step by STEP

Norme minimale TIC pour les eaux usées

Première édition en juin 2019 (en allemand)

Mis à jour en mars 2021

https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/abwasser.html

Introduction

Reto Steinemann / Melchior Zimmermann / Max Schachtler

Adaptation de la norme minimale pour les eaux usées

Le transfert de la théorie pour les praticiens

- Règle les responsabilités
- Liste de contrôle pour l'auto-analyse de la protection
- Instructions

Cybersécurité

Norme minimale TIC pour les eaux usées

Objectifs

Avant un incident	Connaître les situations → forces / faiblesses
Lors de l'incident	Agir préparé → suivre les instructions
Qualité	Eviter événements ultérieurs Manipulation simple
Suivi	Périodique
Adapté à la pratique	Etabli par les praticiens pour les praticiens OT (DCS) et IT (administration)
Application	step by STEP permet de tirer parti de l'expérience accumulée

Referenten

Reto Steinemann – Chestonag Automation AG

- Depuis 2003 chez Chestonag Automation AG
- Électrotechnique ES / DAS ICT
- Réalisation de divers projets d'automation (STEP & industrie)
- Chef développement / membres de la direction

chestonag automation

Referenten

Melchior Zimmermann – Pictet

- Octobre 2020 - présent: Analyste en Cyber-Securité chez Pictet
- 2019 GRID
- 2018 GSEC & GIAC Advisory Board member
- 2017 – 2020 Developpeur & expert en securité informatique, Chestonag Automation AG
- 2015 – 2017 Master en Biologie et informatique, Université de Genève

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie
de la formation et de la recherche DEFR

Office fédéral pour l'approvisionnement économique du pays OFAE
Division TIC

Norme minimale TIC pour les eaux usées

Introduction au manuel et explication de son fonctionnement

Peter Sven
Chef de projets SNPC
Office fédéral pour l'approvisionnement économique du pays OFAE
Domaine TIC

Présentation

Sven Peter

Formation

- Bachelor à l'Université de Neuchâtel: sciences économiques
- Master à l'Université de Fribourg: technologies de l'information et de la communication
- Stage en gestion de projet chez Tamedia
- Chef de projets SNPC à l'OFAE depuis 2 ans

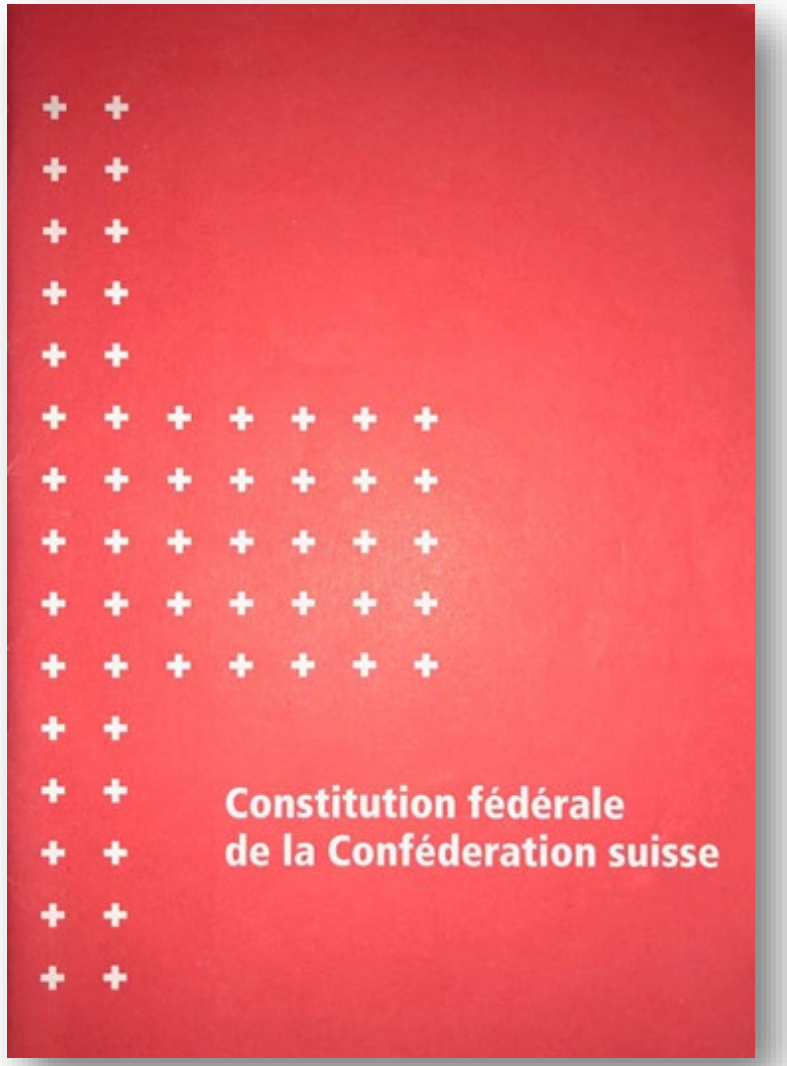
Projets à l'OAFE

- Soutien lors de l'élaboration de :
  - La norme minimale TIC pour l'eau potable
  - La norme minimale TIC pour les eaux usées
  - La norme minimale TIC pour les transports publics
- Chef de projet pour la norme minimale pour le gaz
- Nouveaux projets : chef de projet pour la norme minimale TIC pour la chaleur à distance + pour les terminaux de logistiques

Contact

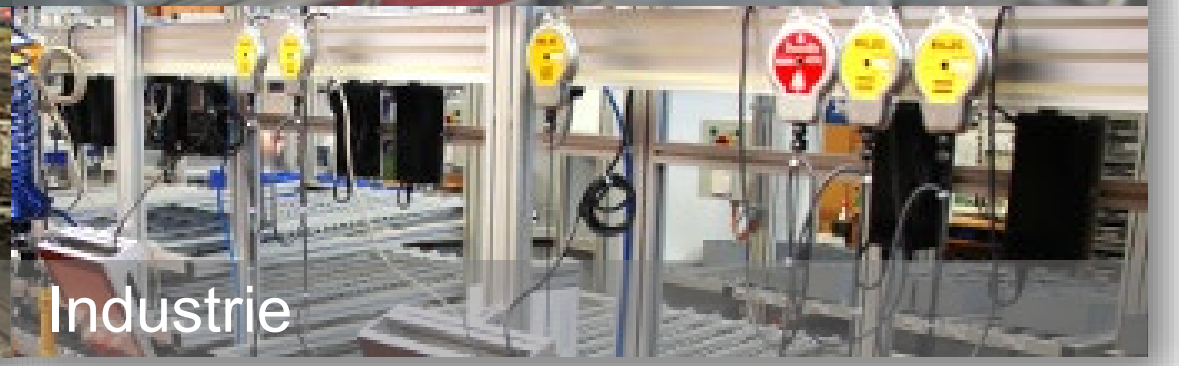
- Tél: +41 58 483 93 75
- E-mail: sven.peter@bwl.admin.ch

Mandat



- **art. 102 Constitution fédérale**
- **loi fédérale sur l'approvisionnement économique du pays**
- **art. 1, Objet :**
  La présente loi régit les mesures visant à garantir l'approvisionnement du pays en biens et services vitaux […] »

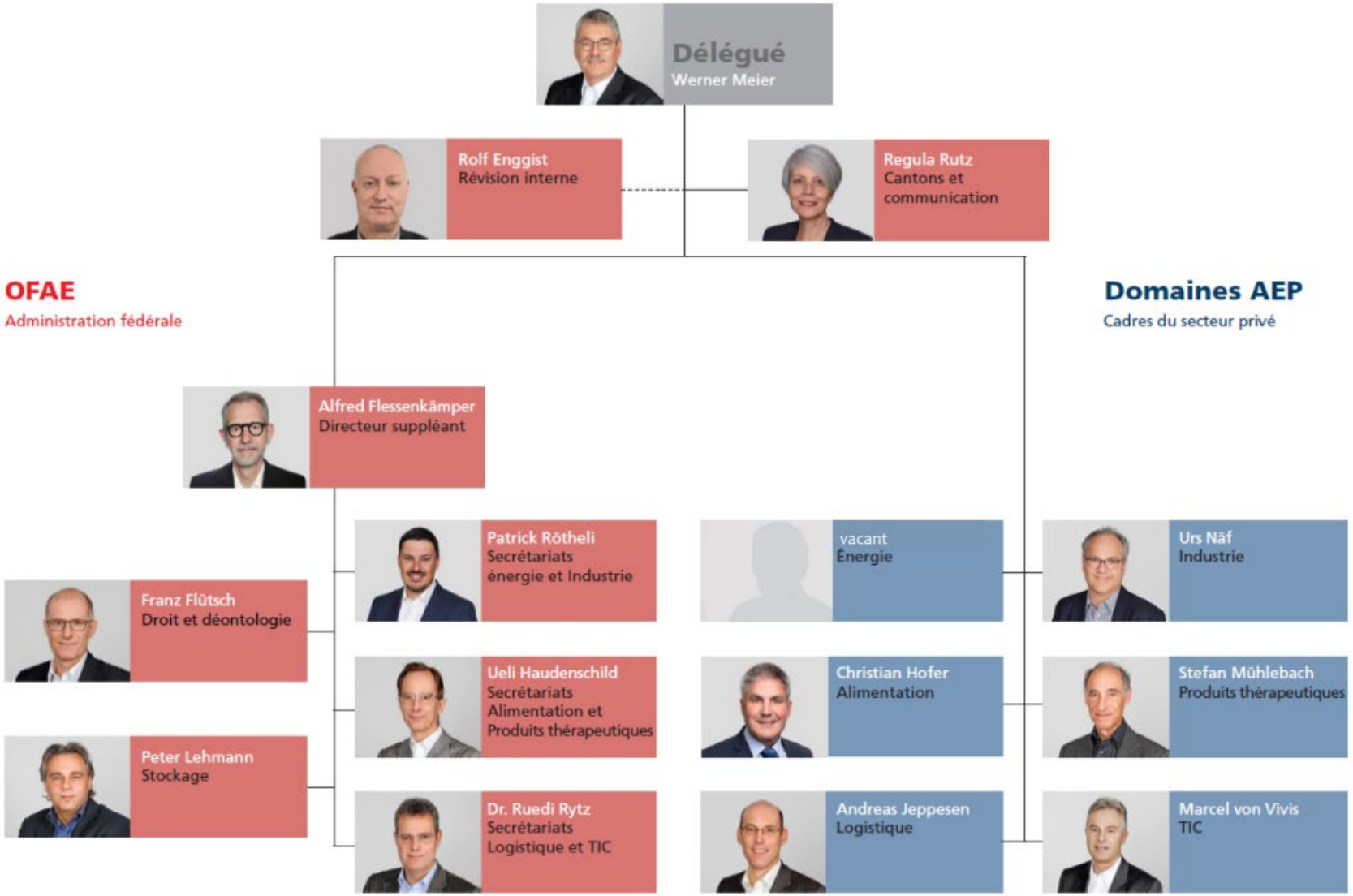
Organisation de l'OFAE



AEP : partenariat public-privé

Confédération
35 personnes

OFAE



Experts
250 personnes

Répartition fédérale des cybertâches

Tâches:

- protection de la Suisse
- poursuite de la cybercriminalité
- protection des infrastructures critiques

Organisation :

- séparation organisationnelle, mais étroite coopération et concertation.

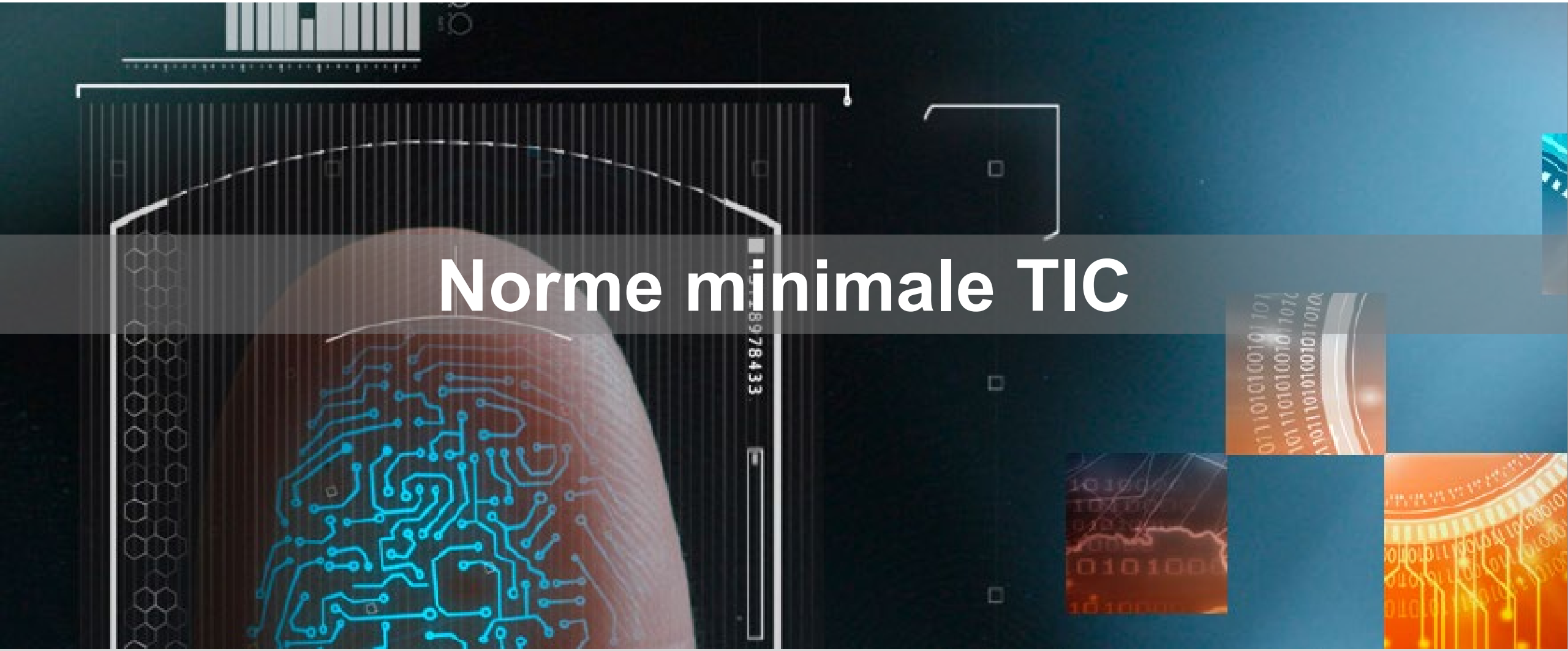
Stratégie nationale pour protéger la Suisse des cyber-risques SNPC

- En 2012, le Conseil fédéral a arrêté la stratégie nationale pour protéger la Suisse des cyber-risques (SNPC).
- Depuis, l'OFAE a mené des analyses de vulnérabilité dans 13 secteurs critiques et proposé différentes mesures.
- La norme minimale TIC est une mesure préventive pour renforcer la résilience informatique conformément à la SNPC.
- En 2018, le Conseil fédéral a arrêté la deuxième stratégie nationale contenant de nouveaux objectifs pour l'OFAE.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie
de la formation et de la recherche DEFR

Office fédéral pour l'approvisionnement économique du pays OFAE
Division TIC



Norme minimale TIC

Exemple de cyberattaques sur différents secteurs

ICTjournal

NEWS

Infrastructures critiques

Un hacker a failli empoisonner l'eau potable d'une ville de Floride

Mer 10.02.2021 - 16:44
par Rodolphe Koller

Via TeamViewer, un pirate est parvenu à augmenter la teneur en soude caustique dans l'eau d'une petite ville de Floride. Plus de peur que de mal, puisqu'un employé a pu rapidement annuler le changement dans le système de traitement.

