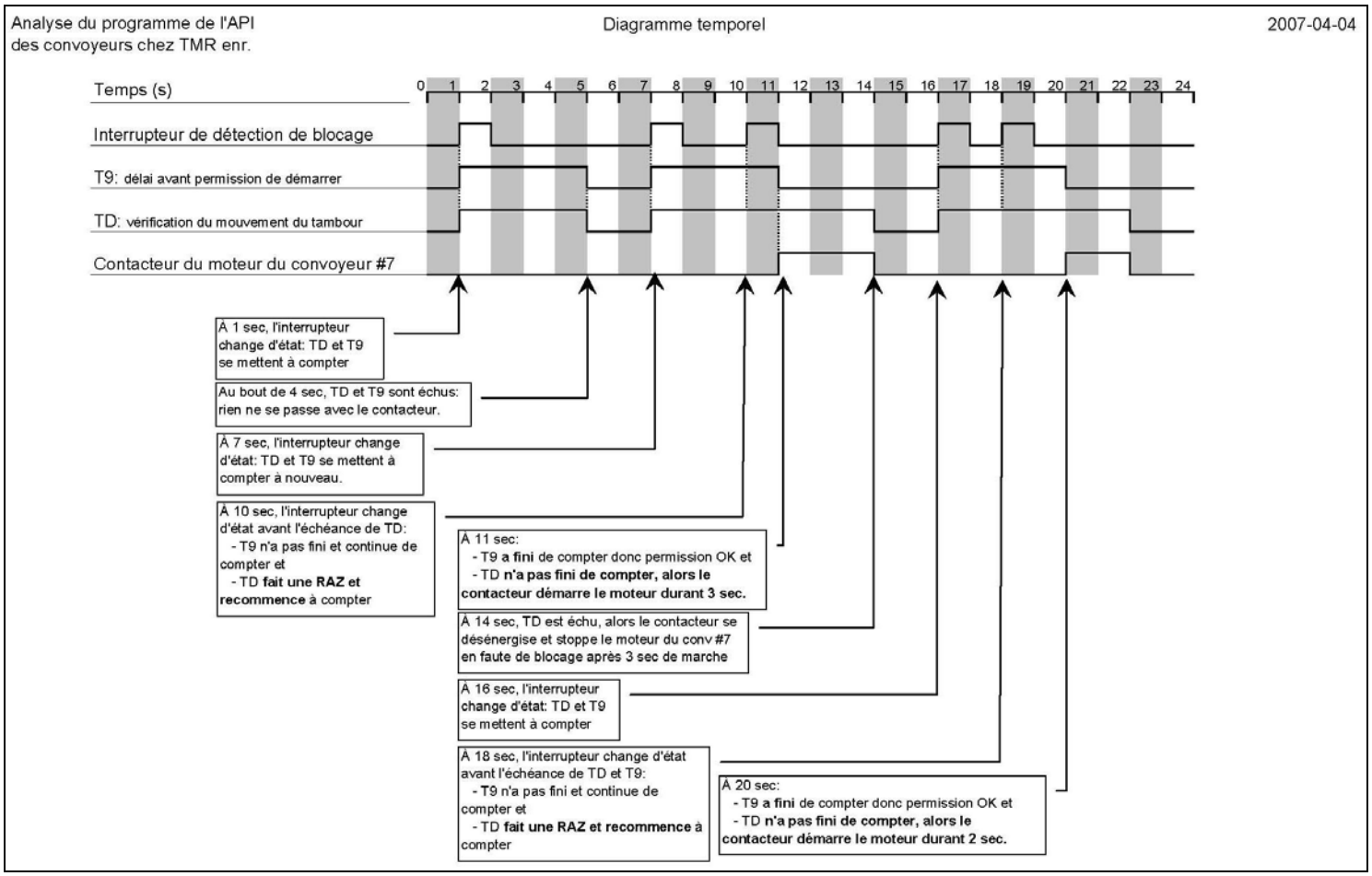


Figure 4: Diagramme temporel de TD, T9, l'interrupteur et le contacteur du conv #7. Représentation de la situation suite à un arrêt du convoyeur #7 en raison d'une détection de blocage.

En résumé, si le contact de l'interrupteur se ferme 2 fois à l'intérieur du délai de 4 seconde (ex : après 3 secondes), le convoyeur #7 sera en marche pour une durée équivalente à ce délai (ex : 3 secondes).

