



Méthaniseurs :
Des procédés peu sûrs

BROUZILS Sentinelles



Santé Sécurité Sérénité



Eric EULA,
Président de BRZ4S, CNVM CH PDL

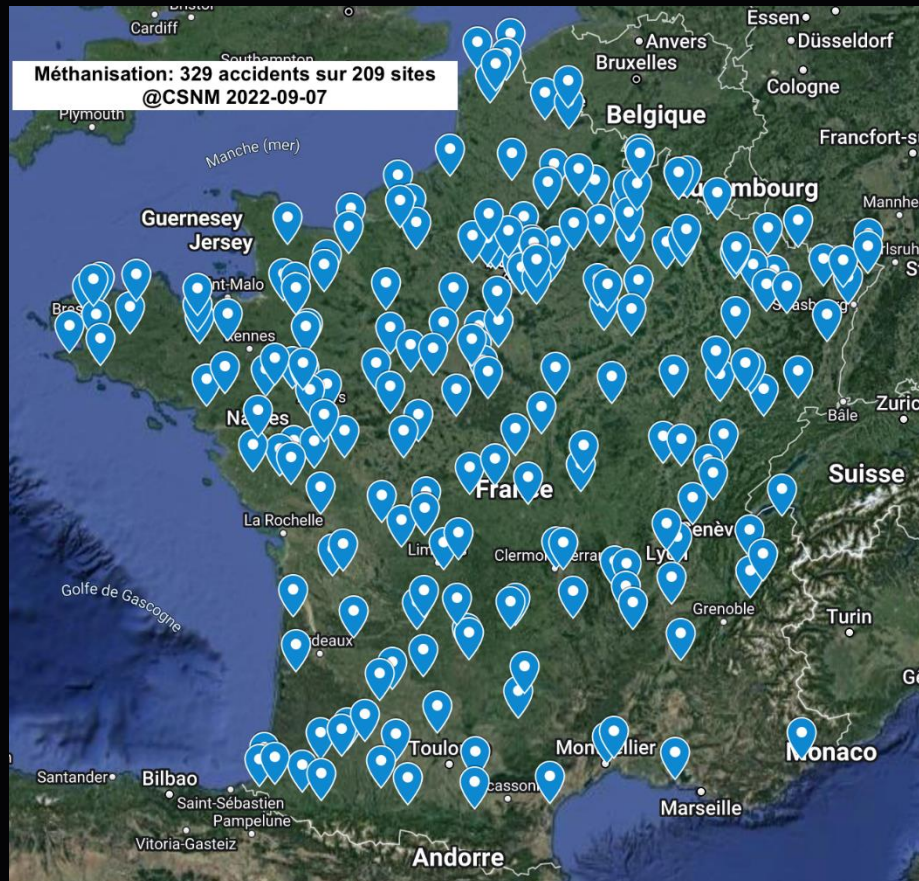
Membre du Bureau du CNVM CH

Ingénieur Applications
Automatisme & Informatique Industrielle (1982)

Consultant Qualité Logiciel & Sûreté de
fonctionnement

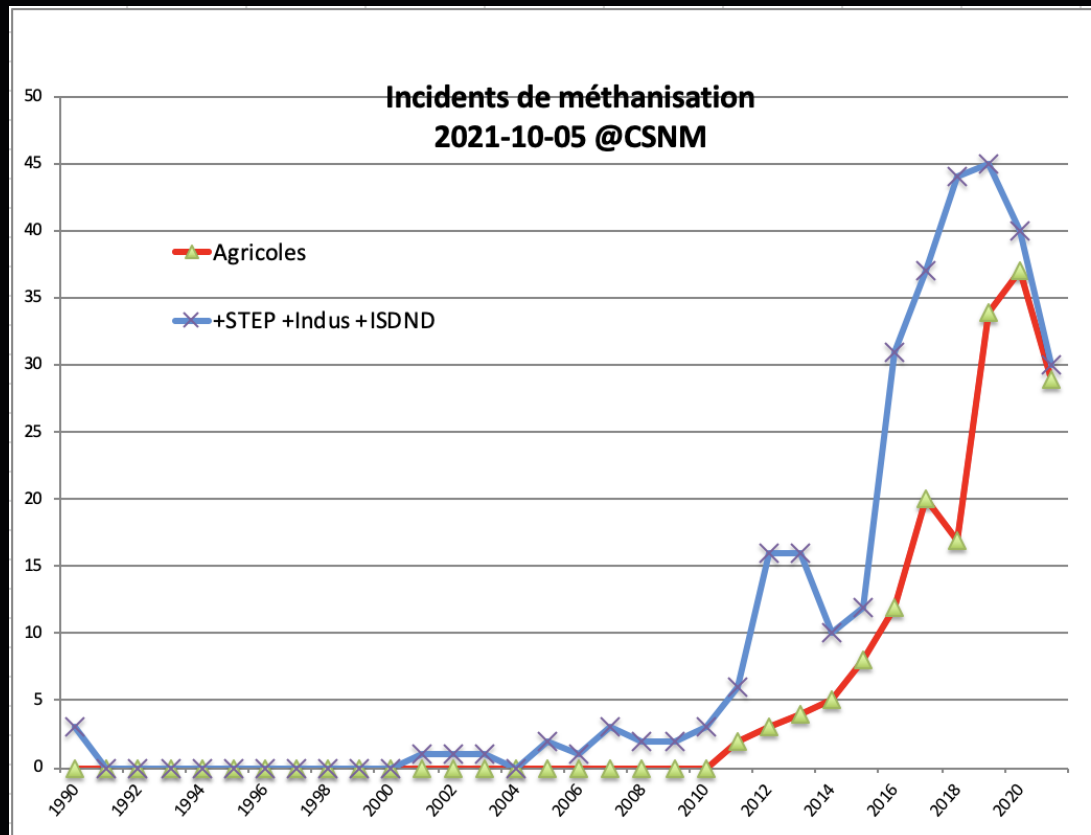
Des statistiques alarmantes

- Au 7/9/2022, 329 accidents sur 209 sites dont 12 accidents sur les 7 derniers mois