Blick TV News Sport Meinung Politik Wirtschaft People Green Mehr

Urheber in London und Korea

Hacker-Attacke auf Wasserversorgung in Ebikon LU

Die autonome Betriebssteuerung der Wasserversorgung der Gemeinde Ebikon LU hat im November Tausende bösartige Software-Anfragen bekommen.

netzwoche

NEWS

Grosser Cyberangriff

Hacker erbeuten 30'000 Passwörter von Suisse Velo

Mo 13.09.2021 - 09:57 Uhr
von Oliver Wietlisbach, Watson

Suisse Velo, Anbieterin der "Suisse Velo Vignette" und weiteren Dienstleistungen rund ums Velo, ist das neuste Hacking-Opfer in der Schweiz. Die Täter erbeuteten rund 30'000 E-Mail-Adressen und Passwörter.

LA CÔTE PREMIUM

RÉGIONS SUISSE SPORTS ECONOMIE MONDE SORTIR LIFESTYLE DOSSIERS PREMIUM

Piratage: Rolle s'explique sur les milliers de données volées et publiées sur le darknet

PIRATAGE Le piratage informatique qu'a subi la commune est plus grave que ce qui a été présenté la semaine passée. Une majorité des Rollois sont concernés. En exclusivité, la commune s'explique et reconnaît "une certaine naïveté". Elle détaille les mesures pour aider les citoyens.

PAR GREGORY BALMAT, LAURA LOSE 26.08.2021, 05:00
LECTURE: 7MIN

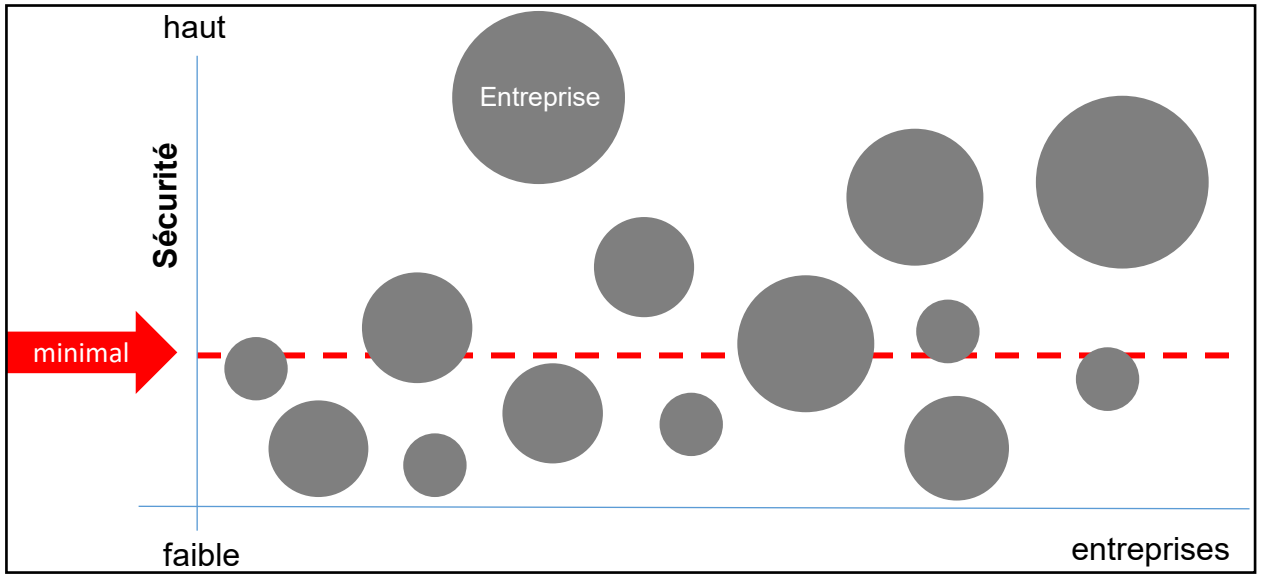
PREMIUM

Sources :
Un hacker a failli empoisonner l'eau potable d'une ville de Floride | ICTjournal
Hacker-Attacke auf Wasserversorgung in Ebikon LU – Blick
Hacker erbeuten 30'000 Passwörter von Suisse Velo | Netzwoche
Piratage: Rolle s'explique sur les milliers de données... (lacote.ch)

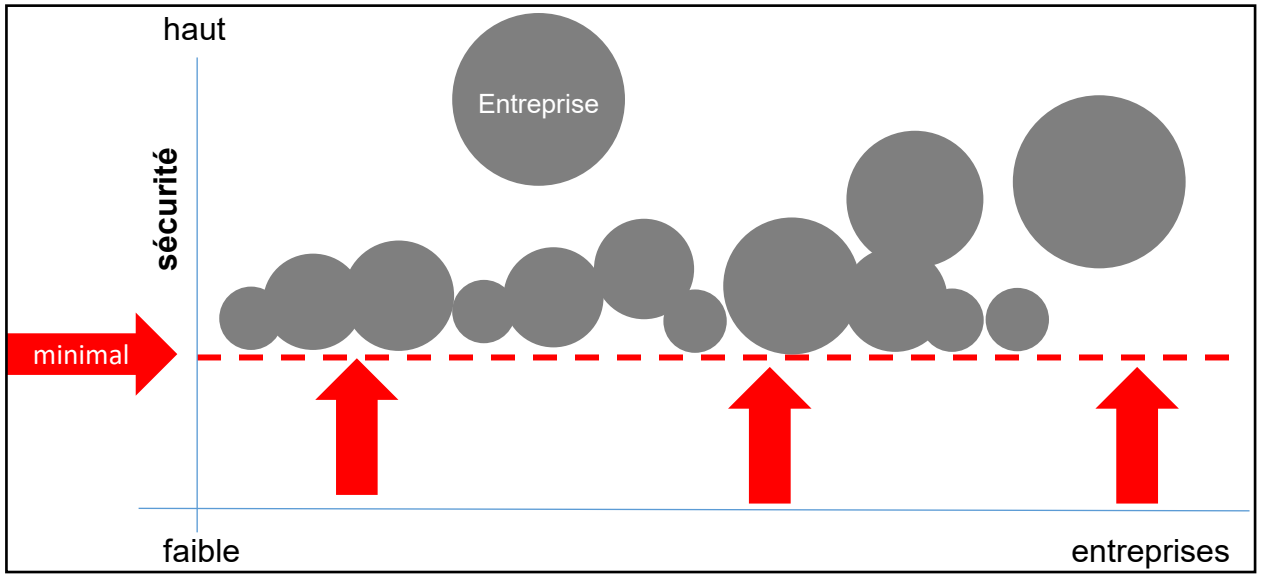
Norme minimale TIC

- La norme peut être utilisée de manière universelle
- L'accent est mis sur les infrastructures critiques
- Il s’agit d’une recommandation
- La norme explique ce qu'il faut faire, mais donne à l'utilisateur la liberté de le faire comme il le souhaite
- La norme est compatible avec de nombreuses normes industrielles, telles que les normes ISO, ISA, BSI, COBIT…

Objectif d’une norme MINIMALE



- Vision actuel d’un secteur



- Vision d‘un secteur après l‘utilisation de la norme minimale TIC

Objectifs de la norme

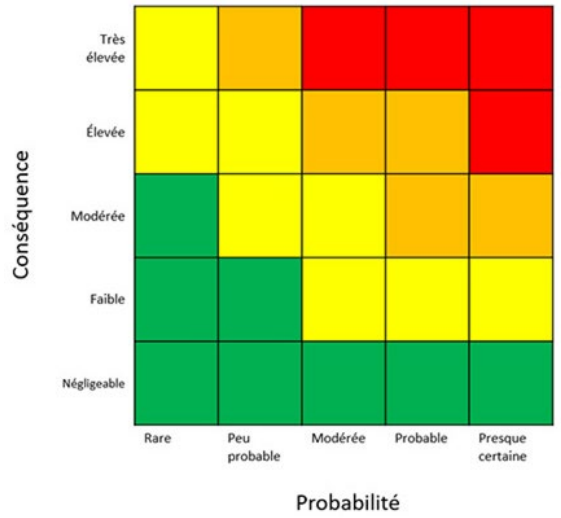
- L’ensemble des mesure contenue dans le programme de cybersécurité de la norme minimale TIC a pour but d’améliorer le niveau de sécurité d’au moins l’un des trois piliers de la cybersécurité.

Fonctionnement de la norme

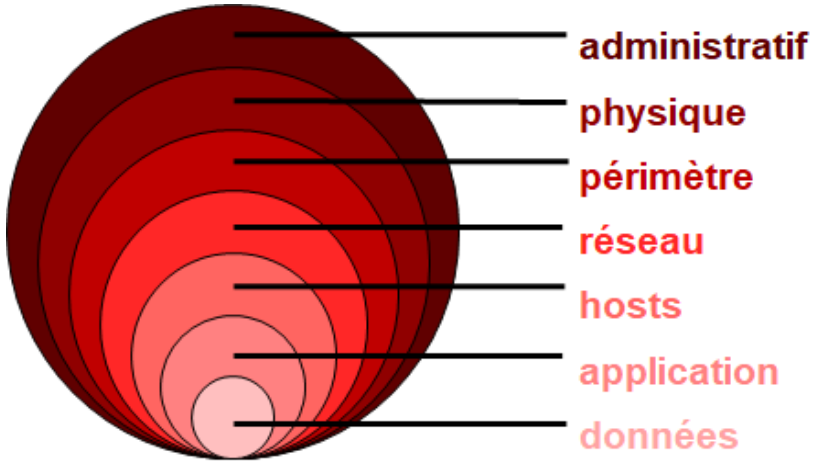
- La norme minimale TIC est basée sur le NIST Framework Core développé par le National Institute of Standards and Technology.
- Les mesures du NIST Framework Core sont basées sur deux concepts :
  - l'approche basée sur les risques
  - la stratégie de « defense-in-depth »
- La norme minimale TIC est composé de 106 mesures réparties entre 5 chapitres.
- Pour chaque chapitre, la norme recommande des activités spécifiques.

Concepts du risque acceptable et de la stratégie de défense en profondeur

- **L'analyse du risque acceptable** est primordiale pour une organisation car cela lui permet d'adapter les mesures du NIST Framework Core à ses propres besoins (selon son secteur, sa taille, ses ressources et ses menaces). Après cette analyse, chaque organisation est en mesure de déterminer, selon ses ressources, le niveau de protection optimale à atteindre.



- **La stratégie defense-in-depth** est dérivée du principe militaire qui veut qu'un système de défense multicouche complexe est plus difficile à franchir qu'une simple barrière. L'objectif de cette stratégie est donc d'appliquer plusieurs mesures de sécurité sur différents niveaux de protection obligeant ainsi l'attaquant à franchir une multitude d'obstacles de sécurité complexes.



Courtes descriptions des 5 chapitres

Identifier : L'objectif des mesures de cette fonction est de répertorier l'ensemble des éléments en lien avec les TIC de l'organisation ainsi que les cyberrisques pouvant affecter ces derniers. Il s'agit de procéder à un « inventaire » des systèmes, des procédures, des ressources, des responsabilités des collaborateurs ou encore des biens de l'organisation. Une fois l'ensemble des éléments TIC répertorié, il est plus aisé de les protéger efficacement en mettant en œuvre les procédures de sécurité adéquates.