Cet essai nous a confirmé que le système en faute pouvait redémarrer à la suite d'une (mauvaise) manipulation ou de l'accrochage de l'interrupteur de détection de blocage. Nous avons aussi pu cerner les conditions qui permettait ce redémarrage.

5.2.1.4 Essai #4 : Comportement normal de l'opérateur suite à une faute de blocage.

Nous avons démarré le système normalement et lorsque tous les convoyeurs furent en marche, j'ai cessé de bouger l'actionneur de l'interrupteur. Au bout de 4 secondes, le système entier s'est arrêté.

J'ai appuyé sur le bouton de RAZ, comme un opérateur aurait eu à faire lorsqu'une telle faute apparaît.

J'ai ensuite bougé à nouveau l'actionneur de l'interrupteur plusieurs fois à l'intérieur des délais d'expiration de TD et T9. Le système est demeuré à l'arrêt.

Cet essai mettait en évidence que lorsque nous appuyons sur le bouton RAZ, qui est aussi le bouton Arrêt, suite à l'apparition de la faute de blocage, le programme de l'API ne permet pas au système de redémarrer suite à une manipulation de l'interrupteur. C'est aussi une façon de montrer que lorsqu'on appuie sur le bouton Arrêt, le traitement du programme maintient la condition d'arrêt jusqu'à l'utilisation du bouton Marche.

Cet essai était en lien avec le troisième paragraphe de la section 2.2.5 ci-haut.

5.2.1.5 Essai #5 : Tentative de redémarrage par l'interrupteur, suite à un Arrêt normal

Nous avons démarré le système normalement et lorsque tous les convoyeurs furent en marche, j'ai appuyé sur le bouton de RAZ, le système s'est arrêté en cascade.

Une fois que le système entier fut arrêté, j'ai bougé l'actionneur de l'interrupteur plusieurs fois à l'intérieur des délais d'expiration de TD et T9. Le système est demeuré à l'arrêt.

Cet essai reprend quelques éléments de l'essai #2, mais dans un contexte d'arrêt normal.

2.2.7. Point 7

Les essais on démontré que le système répondait aux fonctions normales qui étaient d'abord prévues (arrêts, départs détection des fautes prévues). Ils ont aussi permis de mieux cerner les circonstances qui ont permis au système de redémarrer le jour de l'accident.

Ce qui en ressort, c'est d'abord bien sûr cette faille dans la programmation de l'API. Dans les faits, la conception du programme fait en sorte qu'il est nécessaire que l'opérateur appuie d'abord sur RAZ afin de remettre le système en marche. Comme il a été démontré à la section précédente, lorsque nous appuyons sur RAZ, le programme ne permet pas le redémarrage du système par l'interrupteur de détection de blocage.

Le système détecte et traite les éléments suivants qui sont considérés comme des fautes :

- Entraînement à vitesse variable (EVV) en faute ou pas prête;
- Protection moteur (thermique ou de surintensité) déclenchée;
- Arrêt d'urgence (cette faute se retrouve aussi dans la rubrique des causes d'arrêt;
- Blocage du tambour de queue du convoyeur #7;

L'erreur de programmation réside dans le fait que les fautes n'entraînent pas le désamorçage des conditions assurant la mise en marche du système. En effet, si la protection thermique d'un moteur se déclenche, cela entraînera l'arrêt immédiat du système au complet (incluant celle du convoyeur #7, provoquant aussi une faute de blocage). Si la protection thermique est remise en fonction, il sera également possible de redémarrer le système en faisant bouger l'actionneur de l'interrupteur de détection de blocage du tambour de queue du convoyeur #7.

Les fautes ne sont pas traitée comme les autres causes d'arrêt (arrêt d'urgence, arrêt normal), qui elles, désamorcent toutes les conditions de marche.

Une modification a été testée dans l'environnement de simulation du logiciel de programmation de l'API du système des convoyeurs de TMR. J'ai fait en sorte que les fautes détectées par l'API soient traitées comme le fait d'appuyer sur Arrêt ou sur le bouton d'Arrêt d'Urgence. Le résultat est que la faute désamorce les conditions qui permettent au système de redémarrer à l'aide de l'interrupteur de détection de blocage. Voir à cet effet la Figure 5 plus bas.