Des statistiques alarmantes

- Un taux de croissance découplé du taux de croissance du nb de méthaniseurs et largement supérieur (x 1 // x 6)

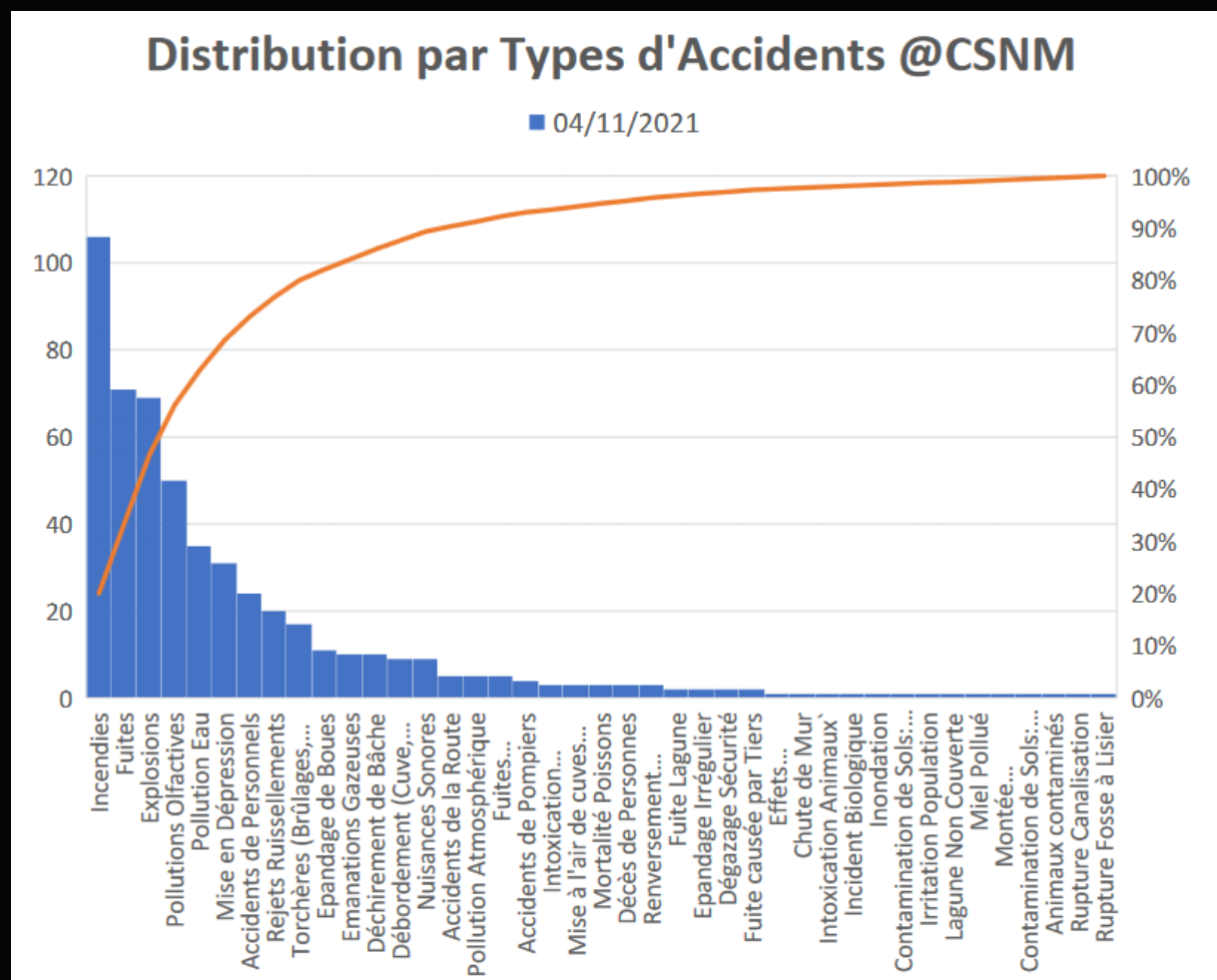


Vous avez dit ‘fiabilité’ ???

- Rapporté au nb de méthaniseurs recensés (sources min.) à ce jour, 17 % (fourchette basse) des sites ont été l'objet d'accidents en tous genres !
- Ce chiffre attendu “socialement acceptable”, rapporté au nombre d'installations ICPE de type « chimie/gaz » correspondrait à 2776 accidents en 20 ans ... Toujours “raisonnablement sûr” // au reste de l'industrie ???



Des statistiques alarmantes



Nature des atteintes



Nature des atteintes



Eaux

Sols



Climat



Air



Population

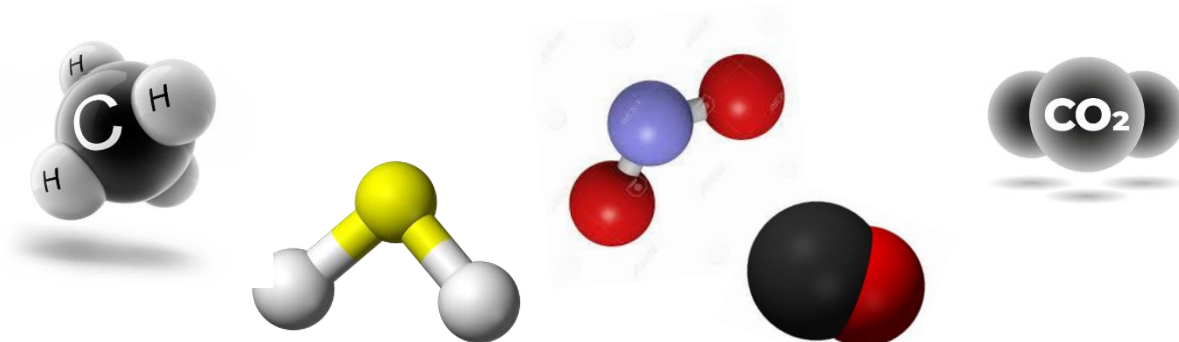


Quelles causes de danger ?



