MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
Liberté
Égalité
Fraternité

Conseil général de l'environnement
et du développement durable
Bureau d'Enquêtes et d'Analyses
sur les Risques Industriels

BEA-RI
Risques industriels

Rapport d'Enquête

Sur le rejet de gaz naturel à l'atmosphère au sein du site industriel Géométhane situé à Manosque (04) le 1er janvier 2021

Bordereau documentaire

Organisme auteur : Bureau d'Enquêtes et d'analyses sur les risques industriels (BEA-RI)
Titre du document : Rapport d'enquête technique sur le rejet de gaz naturel à l'atmosphère au sein du site industriel Géométhane situé à Manosque (04) le 1er janvier 2021

N° : MTE-BEARI-2021-009

Date du rapport : 18/10/2021

Proposition de mots-clés : rejet, gaz naturel, automate de sécurité,

Avertissement

L'enquête technique faisant l'objet du présent rapport est réalisée dans le cadre des articles L.501-1 et suivants du Code de l'Environnement.

Cette enquête a pour seul objet de prévenir de futurs accidents. Sans préjudice, le cas échéant, de l'enquête judiciaire qui peut être ouverte, elle consiste à collecter et analyser les informations utiles, à déterminer les circonstances et les causes certaines ou possibles de l'évènement, de l'accident ou de l'incident et, s'il y a lieu, à établir des recommandations de sécurité. Elle ne vise pas à déterminer des responsabilités.

En conséquence, l'utilisation de ce rapport à d'autres fins que la prévention pourrait conduire à des interprétations erronées.

Au titre de ce rapport on entend par :

- Cause de l'accident : toute action ou événement de nature technique ou organisationnelle, volontaire ou involontaire, active ou passive, ayant conduit à la survenance de l'accident. Elle peut être établie par les éléments collectés lors de l'enquête, ou supposée de manière indirecte. Dans ce cas le rapport d'enquête le précise explicitement.

- Facteur contributif : élément qui, sans être déterminant, a pu jouer un rôle dans la survenance ou dans l'aggravation de l'accident.

- Enseignement de sécurité : élément de retour d'expérience tiré de l'analyse de l'évènement. Il peut s'agir de pratiques à développer car de nature à éviter ou limiter les conséquences d'un accident, ou à éviter car pouvant favoriser la survenance de l'accident ou aggraver ses conséquences.

- Recommandation de sécurité : proposition d'amélioration de la sécurité formulée par le BEA-RI, sur la base des informations rassemblées dans le cadre de l'enquête de sécurité, en vue de prévenir des accidents ou des incidents. Cette recommandation est adressée, au moment de la parution du rapport définitif, à une personne physique ou morale qui dispose de deux mois à réception, pour faire part au BEA des suites qu'elle entend y donner. La réponse est publiée sur le site du BEARI.

Synthèse

L'enquête technique faisant l'objet du présent rapport est réalisée dans le cadre des articles L.501-1 et suivants du code de l'environnement. Cette enquête a pour seul objet de prévenir de futurs accidents. Sans préjudice, le cas échéant, de l'enquête judiciaire qui peut être ouverte, elle consiste à collecter et analyser les informations utiles, à déterminer les circonstances et les causes certaines ou possibles de l'évènement, de l'accident ou de l'incident et, s'il y a lieu, à établir des recommandations de sécurité. Elle ne vise pas à déterminer des responsabilités. En conséquence, l'utilisation de ce rapport à d'autres fins que la prévention pourrait conduire à des interprétations erronées.

Dans la nuit du 31 décembre au 1er janvier 2021, le stockage souterrain de gaz de Géométhane de Manosque (04) est opérationnel mais ne transfère pas de gaz. A partir de 4h34 du matin, la mise en sécurité de l'atelier de traitement est déclenchée automatiquement à cause d'un défaut de communication entre automates de sécurité. A 6h35, l'atelier de compression est également mis en sécurité pour les mêmes raisons. Le site étant à l'arrêt et en sécurité l'astreinte de maintenance est arrivée sur site vers 10 h. Ne constatant pas de défaut apparent, elle réarme les différents systèmes. Dans l'après-midi, les mises en sécurité se déclenchent à nouveau. Ces séquences de mise en sécurité, qui ont fonctionné correctement, provoquent la décompression des ateliers concernés et entrainent la mise à l'atmosphère d'environ 20 000 m^3 de gaz naturel.

Le déclenchement intempestif des mises en sécurité a pour origine :

- D'une part, un défaut non permanent d'un switch réseau déclenchant de manière aléatoire un time-out (dépassement de délai) dans l'acheminement d'informations de sécurité entre les automates de sécurité des différents ateliers de l'installation ;
- Et d'autre part, le non fonctionnement de la redondance entre les réseaux dû à l'incompatibilité entre les versions de logiciel des différents automates.