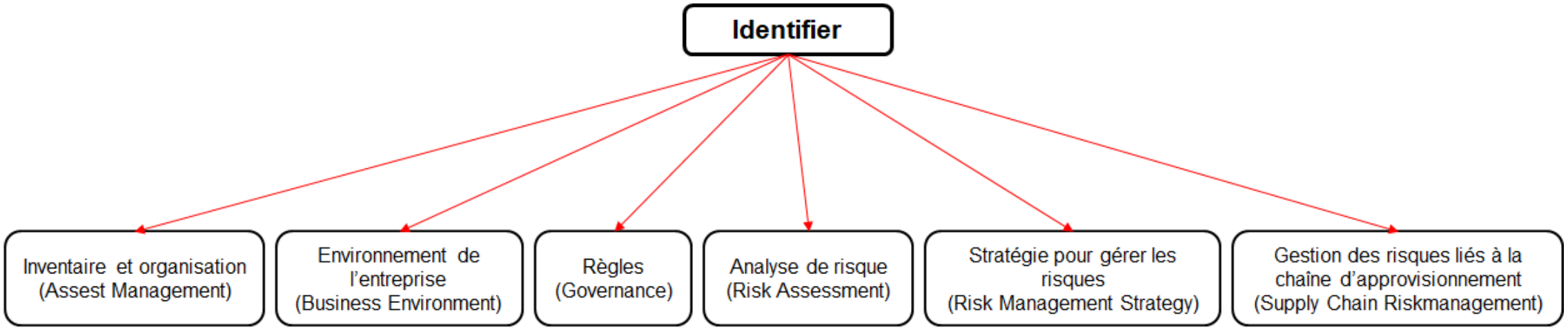
Protéger : Cette fonction englobe les mesures permettant d'assurer une protection et des contrôles de sécurité appropriés à l'ensemble des actifs TIC de l'organisation. Il s'agit principalement de procédés techniques (anti-virus, DMZ, architecture réseau, etc.) mais aussi d'éléments plus globaux comme par exemple la sensibilisation des collaborateurs vis-à-vis des cyberrisques. Le but étant d'éviter ou de limiter les dégâts engendrés par une potentielle menace.

Détecter : Après avoir identifié les éléments TIC et appliqué les mesures de protection adéquates, il est nécessaire de procéder à une surveillance en continue de la sécurité des infrastructures. Les mesures de cette fonction ont pour objectifs de mettre en place un système de surveillance efficace et ciblé des éléments TIC afin déceler suffisamment tôt des menaces et ainsi éviter ou atténuer l'effet d'un cyberincident.

Réagir : Au sein de cette fonction, les mesures permettent d'adapter les procédures de sécurité lors de la détection de cybermenaces. L'objectif est de répondre correctement à un cyberincident en limitant un maximum l'impact de ce dernier sur l'organisation. L'idéal est de disposer de procédures détaillées et approuvées afin de résoudre le plus efficacement possible l'incident.

Récupérer : Cette fonction contient les mesures permettant de restaurer toutes les capacités qui ont été altérés par un incident de cybersécurité. Il s'agit d'appliquer les plans de résilience afin de rétablir les infrastructures de l'organisation pour lui permettre de reprendre rapidement un rythme de travail normal. Cette fonction est primordiale pour permettre de relancer, sur une base saine, les éléments TIC d'une entreprise et donc réduire l'impact d'un incident de cybersécurité.

Exemple : chapitre identifier



Exemple : mesures de la catégorie «Asset Management»

Fonction	Catégorie	Activité	Évaluation	Commentaire	Référence
Identifier	**Inventaire et organisation (Asset Management)** Les données, les personnes, les appareils, les systèmes et les installations d'une entreprise sont identifiés, catalogués et évalués. L'évaluation se fait en fonction de leur criticité pour les processus opérationnels à mettre en place et de la stratégie de l'entreprise en matière de risque.	**ID.AM-1:** Développez un processus d'inventaire garantissant en permanence un recensement exhaustif de vos équipements TIC (Asset).	n/a		CCS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 ISO/IEC 27019:2013 7.1.1, 7.1.2 NERC CIP-002 BSI-Standard 100-2, Kapitel 4.2 Strukturanalyse NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Inventoriez toutes les plateformes, licences et applications logicielles dans votre entreprise.	n/a		CCS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 ISO/IEC 27019:2013 7.1.1, 7.1.2 NERC CIP-002 BSI-Standard 100-2, Kapitel 4.2 Strukturanalyse, M 2.225 NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Listez tous les flux de communication et de transferts de données en interne.	n/a		CCS CSC 1 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1 ISO/IEC 27019:2013 7.2.1 NERC CIP-005 BSI-Standard M 2.393 Regelung des Informationsaustausches NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Listez tous les systèmes TIC externes cruciaux pour votre entreprise.	n/a		COBIT 5 APO02.02 ISO/IEC 27001:2013 A.11.2.6 ISO/IEC 27019:2013 7.2.1 NERC CIP-002 BSI-Standard B 2.10 Mobiler Arbeitsplatz NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Etablissez des priorités pour les ressources inventoriées (équipements, applications, données) selon leur criticité.	n/a		COBIT 5 APO03.03, APO03.04, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 ISO/IEC 27019:2013 7.2.1 NERC CIP-002 BSI-Standard BSI-Standard 100-2, Kapitel 4.3 Schutzbedarfsfeststellung NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Définissez clairement les rôles et les responsabilités en matière de cybersécurité.	n/a		COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 ISO/IEC 27019:2013 8.1.1 NERC CIP-003 BSI-Standard BSI-Standard 100-2, Kapitel 3.4.2 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

Courtes descriptions des niveaux d'évaluation

0 Il s’agit du premier niveau d’évaluation et il signifie que rien n’a été entrepris. Cette mesure n’est même pas connue par l’organisation.

1 L’organisation est consciente de l’existence cette mesure mais il n’existe encore aucune procédure standardisée pour gérer les risques qui sont traités, au jour le jour, de manière réactive.

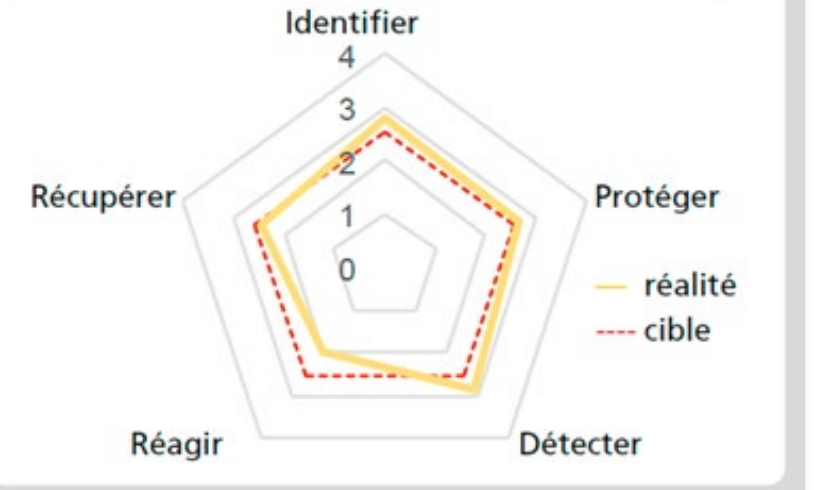
2 Il existe une procédure standardisée pour gérer les risques liés à cette mesure mais l’organisation ne l’a pas rendue obligatoire ou ne l’effectue que partiellement

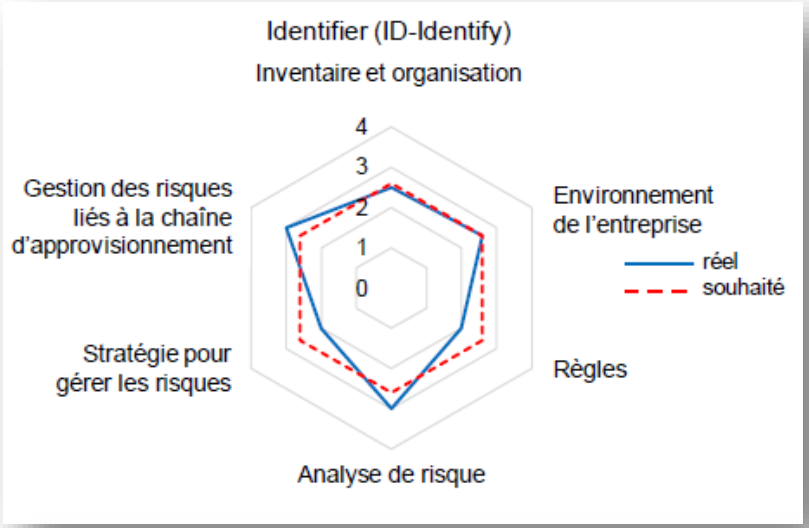
3 La procédure de gestion des risques a été formellement validée ainsi que les instructions pour la faire appliquer correctement. De plus, les risques TIC sont répertoriés de manière standardisée et les directives pour y remédier font régulièrement l’objet de mises à jour.

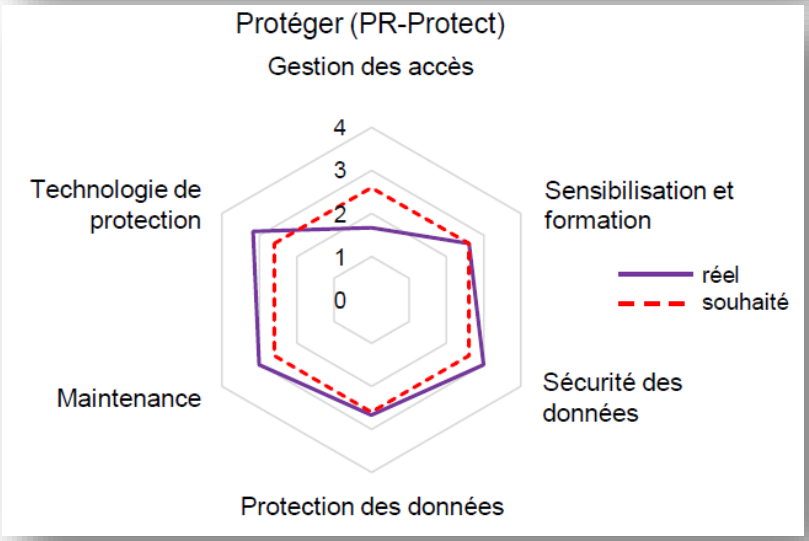
4 Il s’agit du dernier niveau d’évaluation et il signifie que l’organisation répond entièrement aux exigences de niveau 1 à 3. En plus de cela, elle analyse en permanence ses propres processus, méthodes et capacités afin de les améliorer et de s’assurer un niveau de cybersécurité élevé.

Résultat de l'outil d'évaluation

Cote globale de l'évaluation de la cybersécurité	réalité	cible
Identifier *(Identify)*	2.8	2.6
Protéger *(Protect)*	2.7	2.6
Détecter *(Detect)*	2.9	2.6
Réagir *(Respond)*	2.0	2.6
Récupérer *(Recover)*	1.4	2.6



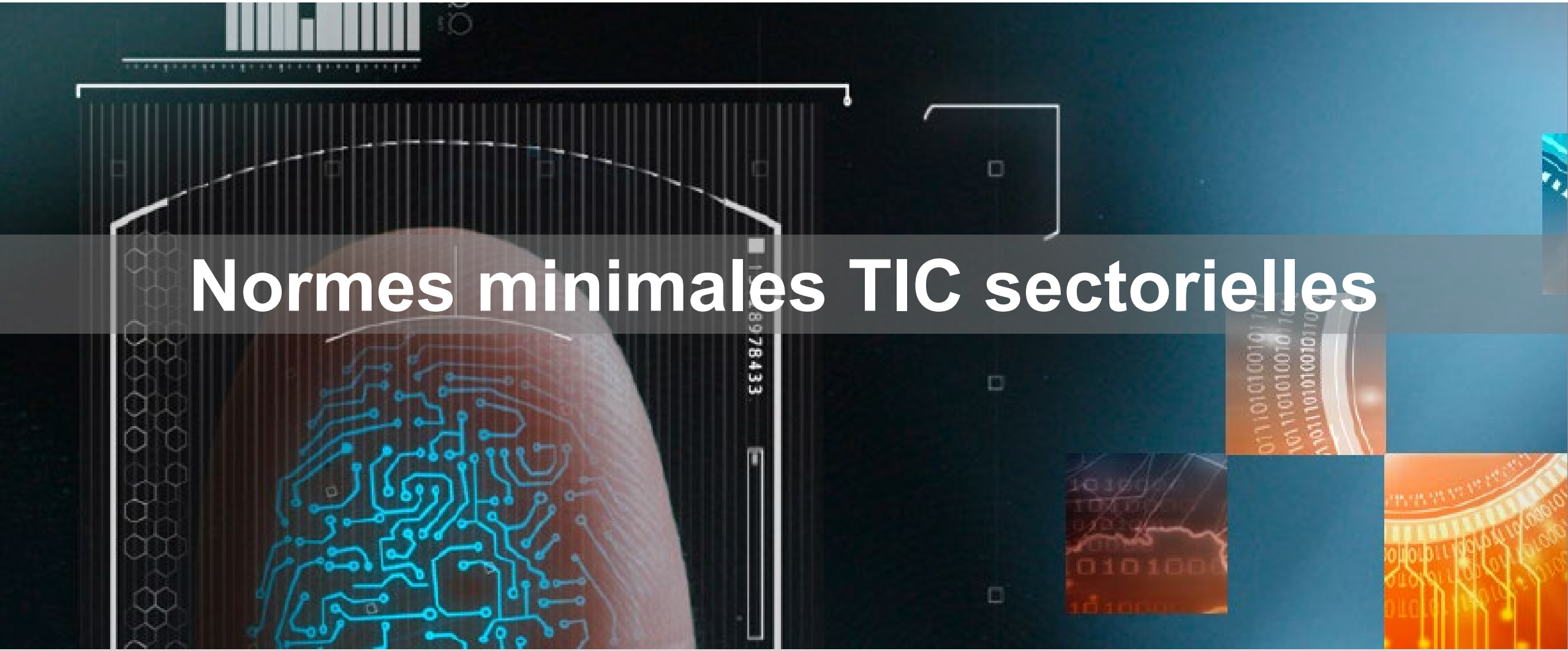




Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie
de la formation et de la recherche DEFR

Office fédéral pour l'approvisionnement économique du pays OFAE
Division TIC



Normes minimales TIC sectorielles

Collaboration avec les associations professionnelles

norme minimale TIC

- En collaboration avec les associations professionnelles, l'OFAE élabore des normes minimales TIC spécifiques qui sont adaptées aux besoins du secteur concerné en identifiant les activités critiques.
- Les normes minimales TIC sectorielles et la norme minimale TIC "générale" sont basées sur le même programme de cybersécurité se référant ainsi aux mêmes mesures.