En grande majorité, des gaz et des liquides

- CH₄ [Méthane], gaz inodore, incolore, hautement explosif, asphyxiant, un PRG de 80
- H₂S [Hydrogène sulfuré], gaz inodore, incolore. Son 1er danger : neuro-toxique
- NoX [Oxydes d'azote], gaz inodores, incolores. Leur dangers : sanitaires, PRG 40 à 300
- CO₂ [Dioxyde de carbone], gaz inodore, incolore. Ses dangers : anoxique, PRG
- CO [Monoxyde de carbone], produit lors des combustions incomplètes durant les incendies, inodore, incolore. Ses dangers : anoxique, PRG

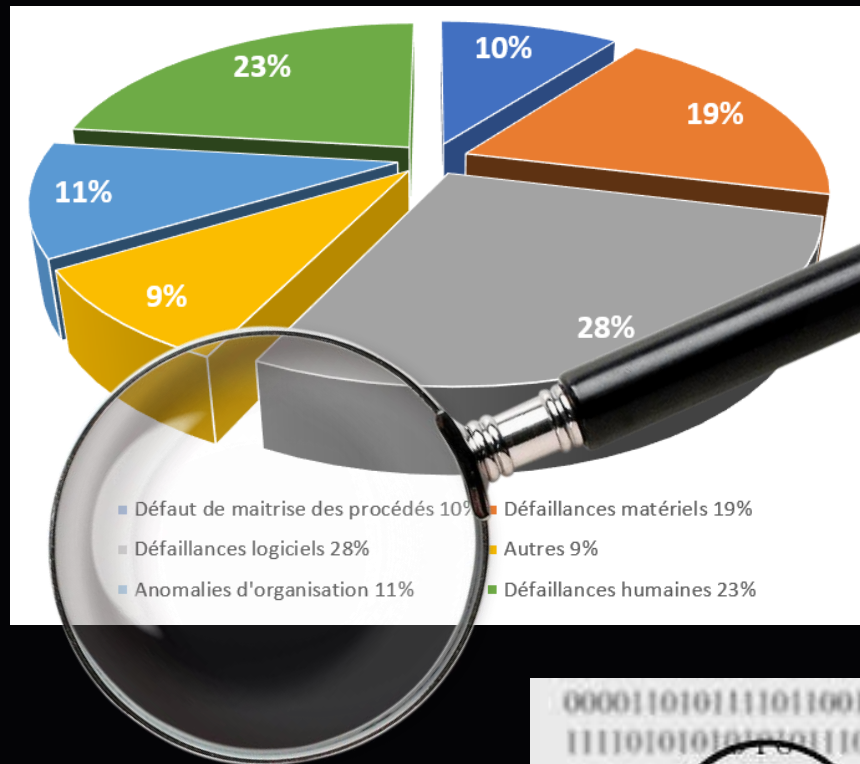


En grande majorité, des gazs et des liquides

- Digestats : liquides à forte concentration d'azote. Leurs dangers : déséquilibre du PH, eutrophisation, potabilité



SURETE DE FONCTIONNEMENT



Sûreté de fonctionnement

- La sûreté de fonctionnement est l'aptitude d'un système à remplir une ou plusieurs fonctions requises dans des conditions données ; elle englobe principalement quatre composantes
 - la fiabilité (je fais exactement ce que je dois faire)
 - la maintenabilité (je suis documenté et accessible)
 - la disponibilité (je le fais 24/24)
 - la sécurité (je le fais sans risques ni dangers)
- La connaissance de cette aptitude à remplir une ou plusieurs fonctions permet aux utilisateurs du système de placer une confiance justifiée dans le service qu'il leur assure
- Par extension, la sûreté de fonctionnement désigne également l'étude de cette aptitude et peut ainsi être considérée comme la « science des défaillances et des pannes ».

Sûreté de fonctionnement

- NON ! Un méthaniseur ne se résume pas à un « gros composteur ». C'est un procédé physico-chimique qui exige que l'on pilote et maîtrise ses réactions en toutes circonstances et ce sans que la chance ou le hasard y aient leur place
- Stations de capa inf. à 100 T/j : pas de Plan de Prévention des Risques Technologiques
- Auto-certification des constructeurs/intégrateurs aux règles de l'art ("dormez tranquilles, faites moi confiance ...")
- Quelles différences RISQUES entre une station 90T/j et une 110 T/J ?

Maitrise du risque

Schématiquement, “maitriser” le risque consiste à

- croiser la probabilité qu’une défaillance (et surtout DES défaillances) apparaisse avec le degré de gravité qu’elle va induire
- Et d’y poser des “barrières” pour en minimiser
 - soit l’occurrence
 - soit la gravité
 - soient les deux



Maitrise du risque

Ceci implique

- une parfaite connaissance du procédé
- une parfaite connaissance des composants matériels et logiciels
- de pouvoir imaginer et modéliser des enchainements improbables de défaillances (cascading)

C'est un des plus gros postes de coût "matière grise"



Maitrise du risque

- Recenser tous les risques (analyse de risque, étude de danger, AMDEC, HAZOP, ...)
- Identifier, risque par risque, les moyens de réduction mis en place (les barrières de sécurité)
- Déterminer le risque tolérable cible pour chaque risque (législation, responsabilités du site, ...)
- Définir et spécifier les “pare-risques”, leurs finalités
- Déterminer (et obtenir) la réduction de risque que les “pare-risques” sont censées viser