Ont contribué également à la survenue de l'évènement, la conception initiale du réseau et la gestion des modifications, la maintenance logicielle des équipements, le manque de possibilité de diagnostic du réseau ainsi que la testabilité de la redondance de ce dernier.

L'enquête a permis d'établir des enseignements de sécurité dans le domaine de la conception, de l'évolution et de la maintenance de tels automates de sécurité.

Par ailleurs, outre ces enseignements de sécurité, le BEA-RI recommande à destination de l'exploitant de :

- **S'assurer, sur l'ensemble de ses sites, de la compatibilité des versions logicielles des automates de sécurité et mettre en place les procédures de gestion de maintenance permettant de garantir dans le temps cette compatibilité ;**
- **Rendre les équipements réseaux testables et diagnosticables.**

Sommaire

Rapport d'enquête sur le rejet de gaz naturel à l'atmosphère le 1er janvier 2021 au sein du site industriel Géométhane situé à Manosque (04)

I. Rappel sur l'enquête de sécurité

L'enquête technique faisant l'objet du présent rapport est réalisée dans le cadre des articles L.501-1 et suivants du code de l'environnement. Cette enquête a pour seul objet de prévenir de futurs accidents. Sans préjudice, le cas échéant, de l'enquête judiciaire qui peut être ouverte, elle consiste à collecter et analyser les informations utiles, à déterminer les circonstances et les causes certaines ou possibles de l'évènement, de l'accident ou de l'incident et, s'il y a lieu, à établir des recommandations de sécurité. Elle ne vise pas à déterminer des responsabilités. En conséquence, l'utilisation de ce rapport à d'autres fins que la prévention pourrait conduire à des interprétations erronées.

II. Constats immédiats et engagement de l'enquête

II.1 Les circonstances de l'évènement

Dans la nuit du 31 décembre au 1er janvier 2021, le stockage souterrain de gaz de Manosque est opérationnel sous le suivi d'une équipe d'exploitation. Aucun mouvement de gaz (entrée ou sortie) n'a lieu durant la nuit. A 4h34 du matin, une première mise en sécurité est déclenchée automatiquement au niveau de *« l'atelier traitement »* du stockage souterrain de gaz. Elle est suivie par une seconde mise en sécurité de « *l'atelier compression* » à 6h35 et enfin d'une mise en sécurité de la station Gaude à 9h56. Ces mises en sécurité sont déclenchées par des pertes de communication entre les automates de sécurité. Après réarmement et vérification de l'installation, une seconde perte de communication intervient à 13h28 et déclenche l'isolement de chacun des trois ateliers. A 14h06, une nouvelle perte de communication déclenche également à nouveau une mise en sécurité de l'installation de traitement et enfin à 19h59 la mise en sécurité de l'atelier de compression.

II.2 Le bilan de l'évènement

Certaines des mises en sécurité qualifiées « d'ultimes », intervenues le 1er janvier, entrainent l'isolement des différents ateliers composant le site et la décompression de ces derniers par ouverture des évents de sécurité. Chacune de ces manœuvres a pour conséquence l'émission de gaz naturel à l'atmosphère dans des zones prévues à cet effet. La somme des deux séries d'évènements a ainsi conduit à l'émission à l'atmosphère d'environ 20 000 m3 de gaz naturel soit 16 tonnes environ, selon l'évaluation de l'exploitant.

Toujours selon l'exploitant, les différentes émissions de gaz naturel ayant eu lieu dans des conditions bien définies par des évents de sécurité situés dans des localisations adaptées et interdites d'accès, il n'y a jamais eu de concentration de gaz dans l'atmosphère supérieure à la limite inférieure d'explosivité au niveau du sol. Ces mises en sécurité par émission à l'atmosphère sont prévues dans l'étude de dangers

et intègrent les mesures nécessaires pour prévenir l'inflammation du gaz (interdiction de survol à basse altitude, protections …).

II.3 Les mesures prises après l'évènement

A la suite de l'évènement, l'installation a été mise à l'arrêt pendant 10 jours dans l'attente notamment d'une première enquête de la part de l'exploitant sur les causes de l'évènement et la mise en place sous sa responsabilité de mesures correctives.

II.4 L'engagement et l'organisation de l'enquête

L'inspection des installations classées a été informée succinctement par l'exploitant de l'évènement le 11 février 2021. L'inspection a collecté des éléments plus précis lors d'une visite sur site le 4 mars 2021.

La quantité de gaz naturel rejetée à l'atmosphère étant supérieure à cinq pour cent de la quantité seuil de la directive Seveso, qui est de 200 tonnes et en application de l'article 18 de la directive Seveso, l'inspection des installations classées (DGPR/DREAL) a considéré le 4 mars 2021 que l'évènement devait être qualifié d'accident majeur au sens de l'annexe 6 de cette même directive.