électricité

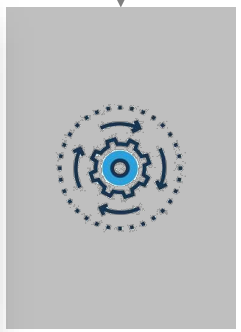
eau potable

alimentation

eau usée

gaz

tp



chaleur à distance
hôpitaux
élimination déchets
terminaux logistiques

De la norme minimale TIC aux normes minimales TIC sectorielles

- Analyse du processus d'approvisionnement
- Identification des acteurs
- Identification des activités critiques et des systèmes TIC associés
- Analyse de vulnérabilité

Objectifs des normes minimales TIC sectoriels

- Les mesures fondées sur le risque permettent d'adapter la norme à différents besoins en tenant compte des éléments suivants : taille, ressources, besoins et menaces de chaque organisation.
- L'identification des activités critiques permet de prioriser certaines mesures du programme de cybersécurité pour assurer la sécurité des éléments critiques du secteur gazier.
- La sécurité des systèmes TIC est un objectif permanent qui doit faire l'objet d'un suivi régulier et d'un processus d'amélioration continue. La norme minimale TIC sert de guide pour la mise en œuvre de ce processus afin d'atteindre cet objectif.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie
de la formation et de la recherche DEFR

Office fédéral pour l'approvisionnement économique du pays OFAE
Division TIC

Norme minimale TIC pour les eaux usées

Norme minimale TIC pour les eaux usées 1/2

- Réalisé par step by STEP en collaboration avec la VSA/FES et l'OFAE
- Publié en 2019, mise à jour en 2021 et publication de la version française fin 2021
- Fait partie de la méthode step by STEP mais peut aussi être utilisée séparément
- Programme de cybersécurité légèrement différent par rapport à la norme minimale TIC comprenant environ 80 mesures
- Permet aux entreprises du traitement des eaux usées de se concentrer sur les éléments principaux de leur secteur

Norme minimale TIC pour les eaux usées 2/2

Exigences	Oui	Non	Support			TIC de référence
			ES	OT	IT	
Inventaire du matériel physique OT Disposez-vous d'un inventaire de tous les systèmes d'OT (serveurs, composants de réseau, panneaux de contrôle, au moins tous les appareils ayant une adresse IP) ?			(x)	x		ID.AM-1
Inventaire du matériel logique (logiciels) OT Disposez-vous d'un inventaire des logiciels utilisés (système d'exploitation, Office, programmes, etc.) ?			(x)	x		ID.AM-2
Inventaire du matériel physique IT Disposez-vous d'un inventaire de tous les systèmes TIC (PC, imprimantes, routeurs, tablettes, smartphones, etc., du moins tous les appareils ayant une adresse IP) ?			(x)		x	ID.AM-1
Inventaire du matériel logique (logiciels) IT Disposez-vous d'un inventaire des logiciels utilisés (système d'exploitation, Office, programmes, etc.) ?			(x)		x	ID.AM-2
OT et IT Inventorier les connexions au réseau et les flux de données Disposez-vous d'un inventaire de toutes les connexions de réseau et des flux de données qui sont acheminés par ces connexions ?			(x)	x	x	

- Validation ou non de la mesure
- Évaluation de la criticité (haut-faible-aucune)
- Défini des soutiens pour chaque mesure (ES, OT, IT)
- Différenciation des mesures entre IT et OT
- Donne l'équivalence des mesures vis-à-vis de la norme minimale TIC
- Contient des mesures spécifiques au secteur des eaux usées

Contact

Office fédéral pour l'approvisionnement économique du pays OFAE

Bernastrasse 28
3003 Berne

Sven Peter
Chef de projets SNPC
Sven.peter@bwl.admin.ch
Tél. : +41 58 462 21 71

Norme minimale pour la cybersécurité dans les STEP

step by STEP

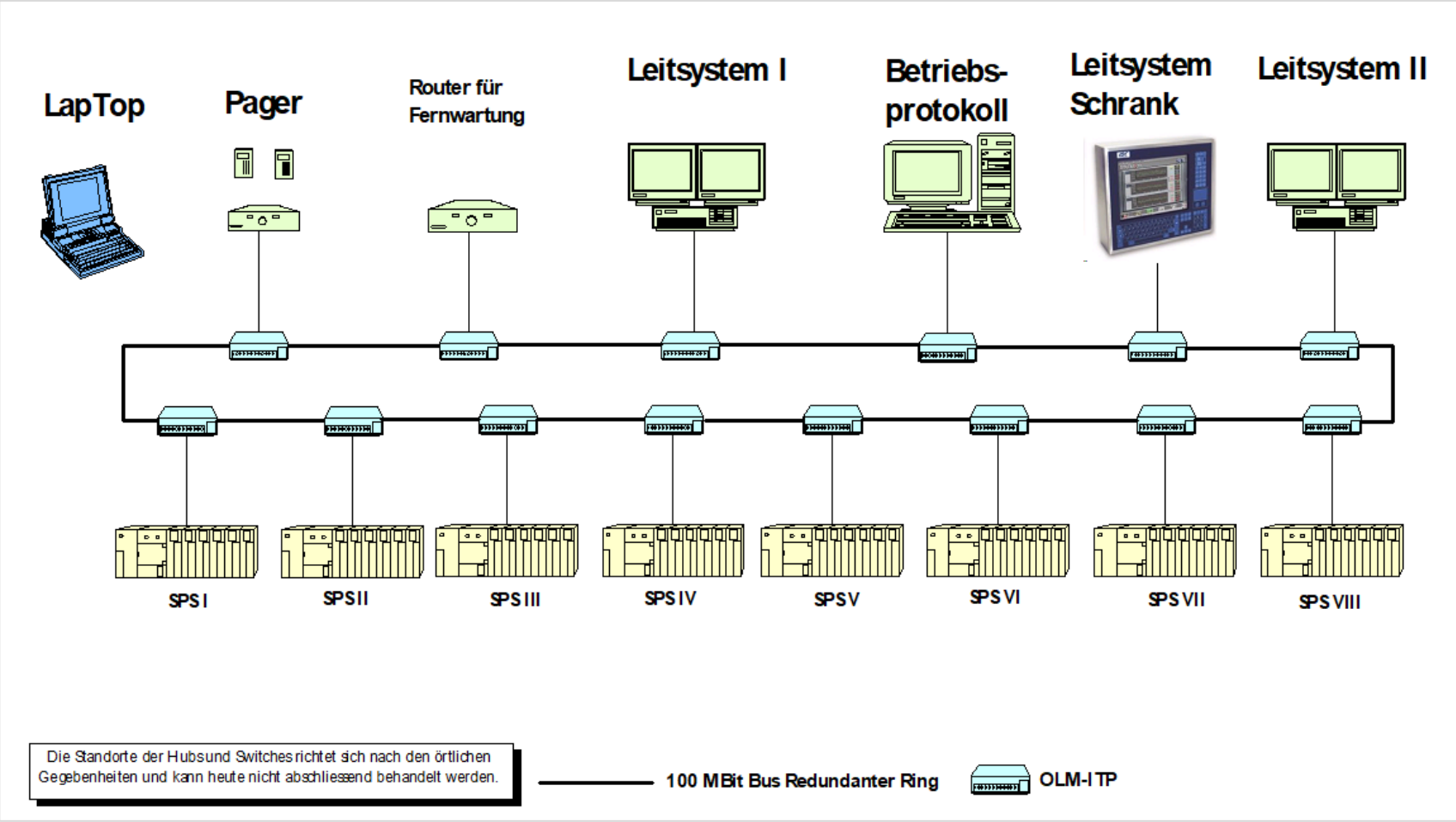
Réseaux OT (technologies opérationnelles; réseau DCS)
Architecture du système et ce dont nous devons nous protéger

Reto Steinemann / Melchior Zimmermann

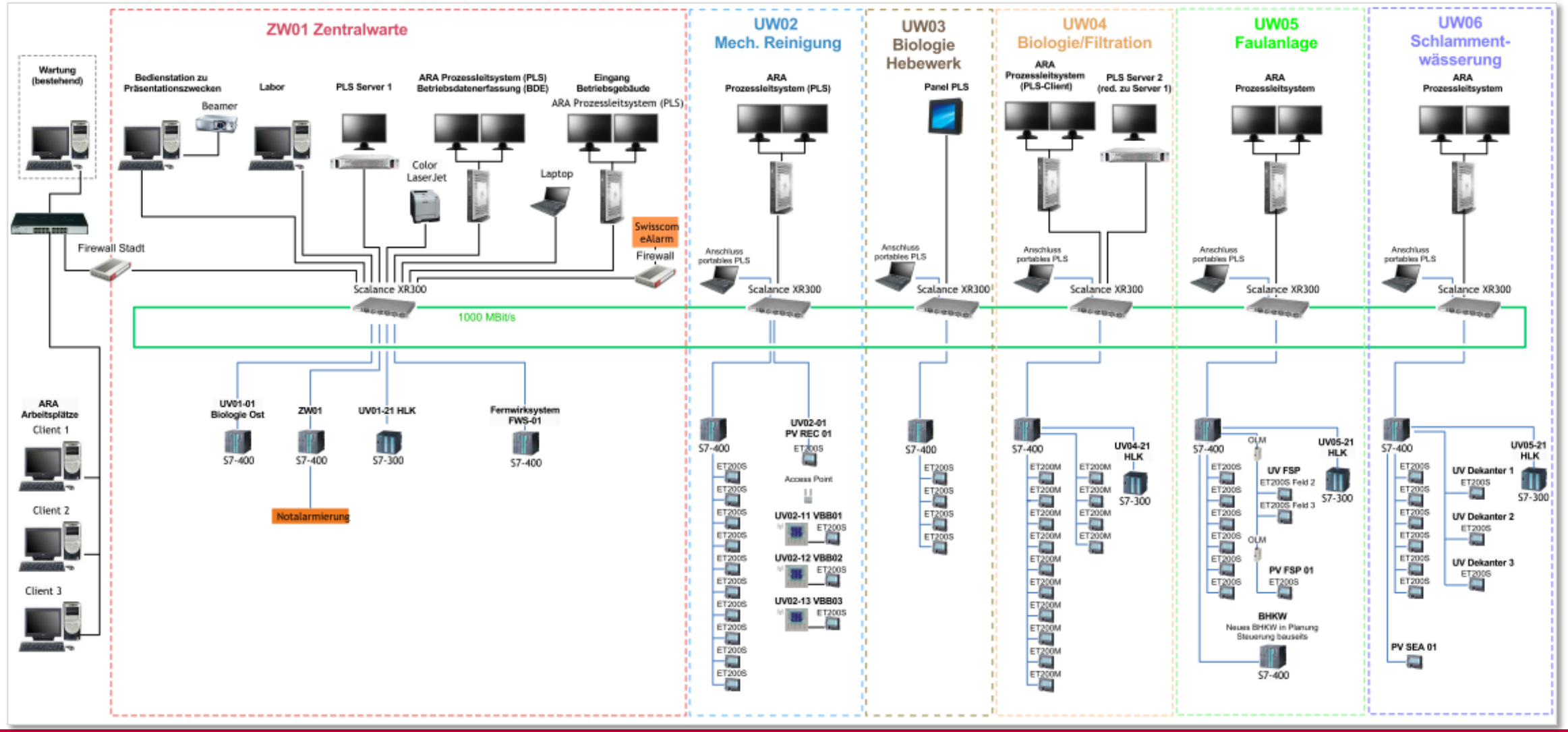
La cybersécurité dans le réseau OT

- Le réseau OT typique
- L’évolution au fil du temps
- Menaces et acteurs
- Comment pouvons-nous nous protéger ?

L‘OT en 2000


LapTop
Pager
Router für Fernwartung
Leitsystem I
Betriebs-protokoll
Leitsystem Schrank
Leitsystem II
SPS I
SPS II
SPS III
SPS IV
SPS V
SPS VI
SPS VII
SPS VIII
Die Standorte der Hubsund Switches richtet sich nach den örtlichen Gegebenheiten und kann heute nicht abschliessend behandelt werden.
100 MBit Bus Redundanter Ring
OLM-I TP

L'OT en 2021

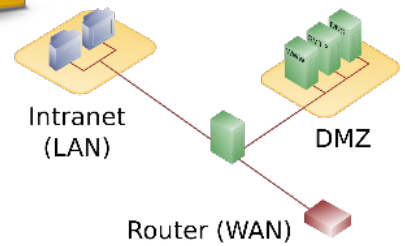

ZW01 Zentralwarte
UW02 Mech. Reinigung
UW03 Biologie Hebewerk
UW04 Biologie/Filtration
UW05 Faulanlage
UW06 Schlammentwässerung
Wartung (bestehend)
Bedienstation zu Präsentationszwecken
Beamer
Labor
PLS Server 1
ARA Prozessleitsystem (PLS) Betriebsdatenerfassung (BDE)
Eingang Betriebsgebäude
ARA Prozessleitsystem (PLS)
Color LaserJet
Laptop
Swisscom eAlarm
Firewall
Firewall Stadt
Scalance XR300
1000 MBit/s
ARA Prozessleitsystem (PLS)
Panel PLS
PLS Server 2 (red. zu Server 1)
ARA Prozessleitsystem (PLS-Client)
Anschluss portables PLS
ARA Arbeitsplätze
Client 1
Client 2
Client 3
UV01-01 Biologie Ost
ZW01
UV01-21 HLK
Fernwirksystem FWS-01
Notalarmierung
UV02-01 PV REC 01
Access Point
UV02-11 VBB01
UV02-12 VBB02
UV02-13 VBB03
UV04-21 HLK
UV05-21 HLK
UV FSP
PV FSP 01
BHKW
Neues BHKW in Planung
Steuerung bauseits
PV SEA 01
UV Dekanter 1
UV Dekanter 2
UV Dekanter 3
S7-400
S7-300
ET200S
ET200M
OLM

Le réseau OT – évolution au fil du temps

- Le réseau d'automation est en principe resté le même
  - L'approche défensive est restée
  - Utilisation aussi isolée et exclusive que possible du réseau
  - Protection des ordinateurs du système de contrôle et des systèmes de commande
- Nouvelles exigences de télémaintenance
    - " Anytime – Anywhere – AnyDevice "
- Un accès de plus en plus important à d'autres réseaux
    - Connectivité avec l'IT
    - Accès Internet pour les alarmes, les données météorologiques, etc.