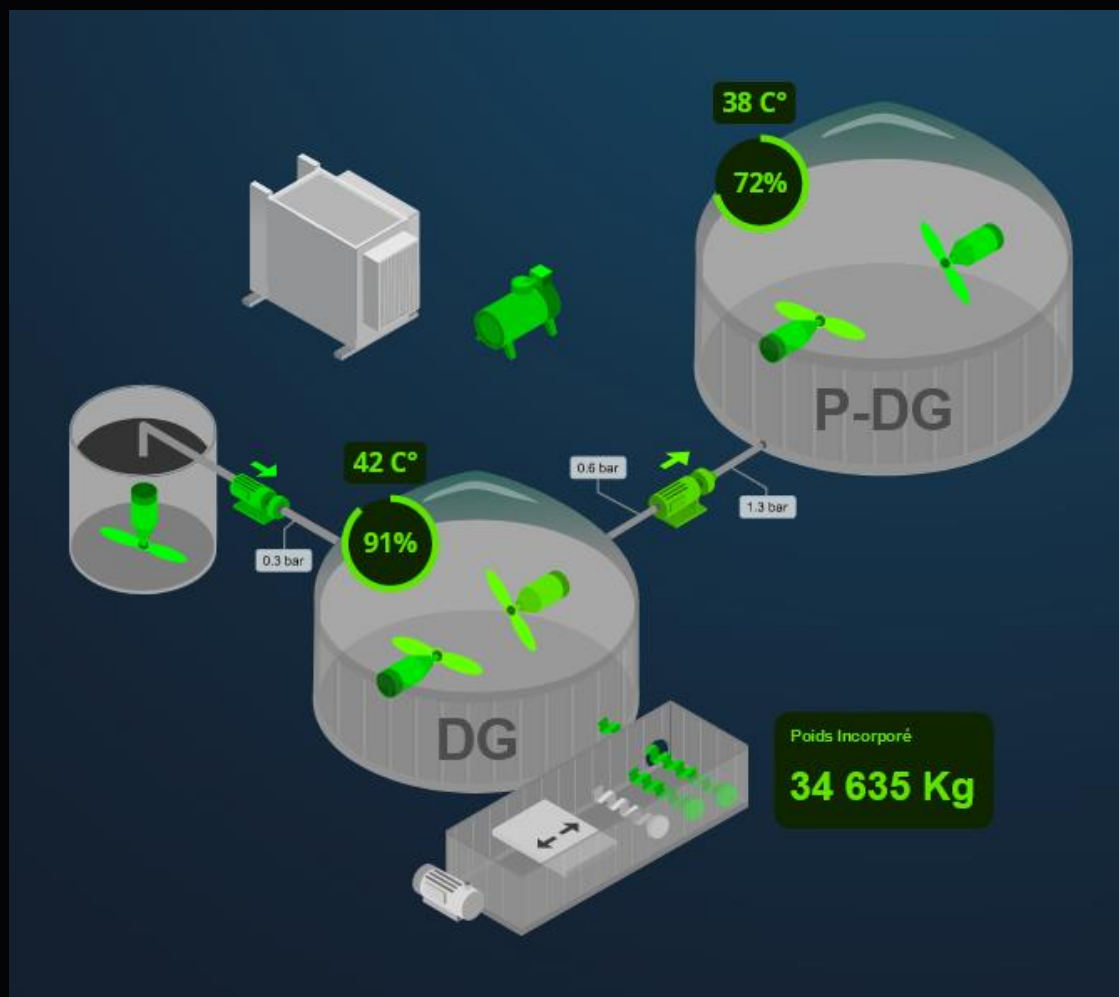
Maitrise du risque

SIL (« Safety Integrity Level ») : Niveau d'intégrité de sécurité d'une Fonction Intégrée de Sécurité)

- SIL 1 : réduction du risque par un facteur >10
- SIL 2 : réduction du risque par un facteur >100
- SIL 3 : réduction du risque par un facteur $>1\ 000$
- SIL 4 : réduction du risque par un facteur $>10\ 000$