Cette qualification conduit à une ouverture d'enquête systématique par le bureau d'enquêtes et d'analyses sur les risques industriels (BEA-RI) qui a été actée par le directeur du bureau le 13 mars 2021 après en avoir informé le directeur général de la prévention des risques (DGPR).

Les enquêteurs techniques du BEA-RI ont ainsi réalisé une première réunion en visio-conférence le 1er avril 2021 avec les responsables de GEOMETHANE.

Ils ont recueilli les témoignages ou déclarations écrites des acteurs impliqués dans l'évènement et dans sa gestion. Ils ont eu, consécutivement à ces entretiens et aux réunions techniques organisées par la suite, communication des pièces et documents nécessaires à leur enquête.

Enfin, une visite sur site a eu lieu le vendredi 9 juillet 2021.

III. Contextualisation

III.1 L'entreprise

Le GIE GEOMETHANE regroupe à parts égales STORENGY (filiale à 100% d'Engie, spécialisée dans le stockage souterrain de gaz naturel) et GEOSUD (groupement de CNP assurance à 98% et de GEOSTOCK à 2%, groupe d'ingénierie international spécialisé dans les stockages souterrains).

Le site emploie 35 salariés.

L'exploitation et la maintenance des installations du site de Manosque sont confiées à STORENGY, qui exploite par ailleurs de nombreux stockages souterrains de gaz en France.

GEOSTOCK fournit une assistance à l'exploitation et assure la gestion du groupement.

STORENGY, réalise au sein du « groupement Salins » la commercialisation des capacités de stockage.

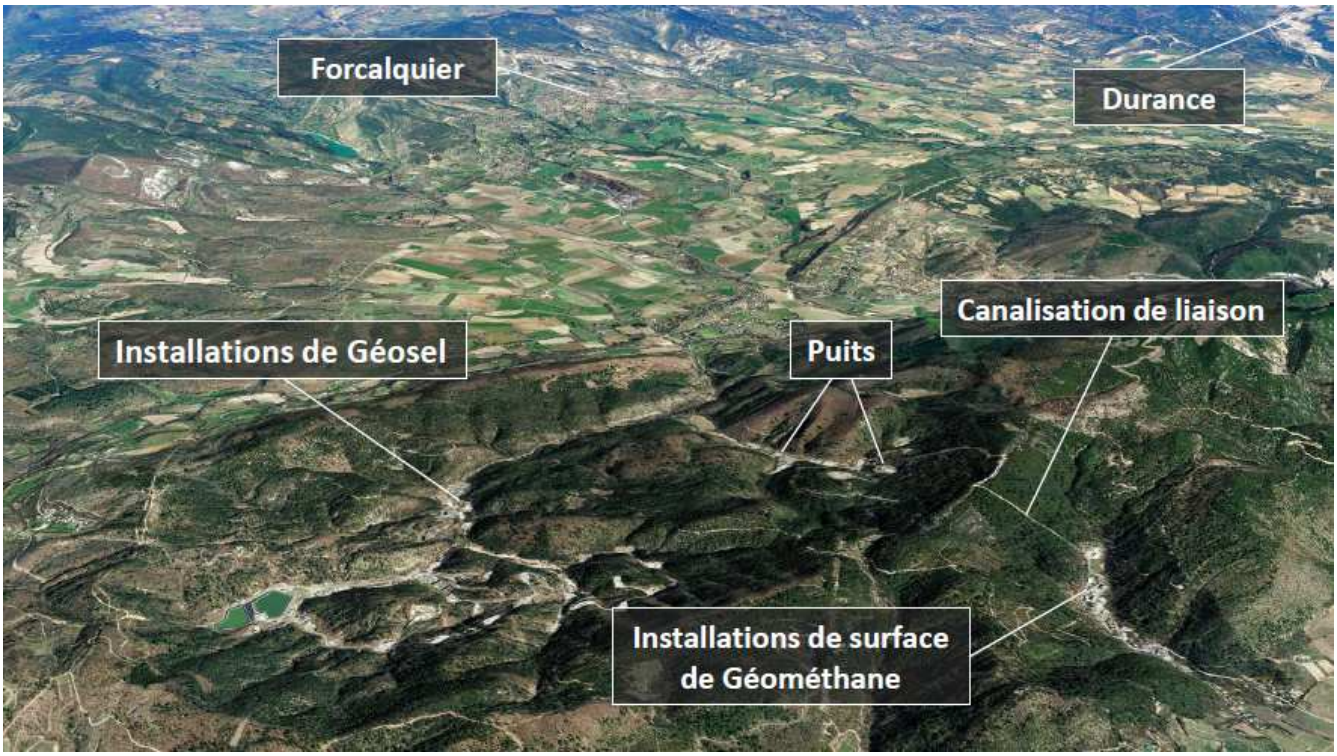

Figure 1 : Situation géographique du site (Source : GEOMETHANE)

III.2 L'installation

III.2.1 Le fonctionnement

Le centre de stockage souterrain du GIE GEOMETHANE est implanté sur les communes de Manosque et Dauphin (Alpes-de-Haute-Provence). Il est constitué de neuf cavités salines.