Le réseau OT – évolution au fil du temps

- Nouveaux appareils et nouveaux réseaux
  - Le réseau IT (bureau)
  - Réseau cantonal / communal
  - Réseau de systèmes externes
  - Réseau de téléphonie
  - Réseau de caméras
  - W-Lan (exploitation, visiteurs, téléphonie, etc.)
  - Réseaux DMZ (maintenance à distance)
- Connexions externes
  - Réseau externe (LWL, SHDSL, etc.)
  - VPN (All IP, xDSL, Cabel, LTE, etc.)



Le réseau OT - Conclusion

- Risques
  - Mauvaise configuration du réseau
  - Lacunes dans la configuration des composantes liées à la sécurité
  - Points faibles vulnérables dans les systèmes (logiciel d'exploitation obsolète, etc.)
  - Contamination par des logiciels malveillants via Internet ou via des supports portables
- Nous avons besoin d'une sensibilisation à la sécurité
  - La sécurité nécessite un entretien
  - La sécurité a un coût

- La simple installation de pare-feux ne suffit pas
- La sécurité de l'OT est devenue une nouvelle discipline dans le domaine de l'automation

Menaces et acteurs

La tentative de piratage du distributeur d'eau de Ebikon en novembre 2018

- „L'installation a été attaquée à l'aide de milliers de demandes malveillantes provenant de Londres et de Corée“
- "Le nouveau système a immédiatement repoussé les attaques".

Que s'est-il passé ?

- Le routeur industriel SSH a été soumis à une attaque Brute-Force.
- L'objectif étant de découvrir les données d'accès à l'aide de tentatives de connexion à répétition.
- La mise à contribution du système que cela a provoqué a pratiquement bloqué le routeur et le VPN a cessé de fonctionner.

→ Comment a réagi la presse ?

watson

Schweiz International Wirtschaft Sport Leben Spass Digital Wissen Blogs Videos Wettbewerbe

Hacker aus London beis Wasservers Ebikon LU d

Blick

News Sp

News Schweiz Zentral

Urheber in London und

Hacker-A Wasserve Ebi

inside-it.ch

ictjobs.ch Beschaffung Newsletter Inserieren Inside-chann

Mittwoch, 19.12.2018 / 11:37 0

Hacker beissen sich an Wasserversorgung von Ebikon die Zähne aus

Wenn Medien über Hacker berichten, dann ist der Anlass le ihrer "Erfolge". Da tut es gut, für einmal auch über einen erf Angriff berichten zu können. Einen solchen meldet die Luze Ebikon. Hacker hätten im November die IT-Infrastruktur der der Gemeinde angegriffen. Das System, das im letzten Her habe die Attacken aber abwehren können. Trotzdem wurde Sicherheitsstufe noch einmal erhöht.

Mehrere tausend Mal sei die Software von bösartigen Anfra worden, teilte die Gemeinde mit. Der Syste t und der Gemeinde gemeldet, sagte Mari g auf Anfrage von 'Keystone-SDA'.

n Eindringungsversuche ins Netzwerk geh e, Reservoire überwache und bei Wasserc er sehr guten Verschlüsselung hätten die Systembetreiber habe die IP-Adressen d nd so den Ursprungsort ermitteln könner Dubach.

n Betriebssteuerung handle es sich um d Europa. Wäre trotz der Sicherheitsvorkel nnten die Betreiber das System als Notlös hanuell bedienen.

6'500 Personen mit Wasser. Angeschloss Adligenswil, Buchrain oder Dierikon. Zudem liefert Ebikon Root. (sda/hjm)

VIDEO

Hacker-Angriff au Wasserversorgur zum mehreren Ta Anfragen»

Ende November wurde das System de gehackt. Der Angriff konnte erfolgrei zeigt.

• Aktualisiert
Sandra Monika Ziegler
19.12.2018, 20:03 Uhr

Hacker versuchten das digitale Leitungsnetz der Wasserversorgung Ebikon lahmzulegen. (Symbolbild: Getty)

tele1

VERKEHRSSERVICE 2 MELDUNGEN | 2° IN LUZERN SCHÖN | LOGIN

Zentralschweizer Fernsehen NEWS TV-PROGRAMM SENDUNGEN EVENTS TICKETS WERBUNG

7°

SRF

Suche MENÜ

News > Zentralschweiz >

Angriffe abgewehrt

Hackerangriff auf die Wasserversorgung von Ebikon

Mittwoch, 19.12.2018, 17:12 Uhr

Dieser Artikel wurde 1-mal geteilt.

Wäre die Attacke erfolgreich gewesen, hätte das grosse Folgen haben können

02:07 min, aus Regionaljournal Zentralschweiz vom 19.12.2018.

- Mehrere tausend Mal versuchten Hacker von London und Korea aus in das Computersystem der Wasserversorgung von Ebikon einzudringen.
- Das im letzten Herbst neu installierte System konnte aber alle Angriffe abwehren und aufzeichnen. So konnten die Angriffe zurückverfolgt werden.
- Wären die Angriffe erfolgreich gewesen, hätte das gröbere Folgen haben können, sagt der Leiter der Wasserversorgung Ebikon, Markus Dubach.
- Dass ausgerechnet Ebikon Opfer von Cyberattacken wurde, sei reiner Zufall meint Dubach. Trotzdem wurden die Sicherheitsstandards erhöht.

SRF 1, Regionaljournal Zentralschweiz, 17:30 Uhr; joel

News > Zentralschweiz >

Der Luzerner Gesundheitsdirektor Guido Graf zum Sparprogramm des Kantonsspitals: «Der Kostendruck war noch nie so gross»

Kilian Küttel / 21.12.2018, 05:00 Uhr

Der Rundweg soll weg vom Ufer des Baldeggersees

Ernesto Piazza / 21.12.2018, 05:00 Uhr

DONNERSTAG, 20. DEZEMBER 2018 / 20MINUTEN

Luzern/Reg

Hacker greifen Ebikoner Wasserversorgung an

EBIKON. Tausende Male ist die Software der Wasserversorgung von Ebikon von bösartigen Anfragen angepinnt worden. Doch das System hielt den Attacken stand.

Das System hielt den Hacker-Attacken aus London und Korea stand.

Aus London und Korea seien bei der IT-Infrastruktur der Wasserversorgung in Ebikon Tausende bösartige Anfragen eingegangen, teilte die Gemeinde gestern mit. Hacker versuchten, sich Zugang zum System zu verschaffen, mit dem Pumpen gesteuert und Reservoire überwacht werden. «Die Motivation für den Angriff ist uns nicht bekannt», sagt Sprecher Roland Beyeler. Es sei kein gezielter Angriff gewesen: «Bei solchen Angriffen werden jeweils verschiedenste Systeme angegriffen.» Die Hacker würden es an etlichen Zielorten versuchen – erst wenn sie beim Angriff Erfolg hätten, schauten sie, was es zu holen gebe.

Dank der guten Verschlüsselung hatten die Hacker keinen Erfolg. Beyeler: «Das System hat den Angriff registriert und sofort gemeldet.» Es war der erste Vorfall dieser Art. In Ebikon freut man sich über die Abwehr: «Das hat bestätigt, dass wir mit dem modernen System vor Angriffen gut geschützt sind», sagt Beyeler. Dennoch reagierte man auf den Vorfall: «Das System wird zwar den Anforderungen gerecht, wir haben aber nun zusätzliche Massnahmen ergriffen, um die Sicherheit noch weiter zu erhöhen.» Würden Hacker trotzdem erfolgreich sein, könnten die Betreiber das System herunterfahren und die Anlagen manuell bedienen. «Die Wasserversorgung könnte nicht fremdgesteuert werden.» GWA/SDA

ANZEIGE

Menaces et acteurs

Quelques questions fondamentales se posent...

- Qui nous menace ?
- Quels sont les vecteurs d'attaque qui nous concernent ?
- De quoi pouvons-nous et devons-nous nous protéger ?
- Comment obtenir une bonne protection de base ?
- En quoi la norme minimale TIC peut-elle nous aider ?

"Il existe une multitude de risques.....

... mais quelles sont les menaces que nous devons réellement prendre en compte ?"

Acteurs

- Script-Kiddies (= néophytes utilisant des scripts déjà établis pour tenter d'infiltrer des systèmes)
  - Utilisation d'outils "trouvés", non ciblés
  - Probabilité moyenne d'attaque, peu de chances de succès
- Cybercriminels
  - Modèles opérationnels dans le but de gagner de l'argent
  - Probabilité élevée d'attaque, chance moyenne de succès (surtout dans le domaine de l'IT)
- Acteurs étatiques
  - Attaques à motivation politique, religieuse ou culturelle
  - Faible probabilité d'attaque, grandes chances de succès
- Initiés malveillants
  - Endommager l'installation
  - Faible probabilité d'attaque, grandes chances de succès

Vecteurs d'attaque

Un vecteur ou vecteur d'attaque désigne en informatique le **moyen** ou la **technique** qu'un intrus non autorisé, quel que soit son type, peut utiliser pour compromettre un système informatique, c'est-à-dire pour y accéder sans autorisation et ensuite en prendre le contrôle ou du moins l'utiliser abusivement à ses propres fins.

Dans la plupart des cas, des failles de sécurité devenues notoires du système attaqué sont utilisées à cette fin. Une telle exploitation est appelée un « **exploit** ».

(Source : Wikipedia, de l'allemand)

Quels vecteurs d'attaque peuvent être exploités dans un réseau OT ?

Vecteurs d'attaque

- Connexion Internet
  - Firmware non sécurisé ou mauvaise configuration du pare-feu.
  - Appareils non sécurisés directement accessibles par Internet
- Accès à Internet
  - Site Web avec logiciels malveillants
  - Téléchargement de programmes contenant un logiciel malveillant
  - E-mail avec un logiciel malveillant en pièce jointe
- Accès à la maintenance à distance (VPN)
  - Accès mal sécurisé
  - Appareil infecté sur le réseau (PC, ordinateur portable, tablette, etc.)

Vecteurs d'attaque

- Supports portables (carte mémoire, clé USB ou disque dur externe)
  - Fichier avec code malvéillant (document Office avec macro)
  - Clé USB manipulée
- Environnement informatique
  - Appareil infecté (PC de bureau, etc.)
- Réseau sans fil
  - Accès mal protégé
  - Appareil infecté sur le réseau (ordinateur portable, tablette, etc.)

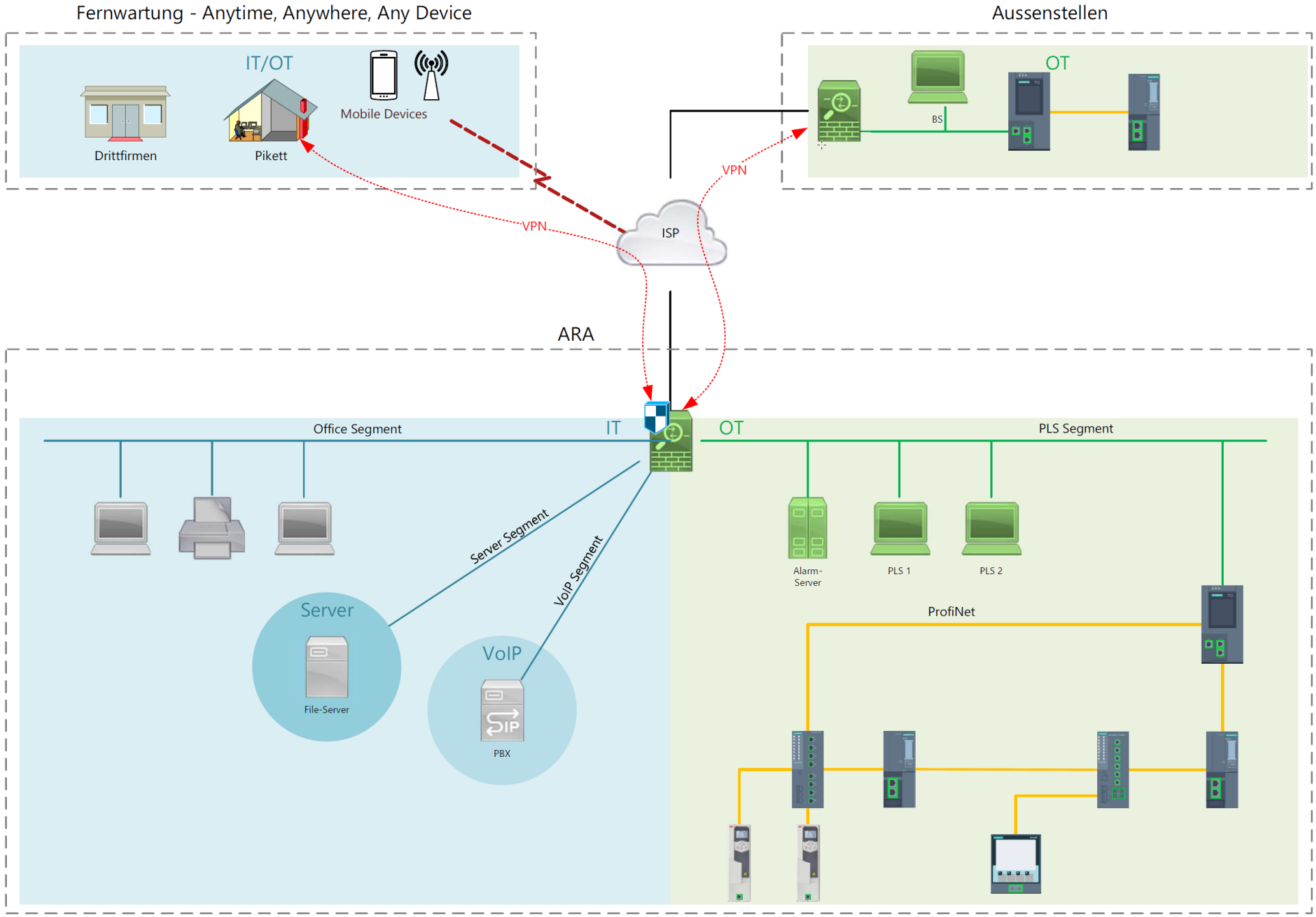
Comment pouvons-nous nous protéger ?