Composantes d'une conduite de procédé

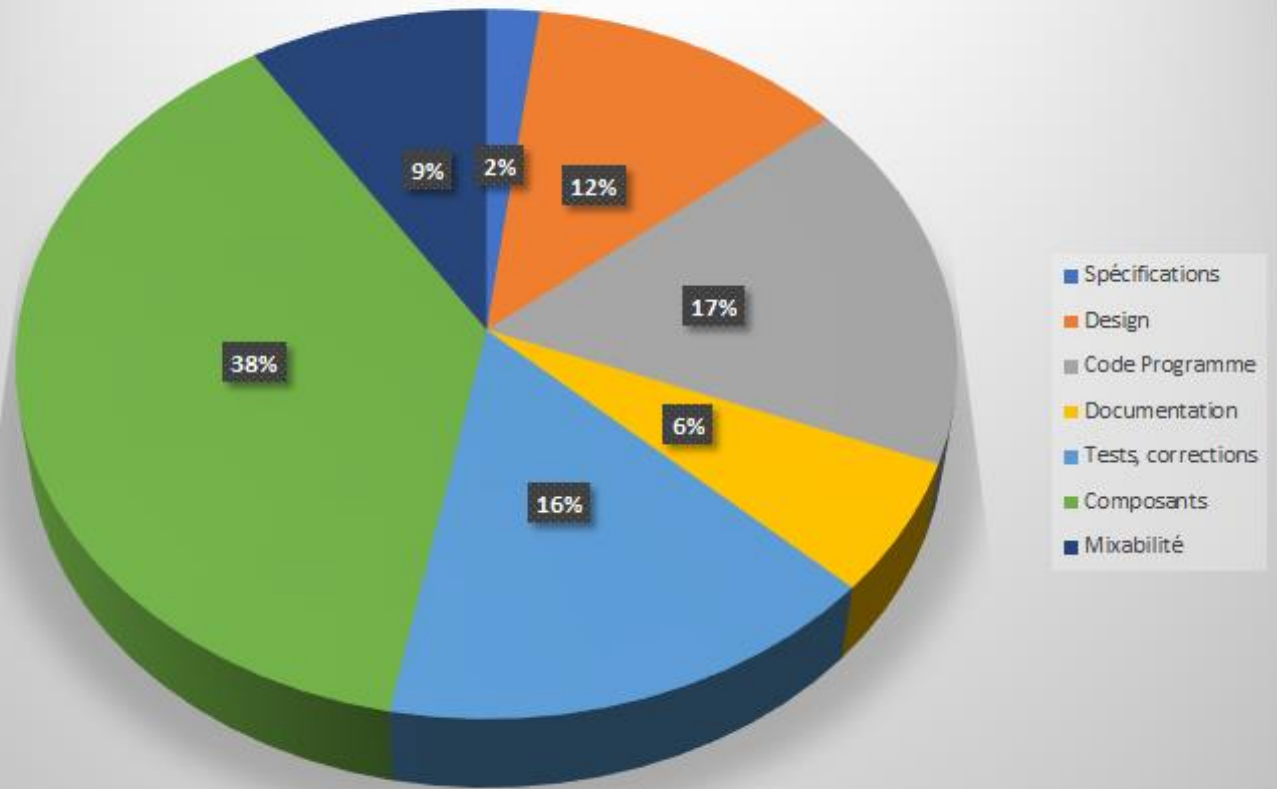


Composantes d'une conduite de procédé

- Capteurs de grandeurs physico-chimiques (température, pression, niveau, débit, concentration, viscosité, turbidité, conductivité, Ph, etc)
- Automates programmables industriels (+ logiciel)
- PC de conduite / supervision (+ logiciel)
- Actionneurs (vannes, moteurs, vérins, etc)

A tous ces niveaux peuvent apparaître des failles critiques de concept ou de mise en oeuvre

Causes de disfonctionnement Logiciel API



SIEMENS 2019

- US Chemical Safety and Hazard Investigation Board (CSB): erreurs de programmation identifiées comme étant l'une des principales causes des accidents industriels graves aux États-Unis
- Selon une étude menée par Siemens, environ 60% des incidents de sécurité industrielle sont causés par des erreurs de programmation.



ex. emblématique : KASTELLIN (29, 2020, ENGIE)

- Loi de Murphy ???
- Modèle de Reason ... !!!

ex. emblématique : KASTELLIN (29, 2020, ENGIE)

t0 - Erreur de manipulation Opérateur

t1 - Pas de filtre logiciel empêchant cette manip

t2 - Remplissage de la cuve digestats au delà du normal

t3 - Absence de personnel / site pour vigilance

t4 - Capteur de niveau mal placé, info non pertinente

t5 - Défaut de redondance de l'information

t6 - Défaut de code logiciel traitant l'événement

t7 - Débordement

t8 - Code logiciel du mode dégradé non codé

Débordement avéré et non maitrisable de la cuve

Pollution des nappes (180 000 personnes privées d'eau potable durant 2 semaines)

Incendie du digesteur (2.5 j pour le maitriser)

Bilan Carbone ? Perdu à jamais ! + particules fines + émanations toxiques (plastiques, peintures) = !!!!!!!!!!!!!!

La base ministérielle ARIA-BARPI regorge (quand elle est à jour) de ces “c’est la faute à pas de chance” ...



203 résultats pour la recherche "methanisation"

Home » You searched for methanisation

RECHERCHE AVANCEE Conseils d'utilisation ?

methanisation ? 🔍

☐ Combiner les termes avec un OU au lieu d'un ET

Appliquer les filtres Réinitialiser le formulaire

Critères généraux

☐ Inclure ☐ Exclure

Secteur d'activité ▼

Secteurs d'activité exclus ▼

Thématique ▼

Type de publication ? ▼

Date de publication ?

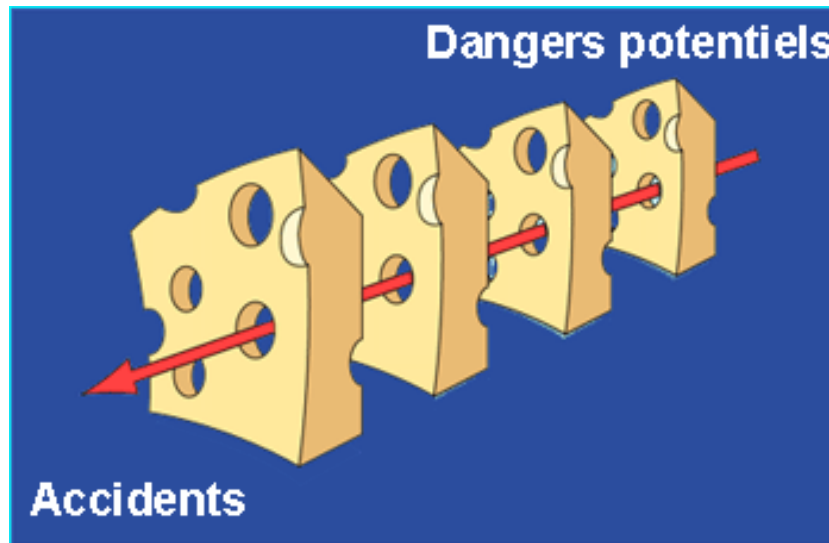
Date de début Date de fin

Critères spécifiques aux événements ?