Une cavité saline est une cavité artificielle creusée par dissolution dans une roche sédimentaire composé de sel gemme. Ces cavités sont situées à grande profondeur (de l'ordre du millier de mètre). Le sel gemme est naturellement étanche au gaz naturel et aux hydrocarbures. Les cavités ont été initialement creusées par GEOSEL pour le stockage d'hydrocarbures liquides. Elles ont été par la suite adaptées pour le stockage de gaz naturel. La mise en gaz de la première cavité a eu lieu en 1993.

Sur les neuf cavités creusées, seulement 7 sont actuellement en service. Le volume total des cavités salines du site équivaut à 2,7M m^3, pour une pression de stockage de 200 bars. Enfin, la capacité de soutirage de pointe est équivalente à la consommation de la région sud en hiver.

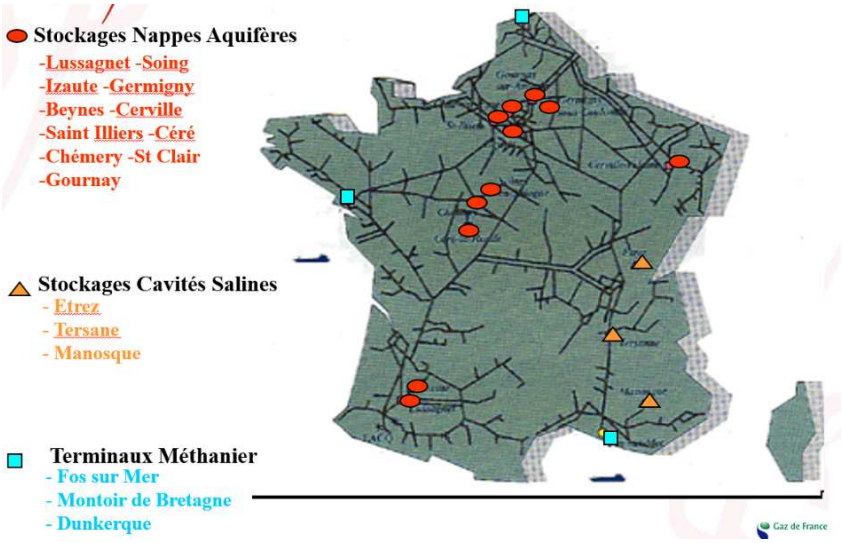

Figure 2 : Les stockages de gaz naturel sur le territoire (source : gaz de France)

Le stockage souterrain de Manosque se compose :

- D'une station centrale (site de Gaude),
- D'un site de stockage excentré (site de Gontard) constitué des 9 cavités (et têtes de puits) et d'un site de regroupement,
- De deux tuyauteries enterrées (dorsales) de diamètre nominal 200 et 750 mm reliant la station centrale et le site de regroupement.

L'objet de l'installation est de permettre le stockage du gaz en période de faible consommation et de le restituer au réseau en période de pointe de consommation. Il est également de constituer une réserve stratégique sur le sol national utilisable en cas de rupture ou de difficultés d'approvisionnement.

Ainsi, le site de Manosque permet le stockage d'environ les deux tiers de la consommation annuelle d'une ville comme Marseille.