- Defense-in-Depth
  - Les attaques nécessitent plusieurs étapes pour réussir
  - Chaque étape est une occasion de repousser l'attaque.
  - Plus il y a d'étapes, moins il y a de chances qu'une attaque réussisse
- Approche fondée sur le risque
  - Vous ne devez pas tout faire, mais...
  - ... vous devez être conscient de ce que vous ne faites pas et savoir pourquoi vous ne le faites pas.
  - Risque = (impact x probabilité) / coûts
  - La disponibilité de l'OT doit également être prise en compte
  - La confidentialité de l'IT doit également être prise en compte
- Nous avons besoin d'une "protection de base" qui couvre les risques pertinents.

Protection de base

- Segmentation des réseaux
  - Un accès à Internet limité au strict nécessaire
  - Dans la mesure du possible, pas d'accès au réseau OT (VPN !)
  - Accès ciblé uniquement depuis le réseau OT
  - Autres réseaux pour les besoins spécifiques

- Entretien régulier
  - Mise à jour des systèmes (pare-feu, PC, etc.)
  - Contrôle des configurations
  - Contrôle des listes d'utilisateurs et des mots de passe


Fernwartung - Anytime, Anywhere, Any Device
IT/OT
Drittfirmen
Pikett
Mobile Devices
Aussenstellen
OT
BS
VPN
VPN
ISP
ARA
IT
Office Segment
OT
PLS Segment
Server Segment
VoIP Segment
Server
File-Server
VoIP
PBX
Alarm-Server
PLS 1
PLS 2
ProfiNet

Protection de base

- Sensibiliser les utilisateurs
  - De quels systèmes OT disposons-nous ?
  - De ques systèmes IT disposons-nous ?
  - Quels sont les risques ?

- Utilisateurs personnels et directives relatives aux mots de passe
  - Tous les systèmes doivent être protégés contre les accès non autorisés.
  - Les utilisateurs doivent être clairement identifiés

- Sauvegarde des données de projet / archives
  - Récupération rapide
  - Prévenir la perte de données

Conclusions

- Technique
  - Bonne protection de base
  - Entretien régulier

- Organisation
  - Les systèmes IT et OT ainsi que les risques doivent être connus.
  - Les actions à prendre en cas d'évènement doivent être définies.

- La norme minimale TIC aide...
  - Gestion des systèmes
  - Introduction des processus
  - Révision régulière des processus

Merci de votre attention !

step by STEP

Réseau IT (Administration)
Architecture des systèmes et ce dont nous devons nous protéger

Reto Steinemann / Melchior Zimmermann

Responsabilités dans la sécurité IT

- Direction

• Définir les mesures organisationnelles
• Définir les objectifs
• Définir les directives

- Techniciens

• Définir les concepts techniques
• Réalisation des concepts
• Entretien

- Utilisateurs

•???

La cybersécurité dans le réseau IT

- Chemins d'attaques
- Comment peut-on établir une "protection de base"
- Social Engineering
- Mots de passe

Chemins d'attaques

- Comment un agresseur peut-il arriver sur mon PC?

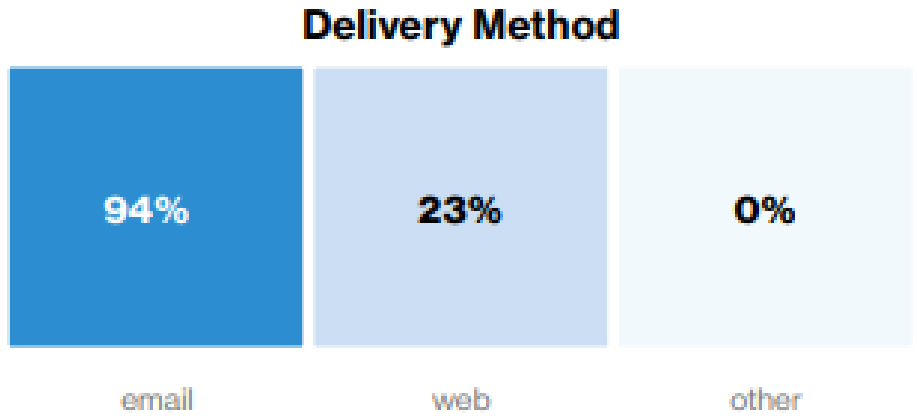


Figure 19. Malware types and delivery methods

2019 Verizon data-breach investigations report

- Les e-mails et les navigateurs sont les chemins d'attaques les plus courants
- Attaquer un système avec les dernières mises à jour depuis l'extérieur est très difficile (est fait de manière ciblée, négligeable dans la plupart des cas)

Mise à jour

- Il n'a jamais été aussi simple de faire des mises à jour

- Automatiques
- Plus fiables et plus stables

- Les mises à jour les plus importantes

- Système d'exploitation
- Navigateurs

JUST DO IT.

Navigateurs

- Ad-Blocker (pas seulement pour le confort)
- Visiter seulement des sites connus
- Ne pas cliquer sur des liens inconnus

uBlock origin

HTTPS
Everywhere

E-Mail

- Ne pas se laisser mettre sous pression
- Ne pas ouvrir de pièces-jointes inattendues
- Ne pas activer les macros
- Ne pas cliquer sur des liens inconnus
- Ne pas entrer de mots de passe

Que faire en cas de doute ?

- Un e-mail d'un contact connu avec une pièce jointe suspecte
- Demander un deuxième avis
- Contacter l'expéditrice/eur directement (p.ex. par téléphone)

- Si vous constatez déjà une infection :
- Débranchez les PC du réseau
- N'éteignez pas les PC
- Contactez un/e spécialiste

Social Engineering - Manipulation

- Comment fait-on pour convaincre une victime potentielle de cliquer sur un lien ou d'ouvrir une pièce jointe ?

→ En utilisant le «Social Engineering»

- Convaincre une personne de faire quelque chose qui va à l'encontre de ses intérêts
- Manipulation par la connaissance du comportement humain
- “Arnaque”

- Pas seulement pour les attaques de hacking :

- Dans la vente
- Dans les médias
- Dans la politique

Résumé

- Le Social Engineering et souvent le point de départ d'une attaque
- Il s'agit d'une composante humaine, et non technique

«Plus le moyen de communication est peu chère, moins il faut lui faire confiance.»

Des mots de passe sécurisés

- sont difficiles à deviner
- sont longs
- sont facile à se rappeler
- ne sont utilisé que pour une application / un site web

Exemple :

- **Thomas** : mauvais mot de passe, facile à deviner
- **@#hjSDF23** : mauvais mot de passe, difficile à se rappeler
- c**haqueMatinJeMangeUneSaucisse** : bon mot de passe, difficile à deviner, facile à se rappeler

Manager de mot de passe

- Une application gère tous vos mots de passe
- Site web, applications, etc.
- Sur une app ou dans un service cloud

- Il ne faut se rappeler que d'un mot de passe principal
- Tous les autres mots de passe sont enregistrés dans l'application
- Bien plus facile que de se souvenir de 30 mots de passe différents

- Pas de redondance
- Si l'application est «hackée», l'agresseur a accès à tous les mot de passes
- Si on oublie le mot de passe principal, on n'a plus accès aux autres

MFA – Authentification multi-facteurs

- L'authentification nécessite un deuxième facteur (2FA)
- APP
- SMS
- Message PUSH
- Appareil externe

- Sécurité grandement augmentée
- Deviner un mot de passe ne sert plus à grand chose
- L'effort nécessaire à une attaque est grandement augmenté

Résumé

- Faire les mises à jour
- Utiliser un Ad-Blocker
- Mieux vaut lire les e-mails deux fois
- Utilisation ciblée du MFA pour les comptes critiques

- … et avec ça, on évite une majorité des attaques

mais: «La sécurité informatique est un processus, et non un état»

Merci de votre attention !

step by STEP

Résumé et pratique
Norme minimale TIC pour les eaux usées

Reto Steinemann / Melchior Zimmermann / Max Schachtler

Le plus important en matière de cybersécurité (1/8)

Les STEP, les ingénieurs et les entreprises sont sensibilisés

- Certaines entreprises veulent saisir l'opportunité → Attention aux failles de sécurité IT !
- Ils y voient un nouveau domaine d'activité → Deviennent tout de suite des cyber spécialistes/experts

Les exploitants fixent les critères/exigences pour les experts en sécurité (cyber)

- Exiger une **certification,** ex. CISA, nécessitant une formation continue, de l'expérience, etc.
- Vérifier que la cybersécurité est le **principal domaine d'activité** de l'entreprise → Compétence professionnelle actuelle
- S'assurer de la neutralité, de l'indépendance, et de l'absence **de conflits d'intérêts** avec des fournisseurs.

Le plus important en matière de cybersécurité (2/8)

L'exploitant connaît son environnement TIC et fournit de la documentation

Outil d'aide :

- Chapitre 5 (Liste de contrôle OUI / NON des documents) et chapitre 6 (Guide d'action)

Exigences	Oui	Non	Support			TIC de référence
			ESS	OT	IT	
Inventaire du matériel physique OT Disposez-vous d'un inventaire de tous les systèmes d'OT (serveurs, composants de réseau, panneaux de contrôle, au moins tous les appareils ayant une adresse IP) ?			(x)	x		ID.AM-1
Inventaire du matériel logique (logiciels) OT Disposez-vous d'un inventaire des logiciels utilisés (système d'exploitation, Office, programmes, etc.) ?			(x)	x		ID.AM-2

Le plus important en matière de cybersécurité (3/8)

Protection de base

N'entamez pas d'actions précipitées où trop hâtives → inapproprié

Se servir de noms d'utilisateurs ainsi que de mots de passe personnels

Standard Chapitre 6

Avoir des sauvegardes des données du projet / des archives

Récupération rapide / éviter des pertes de données

E-mails ; Internet

Ne pas ouvrir tout ce qui a l'air intéressant et prometteur

Le plus important en matière de cybersécurité (4/8)

L'exploitant de la STEP peut préparer les bases

- Utiliser les outils du manuel step by STEP → utiliser l'expérience et s'informer
- Pour compléter, demander au fournisseur d'OT (DCS) et d'IT

L'exploitant de la STEP connait son environnement TIC comme sa biologie !

- La création de l'inventaire est la clé pour connaître son environnement TIC
- **L'exploitant est le patron** → ne pas déléguer

L'exploitant de la STEP décide → Mesures et norme de sécurité !

Le plus important en matière de cybersécurité (5/8)

Les systèmes TIC sont à entretenir → comme les équipements de la STEP

- Contrôle initial par le fournisseur OT et IT → création d'un catalogue de performance (step by STEP)
- Contrat de service annuel avec le fournisseur OT et IT

Expert en sécurité

- Vérifie l'infrastructure TIC et la libère → similaire à une vérification des comptes
- Conclure un accord de service

La sécurité n'est pas un état mais un processus continu

Le plus important en matière de cybersécurité (6/8)

L'exploitant de la STEP connaît son infrastructure et est responsable

Autoriser éventuellement l'accès à distance à des tiers

Infrastructure TIC OT

STEP | Ouvrages externes

Accès à distance à la STEP

Infrastructure TIC IT

Ev. accès IT à distance

Expert cyber
Contrôle et libère
Doit être neutre (pas d'intérêts)

Lors d'une réhabilitation complète, intégrer ces coûts dans le projet
- À travers les planificateurs de procédés ou électriques

Le plus important en matière de cybersécurité (7/8)

Que faire en cas de (cyber)incident ?

Mesures immédiates (plan d'action en cas d'incidents)

- Déconnecter la machine concernée du réseau → **Déconnecter le câble réseau**
- Informer les personnes responsables

Le plus important en matière de cybersécurité (8/8)

A faire → Utilisation des standards de la branche

Utilisation de l'expérience de step by STEP

STEP	Est responsable	En ce qui concerne son système de TIC : - OT - IT - Accès à distance
	Contrats de service	Exiger et définir les performances : - OT (DCS) - IT (Administration) - expert en informatique
	Mesures «cyber»	Mise en œuvre par étapes

Merci beaucoup !

Publications

VSA — Risikoexposition ICT Version DE; Version FR prévue pour début 2022

step-ara — Branchenstandard und Factsheets in DE und FR

IKT Minimalstandard Abwasser
Factsheet: Risikoexposition nimmt mit steigender Vernetzung und Nutzerzahl zu

aqua & gas — 2019/01 step by STEP
Hilfreiches Arbeitsinstrument für Kläranlagen und Industrie- und Gewerbebetriebe

2020/02 Cybersicherheit in Abwasserbetrieben
Wie Kläranlagen den IKT Minimalstandard Abwasser umsetzen können

2020/11 step by STEP und Cybersicherheit in der Praxis
Erfolgreiche Umsetzung in der Kläranlage und Anwendung im Leitsystem de contrôle.