Critères de base	Description de l'événement	Conséquences et causes
Numéro ARIA ?	Classement événement ▼	Conséquences ▼
Date de survenue ?	Type d'événement ? ▼	Echelle européenne des accidents ?
Date de début Date de fin	Phénomènes dangereux ▼	Matières dangereuses relâchées
Traduction anglaise disponible ▼	Matière(s) impliquée(s) ? ▼	0 6
Pays ▼	<input type="radio"/> Inclure <input type="radio"/> Exclure ?	Conséquences humaines et sociales
Région ▼	Classification CLP ▼	0 6
Départements ▼	Classifications CLP Exclues ▼	Conséquences environnementales
	<input type="radio"/> Inclure <input type="radio"/> Exclure ?	0 6
		Conséquences économiques
		0 6

Modèle de Reason

- Un accident est tjrs le résultat d'une accumulation de causes et d'événements isolément peu probables
- L'accident survient lorsqu'il y a conjonction des failles



Modèle du fromage suisse : les sécurités d'un système sont illustrées par une série de barrières, assimilées à des tranches de fromage. Quant à eux, les trous illustrent les défaillances dans chacune des barrières, défaillances qui varient en taille et en position dans chacune des tranches. Le système échoue lorsqu'un trou de chacune des tranches se retrouve momentanément aligné avec les autres, ce qui mène à la défaillance. Le système NE REPOND PLUS aux exigences

Le (un des) talon d'Achille

- Aujourd'hui, l'immense majorité des procédés industriels est pilotée par des systèmes reposant sur du codage logiciel. Or, ces codes logiciels sont produits par des humains dont la caractéristique première est d'être faillible (il n'existe AUCUN code logiciel exempt de défauts)
- $E=MC^2$: Errors = (Mode Code)² : la "fragilité" du code logiciel croît avec le carré du volume de code déployé
- Contrairement aux codes produits pour des systèmes logiciels courant, très peu de codes industriels (hors automobile, militaire, spatial, nucléaire, Seveso) sont soumis à des tests de robustesse poussés
- **Le vendeur est, tour à tour, prescripteur, concepteur, codeur, testeur, correcteur. Ineptie pure et dure et danger !!!**

Où sont passées les exigences IEC 61 508 ???

La norme IEC 61508 traite de la sûreté de fonctionnement des systèmes électriques, électroniques et électroniques programmables (comme l'électronique numérique et les logiciels) pour l'industrie. Régulièrement déclinée en normes spécifiques pour différents secteurs d'activité, elle est la référence en termes de safety.

Assurer la conformité d'un système à la norme IEC 61508, c'est mettre en place, dès son démarrage, une méthodologie délimitée et rigoureuse dont l'objectif est la diminution des risques à un niveau acceptable, et construire une architecture qui répond à des exigences structurelles.

À ce jour,

- Robustesse des concepts très rarement auditée
- Idem pour les spécifications de conception détaillée (par ex. code logiciel jamais audité, opaque, source majeure de criticité)
- Absence de plan qualité documenté
- **Seule l'auto-certification fait foi ... ! Ayez confiance ...**

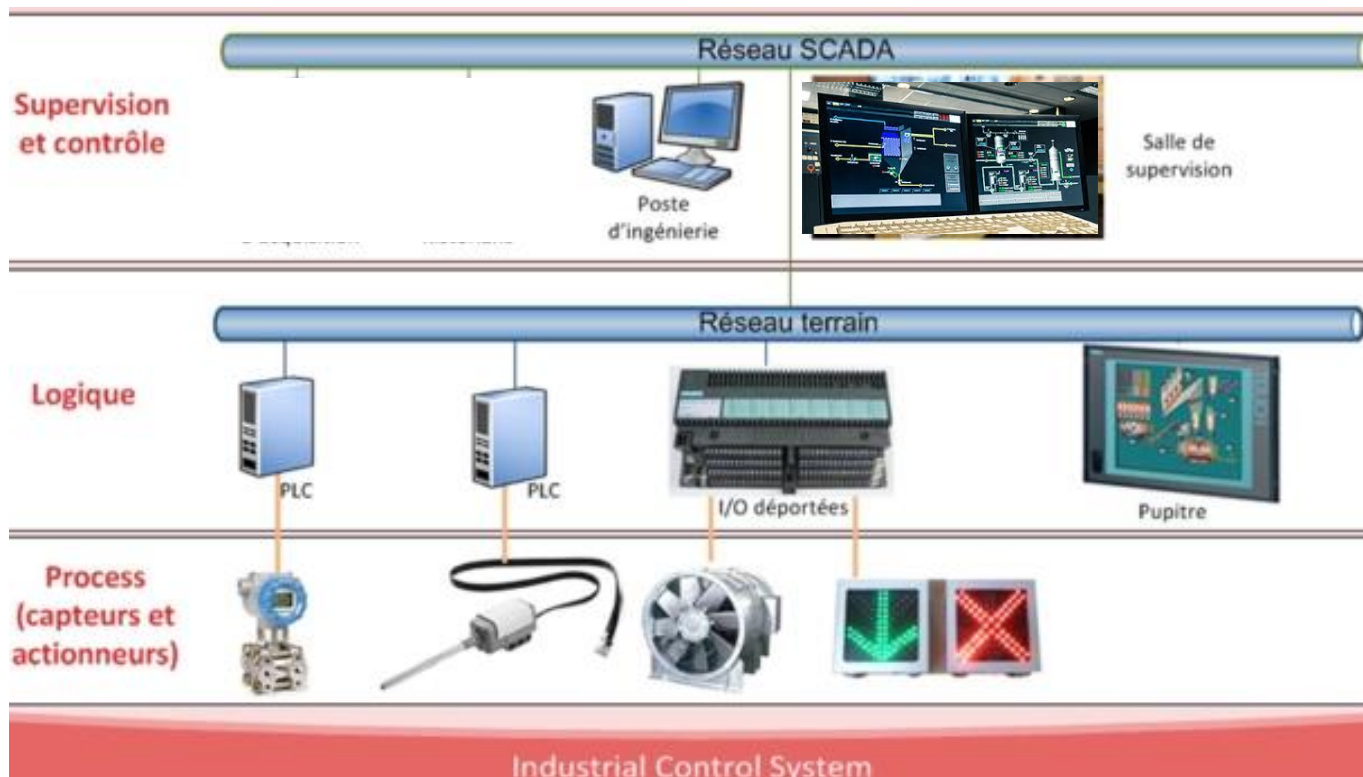
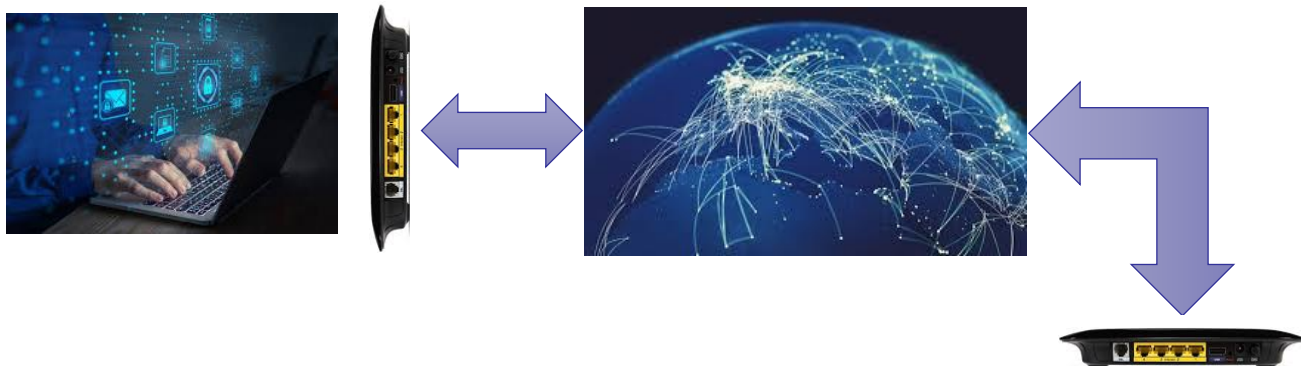
Risques Cyber