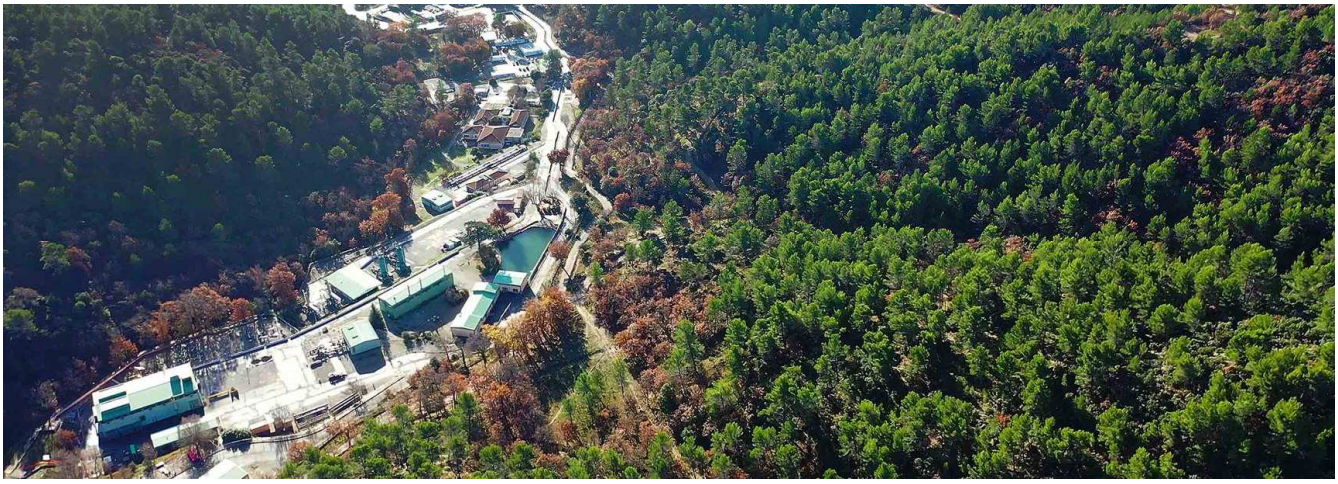

Figure 3 : Site de Gaude

L'exploitation des installations est réalisée sous deux configurations :

- L'injection correspond au remplissage des puits avec le gaz disponible sur le réseau de transport. La pression du réseau étant inférieure à celle du réservoir, il est nécessaire de comprimer le gaz pour l'injecter dans les cavités ;
- Le soutirage correspond à l'alimentation du réseau de transport par le gaz disponible dans les cavités par l'intermédiaire des dorsales.

Figure 4 : Coupe schématique d'un stockage de gaz naturel en cavités salines

Pendant le soutirage, le gaz avant injection dans le réseau fait l'objet des traitements suivants :

- Élimination de l'eau sous forme liquide par les séparateurs des puits et les points bas des collecteurs,
- Réchauffage et détente,
- Élimination de l'eau sous forme de vapeur et de fines particules (tours de déshydratation),
- Odorisation d'appoint au THT[1], si nécessaire.

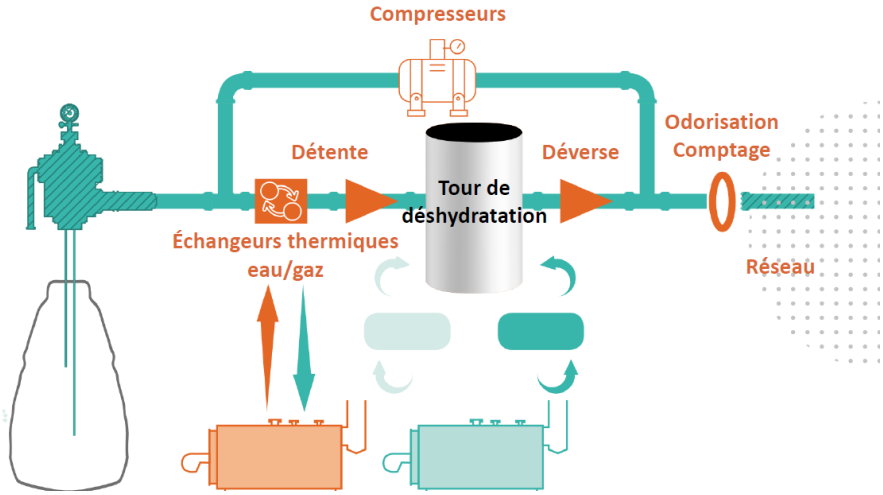

Figure 5 : Schéma général des installations

[1] Tétrahydrothiophène : Le THT est un gaz odorant, utilisé comme additif en très faible quantité au gaz naturel commercialisé, qui, sans lui, resterait inodore.

III.2.2 Le dispositif de contrôle commande

En matière de pilotage et de sécurité, le site est découpé autour d'ateliers, entités fonctionnelles correspondant à une grande fonctionnalité du site ou à une localisation. Dans le cadre de l'évènement du 1er janvier, trois ateliers sont concernés :

- La partie traitement du gaz,
- La partie compression,
- La partie station centrale.

Le système de contrôle-commande est réparti sur deux entités séparées :

- Le système de commande,
- Le système de sécurité.

Le système de commande est dédié uniquement au pilotage de l'installation.

Le système de sécurité gère quant à lui la sécurité de l'installation et notamment les séquences de mise en sécurité. Les deux systèmes ne peuvent dialoguer qu'au-travers d'une interface monodirectionnelle qui ne permet l'échange que dans le sens sécurité vers commande.

Les séquences de mise en sécurité sont de deux natures :

- Les MSA : mise en sécurité atelier qui conduit à l'arrêt des machines et à l'isolement (réseau de gaz de l'atelier),
- La MSU : mise en sécurité ultime de l'atelier qui en plus d'une MSA comprend la mise à l'évent du gaz contenu dans l'ensemble de l'atelier entrainant sa décompression. Dans le cadre d'une MSU, la décompression n'a lieu que dans le cas où l'isolement est confirmé.