Le mauvais usage de l'interrupteur qui a été fait lors de l'accident était difficilement envisageable de la par des concepteurs (du système, mais aussi du programme). Cependant, si à la suite d'un blocage, le tambour de queue cesse de tourner, il était possible d'envisager que lors de la manœuvre de déblocage, avec des outils quelconques (sans retirer le protecteur), un travailleur aurait pu accrocher le capteur à quelques reprises. Dans ce cas, le système serait redémarré de la même façon que nous avons pu reproduire à l'essai #3.

Cette situation nous amène à croire qu'il est possible que des blessures pouvaient survenir suite au démarrage intempestif de l'équipement;

- Des blessures aux travailleurs qui sont près des autres convoyeurs
- Des blessures au travailleur qui tente de débloquer le tambour de queue.

À ce stade, il y a 2 questions qui doivent nous interpeller :

1. Est-il possible que les équipements près desquels les travailleurs s'activent ne soient pas adéquatement protégés?
2. Est-il possible que lors d'un déblocage, tel que décrit plus haut, il serait de mise de procéder à une consignation (cadenassage) de l'équipement?

Outre certains problèmes liés à la programmation, les API peuvent souffrir de défauts à même leur quincaillerie : entrées, sorties, mémoire, communication.

L'utilisation d'un API qui n'est pas éprouvé pour la sécurité ne doit pas être utilisé pour assurer la protection de travailleurs. Le mode de défaillance de ces appareil est bien connu : il est imprévisible. En conséquence, il est découragé, par tous les experts dans le domaine de la sécurité des machines, de compter sur les API conventionnels pour la sécurité.