Des installations connectées à Internet

- Mises à jour des systèmes d'exploitation matériels et logiciels
- Corrections du code logiciel des automates, SNCC
- Télé-diagnostic

Comment ?



Ceci n'est pas un scénario de science-fiction



Dixit ANSSI

Une supervision à partir de systèmes de contrôle et d'acquisition de données (Supervisory Control And Data Acquisition, SCADA) existe sur la majorité des installations industrielles. Elle permet notamment de piloter et de veiller au bon fonctionnement du procédé industriel. En revanche, cette supervision n'est ni prévue ni adaptée pour la détection d'incidents de sécurité, notamment induits par l'ouverture de ces systèmes et par leur interconnexion avec des réseaux largement connectés.

Qui ?

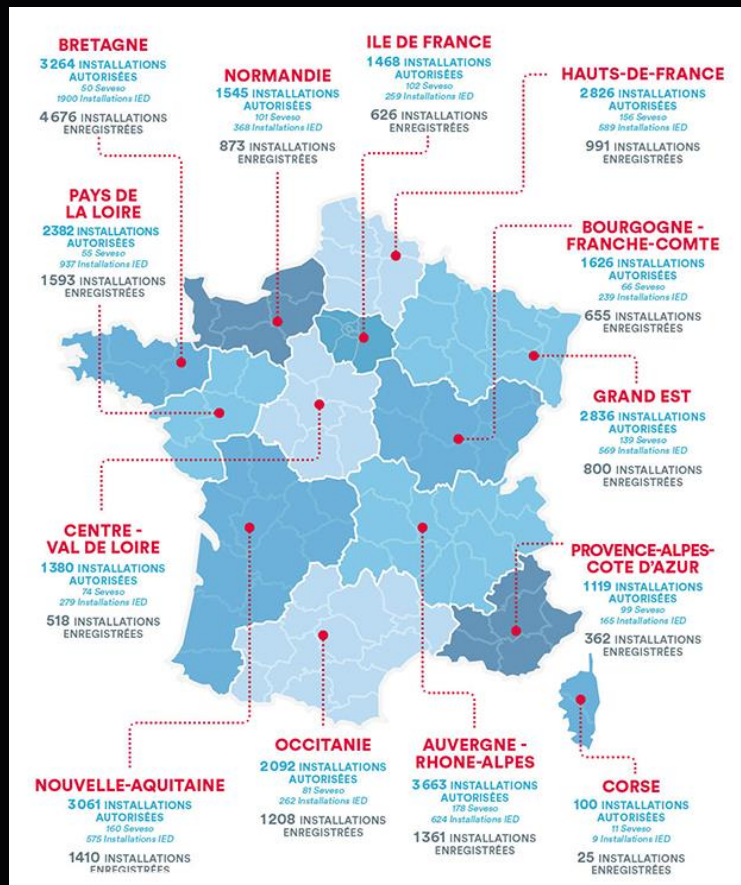
- Geeks en mal de sensations, organisations criminelles, groupes étatiques

Quels risques ?

- Plantages, paralysie
- Rançonnage
- Sabotage

Méthaniseurs : des procédés peu sûrs

Des contrôles ? Quels contrôles ???