Figure 6 : Event de décompression

Figure 7 : Vanne d'isolement

Le système de sécurité repose sur un système à haute disponibilité constitué d'automates programmables et de calculateurs de supervision. Chacun des ateliers est doté d'un automate de sécurité (S7-400 Siemens) qui comprend une structure complétement redondante :

- 1 rack accueillant l'ensemble des cartes spécialisées,
- 2 CPU,
- 4 cartes réseaux Ethernet (2 par UC) dédiées à la communication inter-automates,
- Des entrées/sorties déportées (Profibus Siemens).

Les communications inter-automates sont bidirectionnelles et concernent soit des commandes manuelles de mise en sécurité, soit des indications en matière de détection incendie.

Des informations d'état (compte-rendu des mises en sécurité) sont également échangées.

Ces communications se font au travers de deux réseaux redondants.

Le choix d'Ethernet (avec une surcouche propriétaire Siemens) a été fait pour l'ensemble de ces échanges d'informations. Il est néanmoins à noter que l'échange d'information entre le pupitre situé en salle de contrôle et l'automate de la station est réalisé via des entrées/sorties déportées (Profibus). Le schéma de connexion des automates est reproduit de manière simplifiée ci-dessous.

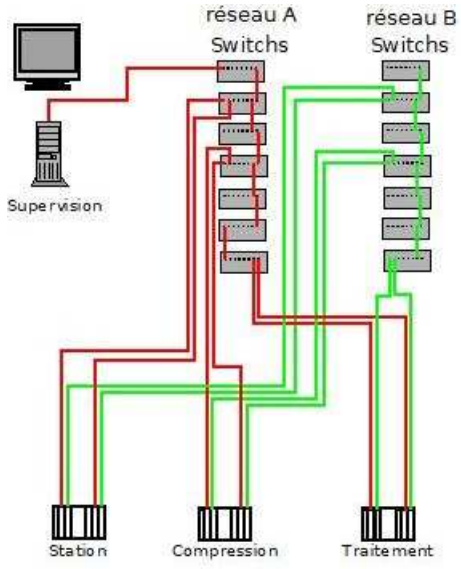

Figure 8 : Schéma réseau de sécurité

Le réseau comprend outre les automates, des équipements actifs (switchs[2], répéteurs, adaptateurs fibre optique) qui, en cas de défaut, peuvent rendre dans certains cas inopérante la détection par la carte réseau d'un problème physique. Pour en tenir compte, la détection d'un problème réseau est donc à la fois physique mais également basée sur un time-out[3] de réception. Ainsi, au sein du traitement de

[2] Un commutateur réseau (en anglais switch), est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication et qui permet de créer des circuits virtuels. La commutation est un des deux modes de transport de trame au sein des réseaux informatiques et de communication, l'autre étant le routage.

[3] Time-out : temporisation au-delà de laquelle le système en l'absence de réponse engage une séquence de repli ou de mise en sécurité.

l'automate, une détection d'un time-out de liaison (par la carte réseau) entrainera le déclenchement d'une séquence particulière de l'automate.

Figure 9 : Switch

La perte de communication entraine pour l'automate qui l'a détectée une MSA et/ou une MSU en fonction de l'atelier.

IV. Compte-rendu des investigations menées

IV.1 Reconnaissance de terrain

Au regard de l'information tardive du BEA-RI, plus de deux mois après l'évènement et de la nature de ce dernier, les investigations ont été menées initialement par des échanges avec l'exploitant. Plusieurs réunions ont été organisées avec celui-ci puis avec les référents techniques de chez Siemens, fabriquant des automates.

Les inspecteurs du BEA-RI se sont ensuite déplacés sur site le vendredi 9 juillet 2021.

V. Déroulement de l'évènement

V.1 Déclenchement de l'évènement

Avant le déclenchement de l'évènement, un premier basculement de réseau a eu lieu du réseau B vers le réseau A (cf. figure 8). La date et l'heure de cette bascule n'ont pu être établies.

A 4h34, l'automate de sécurité du traitement ne reçoit plus (time-out liaison) l'automate de la station. La bascule du réseau A au réseau B n'a pas lieu. L'automate du traitement lance la séquence de MSU de l'atelier et notamment la décompression et la mise à l'atmosphère du gaz. L'ensemble de ces opérations est remonté via le réseau et tracé.

A 6h35, la même séquence se déclenche sur l'automate de compression avec les mêmes conséquences.

A 9h56, c'est l'automate de la station qui ne reçoit plus les messages provenant des deux autres automates et déclenche la MSA de la station (pas de MSU associée sur la station).