ETAT DE FRIBOURG
STAAT FREIBURG

Service de l'environnement SEn
Amt für Umwelt AfU

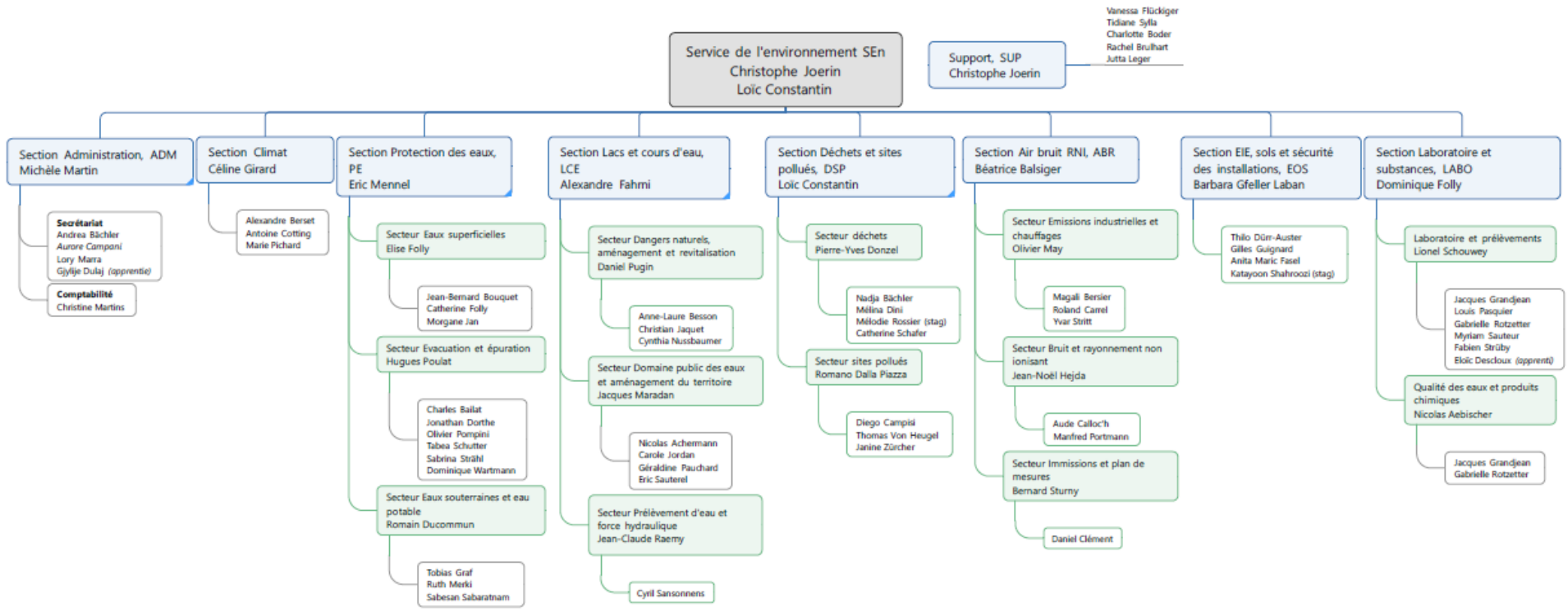
News de la section «Laboratoire et substances»

InfoSTEP 2021

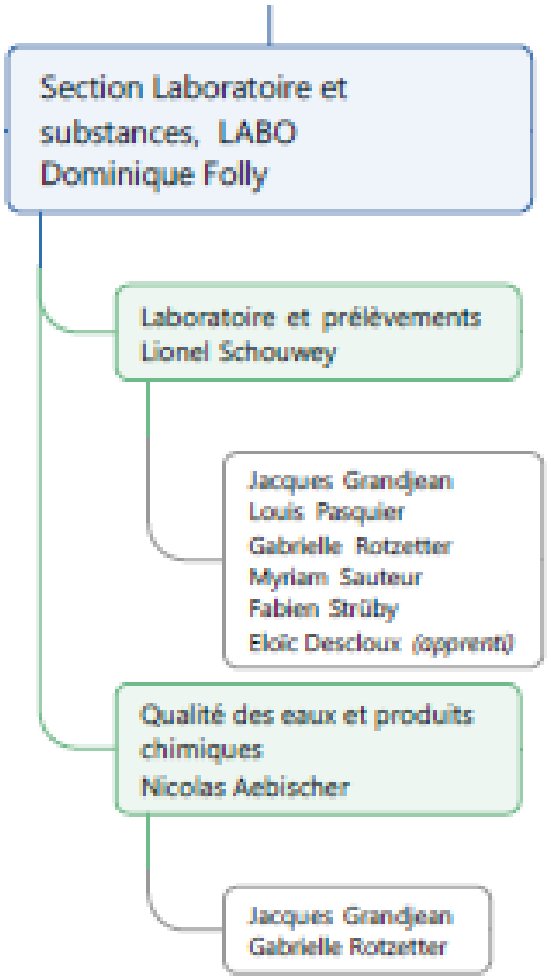
Givisiez, 13 octobre 2021

Direction de l'aménagement, de l'environnement et des constructions **DAEC**
Raumplanungs-, Umwelt- und Baudirektion **RUBD**

Restructuration de la section



Restructuration de la section



InterSTEP 2021

Cadre général

20 participants

Nouvelle base de données Lab'Eaux depuis 2019

Messagerie automatique – bilingue

Fichier excel commun

ARA Kerzers

ARA Murten

ARA Zumholz

Section laboratoire et substances

STEP Broc

STEP Bussy

STEP Charmey

STEP Delley

STEP Domdidier

STEP Ecublens

STEP Estavayer-le-Lac

STEP Fribourg

STEP Grolley

STEP Marly

STEP Montagny

STEP Pensier

STEP Romont

STEP Torny-le-Grand

STEP Villars-sur-Glâne

STEP Vuippens

InterSTEP 2021

Cadre général

Points d'améliorations

Fichier imprimable sur une page

Décimales ajustables

ARA Kerzers

ARA Murten

ARA Zumholz

Section laboratoire et substances

STEP Broc

STEP Bussy

STEP Charmey

STEP Delley

STEP Domdidier

STEP Ecublens

STEP Estavayer-le-Lac

STEP Fribourg

STEP Grolley

STEP Marly

STEP Montagny

STEP Pensier

STEP Romont

STEP Torny-le-Grand

STEP Villars-sur-Glâne

STEP Vuippens

InterSTEP 2021

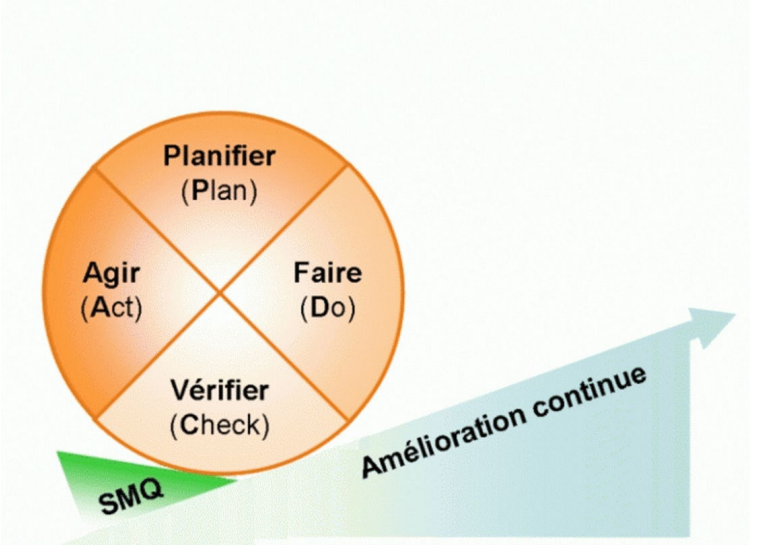
Pourquoi?

S’assurer que ses résultats routiniers soient correctes

Comparer ses pratiques avec ses pairs

Corriger d’éventuelles déviations

Documenter l’évolution de ses résultats



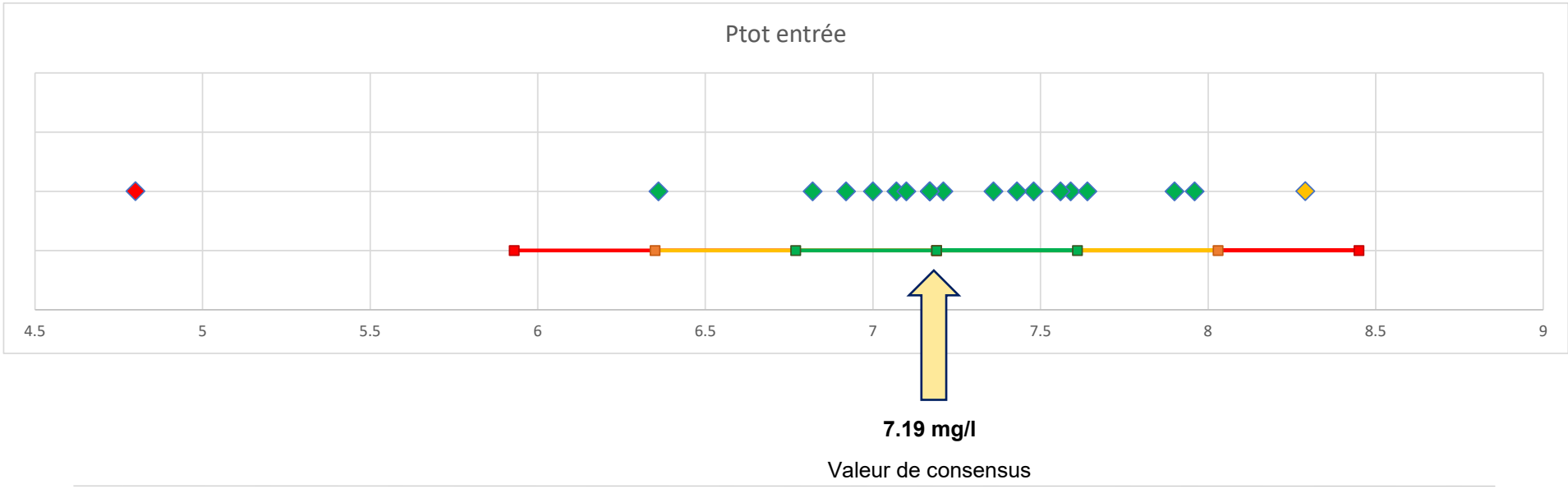
InterSTEP 2021

Z score

De façon barbare:

$$z = \frac{X - \mu}{\sigma}$$

De manière graphique:



InterSTEP 2021

Z score

InterSTEP 2021

Rapport

PARAMETRES		N	Mediane	Ecart médian lissé (rel.)	Incertitude sur la médiane (rel.)	Z>2	Z>3	Z<2
PARAMETERN		N	Median	Gemittelt Medianabweichung	Median Unsicherheit	Z>2	Z>3	
DBO5 Oxitop E	ENTREE	9	340 mg/l	21.8%	9.1%	0	1	8
DBO5 Oxitop S	SORTIE	8	4 mg/l	74.1%	32.8%	0	0	8
DBO5 Winkler E	ENTREE	12	295 mg/l	27.8%	10.0%	1	0	11
DBO5 Winkler S	SORTIE	11	2 mg/l	74.1%	27.9%	2	0	9
DCO	ENTREE	20	770 mg/l	3.2%	0.9%	1	2	17
DCO S	SORTIE	20	19 mg/l	6.9%	1.9%	1	1	18
DOC S	SORTIE	20	6.4 mg/l	16.0%	4.5%	0	0	20
MeS S	SORTIE	20	8 mg/l	18.5%	5.2%	2	1	17
N-NH4 S	SORTIE	18	0.032 mg/l	56.4%	16.6%	1	3	14
N-NO2 S	SORTIE	18	0.008 mg/l	61.8%	18.2%	1	2	15
N-NO3 S	SORTIE	20	35.2 mg/l	2.5%	0.7%	1	1	18
Ntot E	ENTREE	9	58.6 mg/l	18.5%	7.7%	1	0	8
Ntot S	SORTIE	9	36.6 mg/l	7.7%	3.2%	0	1	8
pH E	ENTREE	20	7.8	1.6%	0.4%	1	3	16
Ptot E	ENTREE	20	7.19 mg/l	5.8%	1.6%	2	1	17
Ptot S	SORTIE	20	0.32 mg/l	2.4%	0.7%	0	3	17
Snellen S	SORTIE	20	50 cm	23.2%	6.5%	0	0	20
TOC E	ENTREE	20	189 mg/l	7.8%	2.2%	2	2	16

InterSTEP 2021

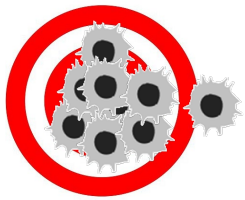
Rapport

PARAMETRES / PARAMETERN		N / N	Mediane / Median	Ecart médian lissé (rel.) / Gemittelt Medianabweichung	Incertitude sur la médiane (rel.) / Median Unsicherheit	Z>2 / Z>2	Z>3 / Z>3
DBO5 Oxitop E	ENTREE	9	340 mg/l	21.8%	9.1%	0	1
DBO5 Oxitop S	SORTIE	8	4 mg/l	74.1%	32.8%	0	0
DBO5 Winkler E	ENTREE	12	295 mg/l	27.8%	10.0%	1	0
DBO5 Winkler S	SORTIE	11	2 mg/l	74.1%	27.9%	2	0
DCO	ENTREE	20	770 mg/l	3.2%	0.9%	1	2
DCO S	SORTIE	20	19 mg/l	6.9%	1.9%	1	1
DOC S	SORTIE	20	6.4 mg/l	16.0%	4.5%	0	0
MeS S	SORTIE	20	8 mg/l	18.5%	5.2%	2	1
N-NH4 S	SORTIE	18	0.032 mg/l	56.4%	16.6%	1	3
N-NO2 S	SORTIE	18	0.008 mg/l	61.8%	18.2%	1	2
N-NO3 S	SORTIE	20	35.2 mg/l	2.5%	0.7%	1	1
Ntot E	ENTREE	9	58.6 mg/l	18.5%	7.7%	1	0
Ntot S	SORTIE	9	36.6 mg/l	7.7%	3.2%	0	1
pH E	ENTREE	20	7.8	1.6%	0.4%	1	3
Ptot E	ENTREE	20	7.19 mg/l	5.8%	1.6%	2	1
Ptot S	SORTIE	20	0.32 mg/l	2.4%	0.7%	0	3
Snellen S	SORTIE	20	50 cm	23.2%	6.5%	0	0
TOC E	ENTREE	20	189 mg/l	7.8%	2.2%	2	2