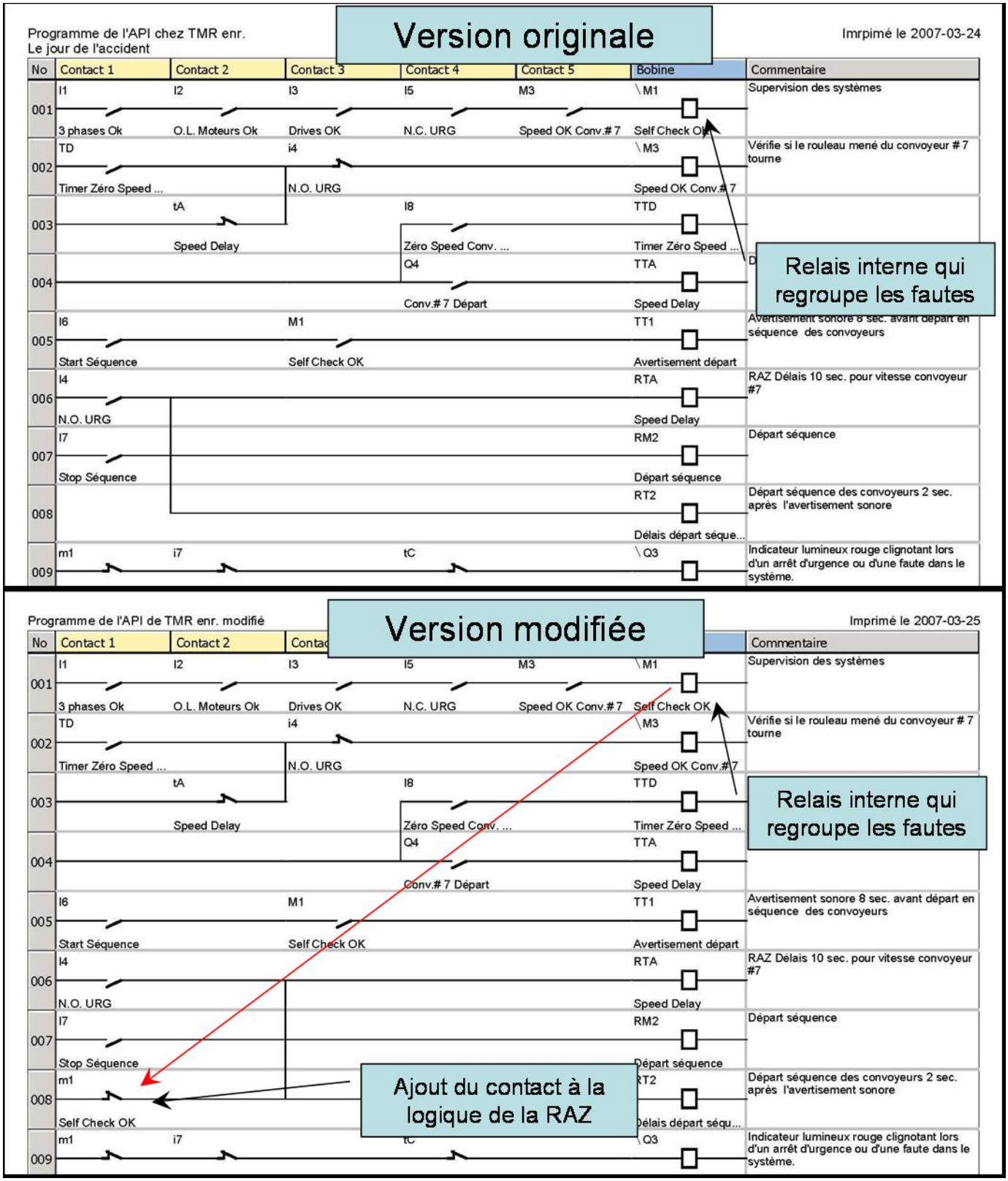


Figure 5: Description graphique de la modification pour empêcher le système de repartir à l'aide de l'interrupteur.

2.2.8. Point 8

L'écriture de ce rapport constitue la seule réponse à ce point.

3. Conclusion

Ce rapport vise à déterminer quel rôle ont joué la conception électrique et la programmation de l'API dans l'accident survenu le 31 mai 2006 aux installations que j'ai visitées chez TMR enr.

Ce qu'on peut établir d'emblée, c'est que la conception électrique de même que la programmation de l'API n'avaient pas comme objectif de protéger les travailleurs.

Le tambour de queue du convoyeur #7 possède un protecteur fixe pour protéger les travailleurs contre les risques présents à cet endroit lorsque le convoyeur est en fonction. Lorsqu'il est retiré, les travailleurs ont donc accès aux zones dangereuses désormais non protégées. Le protecteur fixe constitue la principale protection à cet endroit. Les autres mesures (séquence de démarrage avec avertissement sonore, délais, etc.) constituent des mesures complémentaires.

Le fait de faire fonctionner le système de convoyeurs alors que le protecteur était retiré est questionnable, au sens de l'article 184 du RSST, mais aussi en fonction des bonnes pratiques. Il est nécessaire d'appliquer les bonnes pratiques et les règles de l'art pour fabriquer des machines sécuritaires à opérer. Les règles de l'art sont aussi nécessaires pour assurer le maintien des moyens de protection. La limite dans la conception d'une machine et de son utilisation sécuritaire réside dans le respect de son fonctionnement prévu.

Le fait que des travailleurs soient intervenus sur le convoyeur #7 alors que le protecteur ait été enlevé constituait un risque certain. Selon l'article 185, les travailleurs auraient dû cadenasser les sources de mouvement dangereuses avant d'entreprendre les travaux cet endroit.

Le fait qu'un capteur destiné à détecter un blocage ait été utilisé pour assurer un arrêt sécuritaire constitue une utilisation qui n'était pas prévue par les concepteurs.

La faille dans la programmation de l'API a permis au système de redémarrer, mais cette faille n'aurait jamais dû être trouvée. Le système a été utilisé de manière imprévue et il a réagi de manière tout aussi imprévue.

Bibilographie :

Manuel d'opération général (installation et entretien), Vibrotech
ISO 12100-1, *Sécurité des machines — Notions fondamentales, principes généraux de conception — Partie 1: Terminologie de base, méthodologie*
ISO12100-2, *Sécurité des machines — Notions fondamentales, principes généraux de conception — Partie 2: Principes techniques*
ISO 13849-1, *Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 1: Principes généraux de conception*
ISO 13849-2, *Sécurité des machines — Parties des systèmes de commande relatives à la sécurité —Partie 1: Principes généraux de conception*
ISO14121, *Sécurité des machines — Principes d'Appréciation du risque*
IEC 60204 *Sécurité des machines – Equipement électrique des machines – Partie 1:Règles générales*
IEC 61310-3, *Sécurité des machines – Indication, marquage et manoeuvre – Partie 3: Spécifications sur la position et le fonctionnement des organes de service*