Le site étant en sécurité, les équipes de maintenance interviennent sur site vers 10h pour analyser les disfonctionnements et les résoudre. Ils quittent le site vers 13h10 après avoir réarmé l'ensemble des ateliers.

A 13h28, à nouveau, l'automate de la station ne reçoit plus les messages des automates de la compression et du traitement. La bascule du réseau A au réseau B n'a pas lieu. L'automate de la station déclenche une séquence de MSA. Cette information est correctement transmise aux deux autres automates qui déclenchent également une séquence de MSA. L'ensemble des trois MSA est correctement retransmis à la supervision et tracé.

A 14h06, l'automate de traitement ne recevant plus l'automate de la station lance la séquence de MSU de l'atelier et notamment la décompression et la mise à l'atmosphère du gaz. L'ensemble de ces opérations est remonté via le réseau et tracé.

A 19h59, la même séquence se déclenche sur l'automate de compression avec les mêmes conséquences.

Au vu de l'ensemble des incidents sur la journée, la décision est prise d'arrêter tout transfert de gaz pour investigation.

V.2 L'intervention des secours publics

Au regard des conséquences de l'évènement (utilisation des dispositifs de sécurité prévus à cet effet), il n'y a pas eu de demande d'intervention des secours publics.

VI. Conclusions sur le scenario de l'événement

VI.1 Scénario

Avant l'évènement, une bascule entre les réseaux a eu lieu. Sur le réseau en fonction, un équipement actif (switch) connait des pertes de fonctionnement aléatoires. A 4h34, les pertes de trames sont suffisamment longues pour dépasser le temps de time-out fixé dans le programme de l'automate de traitement.

La bascule du réseau n'a pas lieu malgré la détection du time-out.

L'automate de traitement comprend le plus d'équipements actifs entre lui et l'automate de station. L'automate du traitement déclenche, conformément à sa programmation, la MSA puis la MSU de l'atelier ce qui comprend la décompression de l'atelier et génère le premier rejet aux évents de gaz.

A ce stade, les communications sont encore suffisamment fonctionnelles pour permettre à l'automate du traitement de rendre compte de la séquence de sécurité à l'automate de la station ainsi qu'au logiciel de supervision. Le stockage n'étant pas sollicité (ni entrée ni sortie de gaz) et la MSU s'étant correctement déroulée, il n'y a pas d'intervention immédiate de maintenance.

A 6h35, le même scénario se déroule, mais cette fois ci, c'est l'automate de compression qui détecte la perte des trames.

A 9h56, c'est l'automate de la station qui constate le time-out et déclenche une MSA (isolation et arrêt sans décompression associée).

L'astreinte maintenance intervient vers 10h mais rien ne lui permet de diagnostiquer la problématique de réseau que ce soit l'absence de bascule des réseaux ni la panne intermittente liée aux switchs défectueux. En l'absence de défauts constatables, elle procède au redémarrage des installations.

A 13h28, l'automate de station détecte de nouveau une impossibilité de réception dans les temps et déclenche, en l'absence d'une bascule de réseau, une MSA de la station qui entraine la MSA de la compression et du traitement sans émission de gaz à l'atmosphère.

Successivement, à 14h06 et à 19h59, le time-out réseau se déclenche sur les automates de traitement puis de compression entrainant la MSU et donc le rejet de gaz aux évents.

La cause initiale est le dysfonctionnement intermittent d'un switch entrainant de manière aléatoire la détection d'un time-out sur les différents automates du réseau de sécurité. Est à ranger également au rang de cause initiale, l'absence de bascule entre les réseaux redondants lors de la détection de ces time-out.

VI.2 Facteurs contributifs

VI.2.1 La conception initiale et la gestion des modifications

Le réseau tel que conçu initialement et dans son évolution, permet de relier l'ensemble des locaux techniques entrainant la multiplication des équipements actifs : 7 switchs sont présents au total alors que seulement 4 d'entre eux sont utilisés pour relier un équipement de contrôle (automate, serveur supervision). L'évolution technique du matériel et de sa mise en place n'a pas donné lieu à une reconfiguration du réseau et a maintenu en place des équipements actifs inutiles susceptibles de pannes. Ainsi, le switch défectueux par exemple ne sert plus que de répéteur sans que des problèmes de distance entre équipement rendent sa présence indispensable.
Dans la même idée, lors de la conception initiale et/ou lors des évolutions, le choix d'un réseau de « haut niveau » type Ethernet pour véhiculer de l'information en temps réel aurait pu être comparé par rapport à des réseaux de type capteur/actionneur avec des protocoles de sécurité plus adaptés à ce type de trafic.

VI.2.2 La maintenance logicielle des équipements

L'absence de bascule entre les deux réseaux est due aux différences entre les versions logicielles des cartes réseaux. Ce point a été confirmé par le fournisseur des équipements. La différence entre ces versions logicielles était soit initiale soit liée à des opérations de maintenance (changement de cartes). Il n'a pas été possible de retracer le moment ou des versions différentes ont été mises en place.