(2018)

- 25.000 ICPE relevant du régime d'autorisation
- 1312 en Seveso I & II
- 16.000 relevant de l'enregistrement

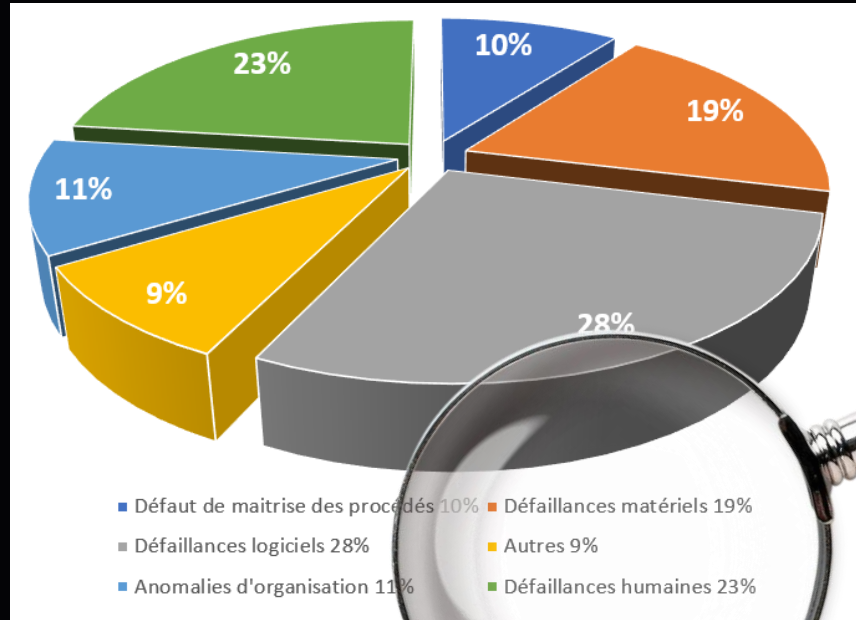
Pendant ce temps-là ...

“Les inspecteurs de l'environnement chargés des installations classées sont au nombre de 1.607 en 2018 (contre 1.627 en 2016 et 1.555 en 2014) répartis entre

- les directions régionales de l'environnement, de l'aménagement et du logement (DREAL) soit 1355*
- les directions départementales de la cohésion sociale et de la protection des populations (DDCSPP) pour les installations agricoles, soit 207*

- Selon le plan projeté ENR 2030 (10 000 méthaniseurs), un inspecteur pour 50 méthaniseurs, soit env. une inspection tous les 4 ans ...*

Compétences & Qualification



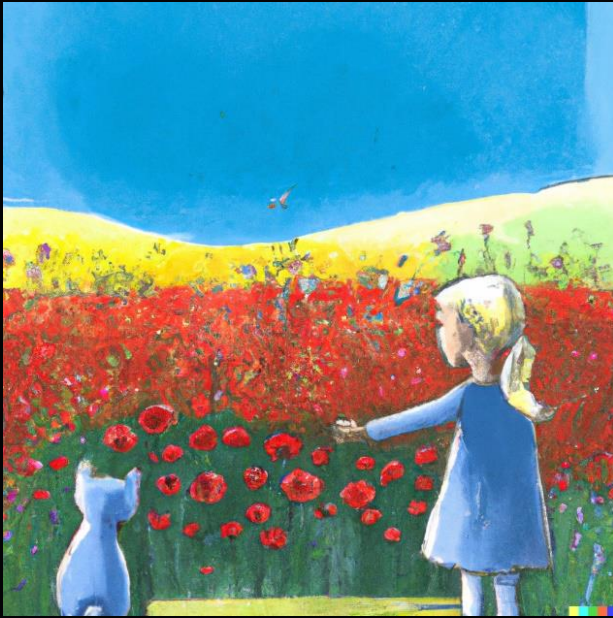
Compétences et Qualification

- Aucune formation diplômante exigée, simple formalité de présence, formation par les intégrateurs
- Aucune évaluation en conditions critiques



Si un agriculteur peut prétendre savoir réagir en toutes circonstances aux aléas techniques d'un réacteur chimique après une formation de 10 j au mieux,

alors vous et moi pouvons prétendre devenir agriculteur en 10 j ...



Un avenir plus sûr ?



- Moratoire (demandé depuis 2019)
- Retour au régime unique autorisation pour les >20t/j (sans passage possible <20t vers +20t)
- Etudes d'impact et PPRT systématiques
- Accès aux délibérés CODERST
- Accès à tous les documents relatifs à la sûreté de fonctionnement
- Exigences réglementaires à IEC 61508
- Audits et certifications ANSSI
- Des contrôles fréquents et inopinés
- Des sanctions financières dissuasives corrélées aux aides, subventions et CA
- Un circuit judiciaire & admin non entravé par les courroies préfectorales et min.
- La fin des dérogations et exceptions par décrets et le retour au débat parlementaire



En conclusion, viser l'acceptabilité impliquerait

- L'exigence tendant vers le ZERO défaut mais aussi les moyens et garanties qui s'y rattachent
- de l'information et de la transparence
- de la concertation préalable (cf convention AARHUS)
- de l'objectivité transpartisane (cf CNDP)
- un bien-fondé écologique, scientifique, économique démontré (cf CNVM CH, GREFFE, CONF PAYS, AT, etc)
- Des engagements (et non des promesses) d'avenir sûr

Nous n'héritons pas de la Terre de nos parents, nous l'empruntons à nos enfants



Méthaniseurs : des procédés peu sûrs

BROUZILS Sentinelles



Santé Sécurité Sérénité



brouzils.sentinelles.3s.asso@gmail.com

<https://brouzils-sentinelles-asso.over-blog.com/>

Merci pour votre intérêt et votre attention ...



Ce document est le fruit d'un long travail mis à disposition de l'ensemble de la communauté associative du CNVM CH

Il est soumis à la propriété intellectuelle de l'auteur. Ceci implique une obligation de citation et de référencement lors de l'utilisation de ce document.

D'autre part, toute contrefaçon, plagiat, reproduction illicite encourt une poursuite pénale.

Code de la Propriété Intellectuelle. articles L 122. 4

Code de la Propriété Intellectuelle. articles L 335.2- L 335.10

http://www.cfcopies.com/V2/leg/leg_droi.php

<http://www.culture.gouv.fr/culture/infos-pratiques/droits/protection.htm>