VI.2.3 Le manque de possibilité de diagnostic réseau

Le système tel qu'il est mis en place ne permet pas :

- D'indiquer et/ou de tracer des évènements de type indisponibilité de la redondance. A priori, en amont de l'évènement, l'indisponibilité de cette redondance causée par la différence entre les micros logiciels des cartes réseau, est survenue sans qu'aucun élément n'ait fait l'objet d'une remontée ni à la maintenance ni aux opérateurs,
- L'état même des réseaux (disponibilité /indisponibilité/ intermittent) ne fait pas non plus l'objet d'une surveillance.

De ce fait, aucune préalerte sur l'état du switch ni aucun élément de diagnostic n'étaient disponibles pour les opérateurs pour prévenir les deux premières MSU ni pour empêcher les deux suivantes en cours

d'après-midi. De même, la durée des investigations et par conséquence la durée d'indisponibilité du stockage aurait pu être réduite avec les moyens de traçabilité et diagnostic ad hoc.

VI.2.4 La testabilité de la redondance réseau

Il n'existait pas, avant l'évènement, de procédure de test de la redondance des réseaux réalisée de manière régulière. La mise en place de telles procédures auraient permis d'identifier notamment les problèmes de bascule entre réseaux.

VII. Enseignements de sécurité

La conception et l'évolution dans le temps des réseaux utilisés dans l'architecture de sécurité doit être menée en privilégiant la simplicité et l'adaptation du type de réseau à la nature des informations qui y transitent :

- A la phase de conception, l'utilisation d'un réseau d'entrées/sorties déportées sera privilégiée notamment pour les commandes tout ou rien (pupitre de contrôle notamment) ;
- Lors des évolutions, une nouvelle analyse complète de l'architecture réseau notamment devrait identifier les équipements inutilisés.

L'examen attentif de la documentation du constructeur a permis de relever que pour garantir la redondance de la communication les versions du logiciel constructeur des différents équipements doivent être identiques. En matière de système de contrôle commande (et particulièrement en matière d'automate programmable), les systèmes, une fois installés et testés, font rarement l'objet de remise à niveau du logiciel constructeur. Par contre, le remplacement de carte électronique en cas de panne est une pratique courante. Dans ce cas, il faut être à même de garantir que l'ensemble des équipements connectés restent au même niveau en matière de version. Il est à noter que la mise en place d'un matériel de version différente n'entraine pas de dysfonctionnement apparent.

La mise en place d'un suivi de maintenance intégrant cette contrainte par l'exploitant et l'émission par le constructeur d'une information sous forme d'informations ciblées et diffusées aux exploitants (par abonnement par exemple) indiquant les modifications de versions, leurs impacts et leurs compatibilités constituerait une bonne pratique à encourager.

VIII. Recommandation de sécurité

VIII.1 A destination de l'exploitant qui accueille ce type d'équipement

Outre les enseignements de sécurité formulés ci-dessus, le BEA-RI formule les recommandations de sécurité suivantes à destination de l'exploitant :

VIII.1.1 En matière de gestion de maintenance

S'assurer, sur l'ensemble des sites de l'exploitant, de la compatibilité des versions des logiciels des automates de sécurité et mettre en place les procédures de gestion de maintenance permettant de garantir dans le temps cette compatibilité.

VIII.1.2 En matière de test et de diagnostic

Rendre les équipements réseaux testables et diagnosticables :
L'essentiel du traitement des défauts des réseaux de capteurs/actionneurs repose sur le logiciel des coupleurs de communication.
Inversement, les réseaux de plus haut niveau (type Ethernet) traitent les défauts à la fois au niveau des micro-logiciels embarqués et de l'applicatif développé spécifiquement pour l'installation y compris pour des paramètres très sensibles (temps de time-out par exemple).
Dans ce cas, la détermination de la nature du défaut est très délicate surtout si ce dernier est intermittent. De ce fait, l'échange de données de sécurité, les tests initiaux et les tests réguliers en fonctionnement sont une nécessité.
De même, en cas de mise en défaut, les personnels de maintenance doivent pouvoir, soit directement sur le système soit au-travers d'équipements spécifiques, disposer des moyens de diagnostic et accéder à l'historique du défaut.

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE

Liberté
Égalité
Fraternité

BEA-RI
Risques industriels

Bureau d'enquêtes et d'Analyses sur les Risques Industriels

MTE / CGEDD / BEA-RI
Tour Séquoïa
92055 La Défense Cedex

+33 1 40 81 21 22
bea-ri.cgedd@developpement-durable.gouv.fr

http://www.cgedd.developpement-durable.gouv.fr/bea-ri-r549.html