InterSTEP 2021

Rapport

pH E								ENTREE
Laboratoire Labor	Date analyse Analyse Datum	Méthode Method	N N	Min. Min.	Max. Max.	Moyenne Mittelwert	Std Dev Std Dev	Z-score Z-score
1	21.04.2021	HQ 30 D	2	7.9	7.9	7.9	0.00	0.63
2	26.04.2021	PHC101	3	8.3	8.5	8.4	0.12	4.41
3	21.04.2021	ME-pH-013	3	7.8	7.8	7.8	0.00	-0.18
4	23.04.2021	Sonde LDO Ha	3	7.8	8	7.8	0.12	0.01
5	22.04.2021	Hach HQ 40 d	2	8	8	8	0.02	1.56
6	21.04.2021	potentiométri	2	7.8	7.8	7.8	0.02	-0.22
7	21.04.2021	sonde portativ	3	7.8	7.9	7.8	0.06	0.09
8	21.04.2021		1	7.8	7.8	7.8		-0.01
9	13.05.2021	WTW	2	7	7	7	0.01	-6.69
10	20.04.2021	WTW Multi 34	2	8	8	8	0.00	1.69
11	22.04.2021	WTW 3510 ID	1	7.8	7.8	7.8		-0.18
12	21.04.2021		2	8.1	8.2	8.1	0.01	2.62
13	21.04.2020		1	7.8	7.8	7.8		0.07
14	21.04.2021		1	7.9	7.9	7.9		0.71
15	21.04.2021	Metrohm 605	3	7.9	8	8	0.07	1.20
16	21.04.2021		1	7.8	7.8	7.8		-0.09
17	21.04.2021	WTW	1	7.8	7.8	7.8		-0.18
18	21.04.2021	Hach One	3	7.6	7.7	7.7	0.06	-1.25
19	21.04.2021	pH Meter	1	7.7	7.7	7.7		-0.90
20	21.04.2021	HQ 40 D HACH	1	7.4	7.4	7.4		-3.17



Inter[illegible] 2021

Ra[illegible]

		DBO5 Oxitop S					SOR
[illegible]e	Date analys Analyse Datu	[illegible]e [illegible]od	N N	Min. Min.	Max. Max.	Moyen Mittelwer	Z-score Z-score
	26.04.2[illegible]		1			6 mg/l	0.62
	22.04.2[illegible]	[illegible]l 250 ml	2			6 mg/l	0.77
	21.04.[illegible]		1			3 mg/l	-0.31
	13.05.[illegible]	[illegible]	2			5 mg/l	0.31
	22.04.2[illegible]	[illegible]p 0-40	1			3 mg/l	-0.31
	21.04.2[illegible]		1			6 mg/l	0.62
	21.04.20[illegible]		1		1	1 mg/l	-0.93
	21.04.202[illegible]		1	1	1	1 m[illegible]	-0.93

L[illegible]itop / Win[illegible] mais écart[illegible]emblable

DBO5 [illegible]	ENTREE	9	[illegible]	9.1%	
DBO5 Win[illegible]	ENTREE	12	293 mg/l	27.8%	10.0%

InterSTEP 2021

Conclusions

♥ **Pas de tendance sur les écarts entre entrées et sorties**

E: Matrices plus compliquées / S: Analytes en faible concentration

→ *Les analyses des eaux de STEP ne sont pas des analyses faciles*

♣ **93% de résultats dans la cible**

273 résultats avec un z-score < 2, contre 21 avec un z-score supérieur à 2 (< 8%)

♦ **Attention à l'étalonnage des sondes**

Petit écart, grande conséquence

♠ **Quelques résultats aberrants**

Toujours vérifier la plausibilité, ne pas hésiter à réanalyser une seconde fois

InterSTEP 2023

Perspectives

Interlaboratoire intercantonal des STEP → 2023

- 2021: 96 laboratoires participants

- Mélange entre STEP et laboratoires cantonaux

- Statistiques plus robustes

Section laboratoire et substances

Questions

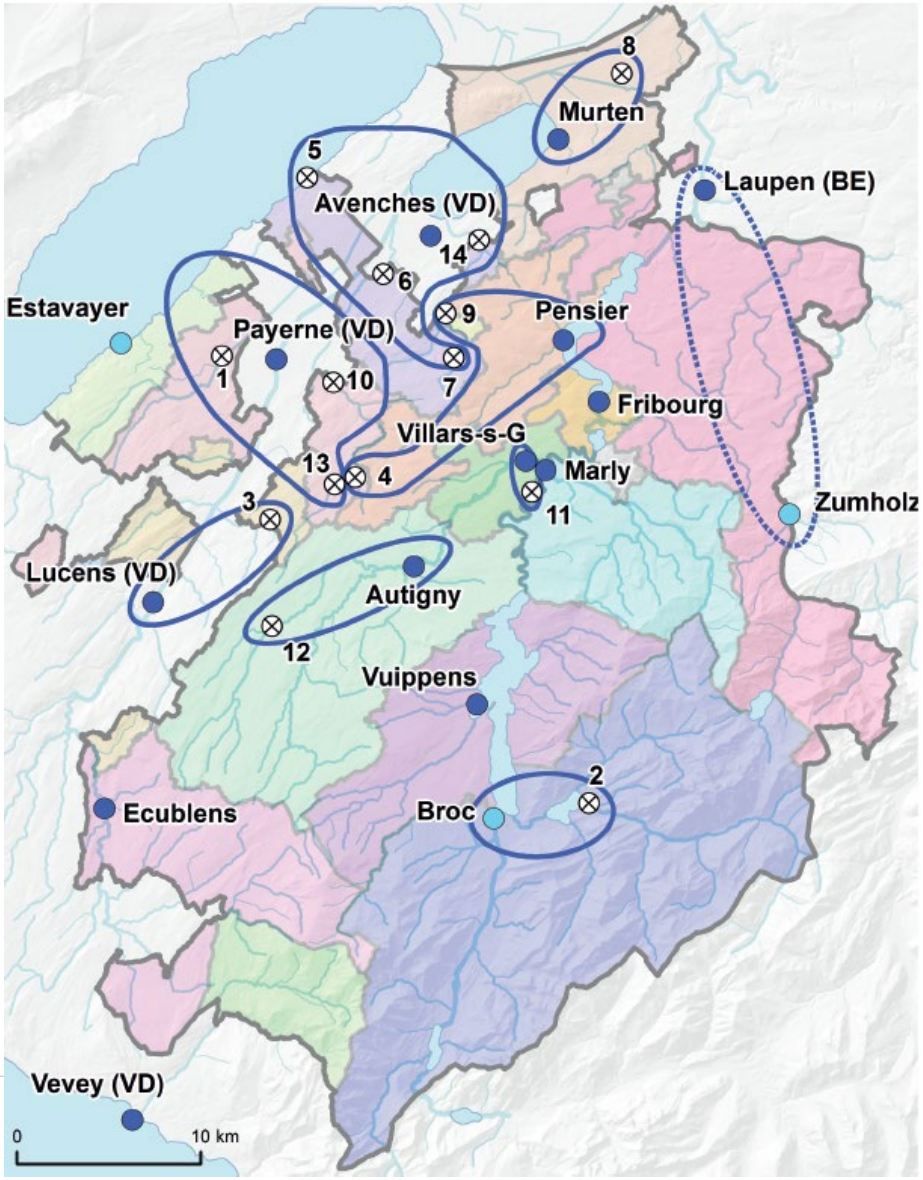
Actualités protection des eaux 2021

Actualités protection des eaux

> Planification cantonale :

- > Etat des **regroupements**
- > Etat **projets en cours**

Actualités protection des eaux



STEP centrale d'importance cantonale avec élimination des micropolluants

STEP centrale d'importance cantonale sans élimination des micropolluants

STEP à raccorder

Regroupement

Regroupement éventuel à long terme

Périmètre d'épuration de la STEP

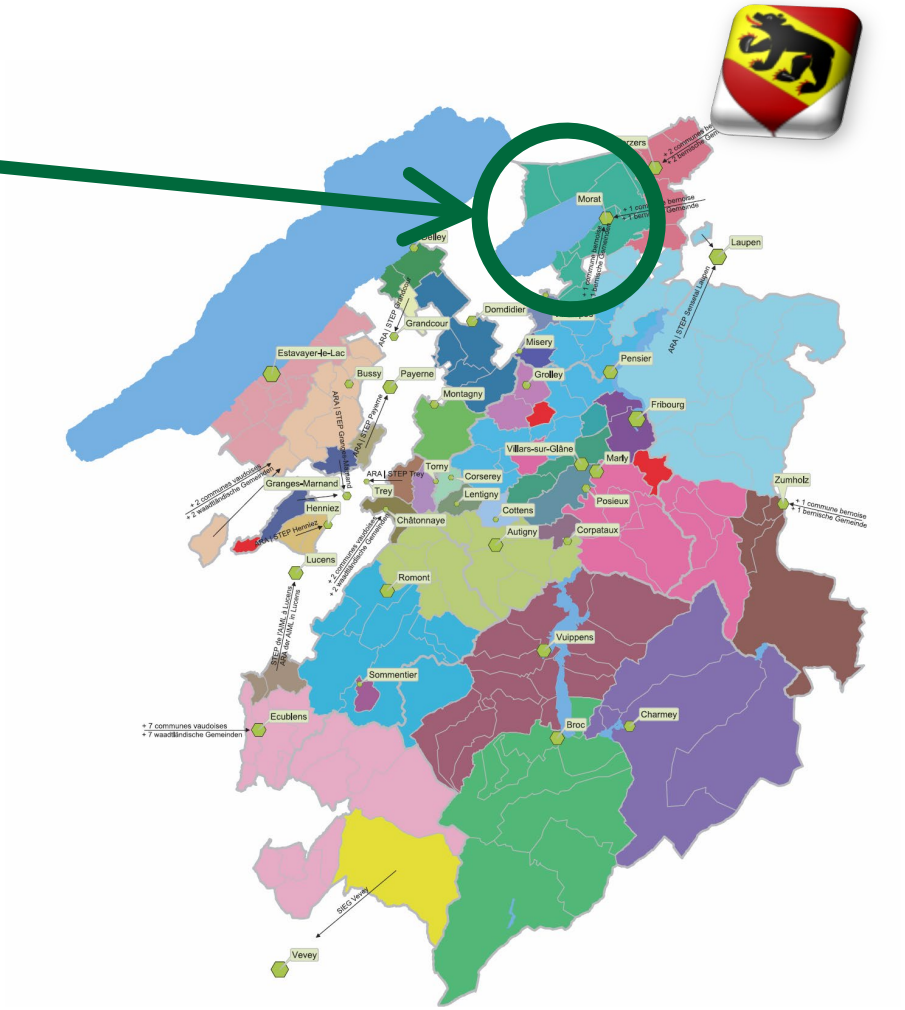
1. Bussy
2. Charmey
3. Châtonnaye
4. Corserey
5. Delley
6. Domdidier
7. Grolley
8. Kerzers
9. Misery
10. Montagny
11. Posieux
12. Romont
13. Torny
14. Villarepos

Planification cantonale de l'épuration

Région Seeland
STEP Kerzers, Morat, BE,

Projet **STEP Seeland Süd :**

- Agrandissement **82'000 EH**
- raccordement de la STEP de **Kerzers**
- traitement MP par **ozonation et filtre à sable**

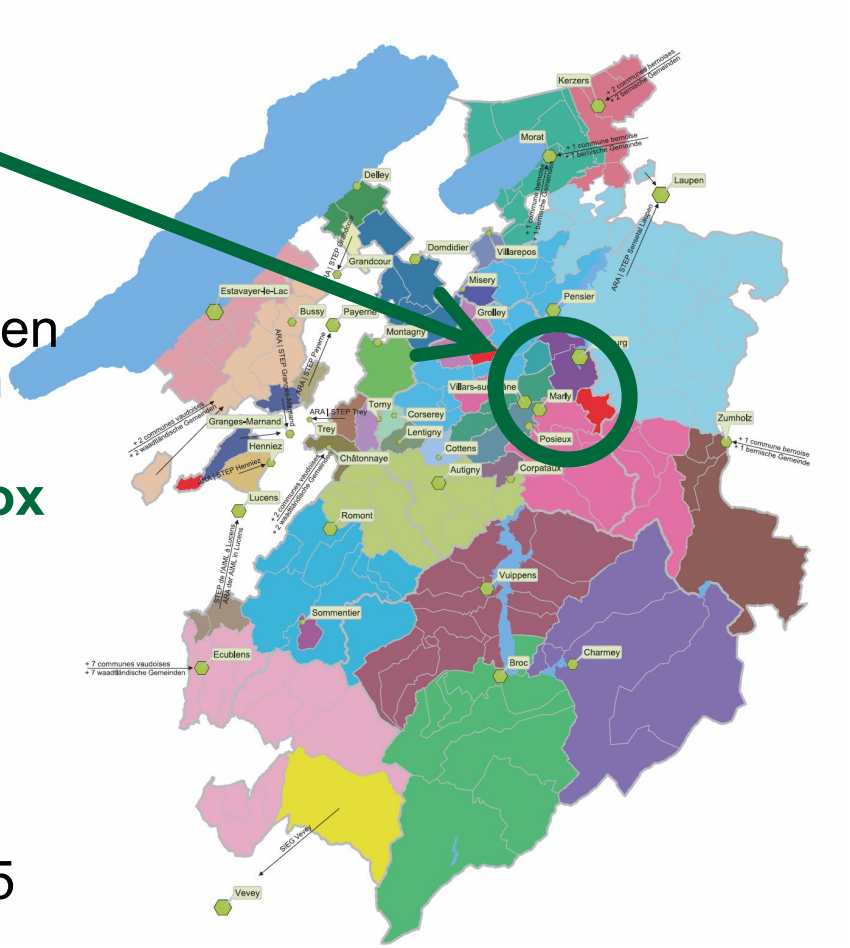


Planification cantonale de l'épuration

Région Basse Sarine
STEP Fribourg, Marly, Hauterive, Villars-s-G

STEP de **Fribourg** :
- Traitement MP par **ozonation** et filtration sur **sable bicouche** : projet en cours – REP consultation, réalisation 2025
- Essais-pilotes **nitritation** et **anammox**

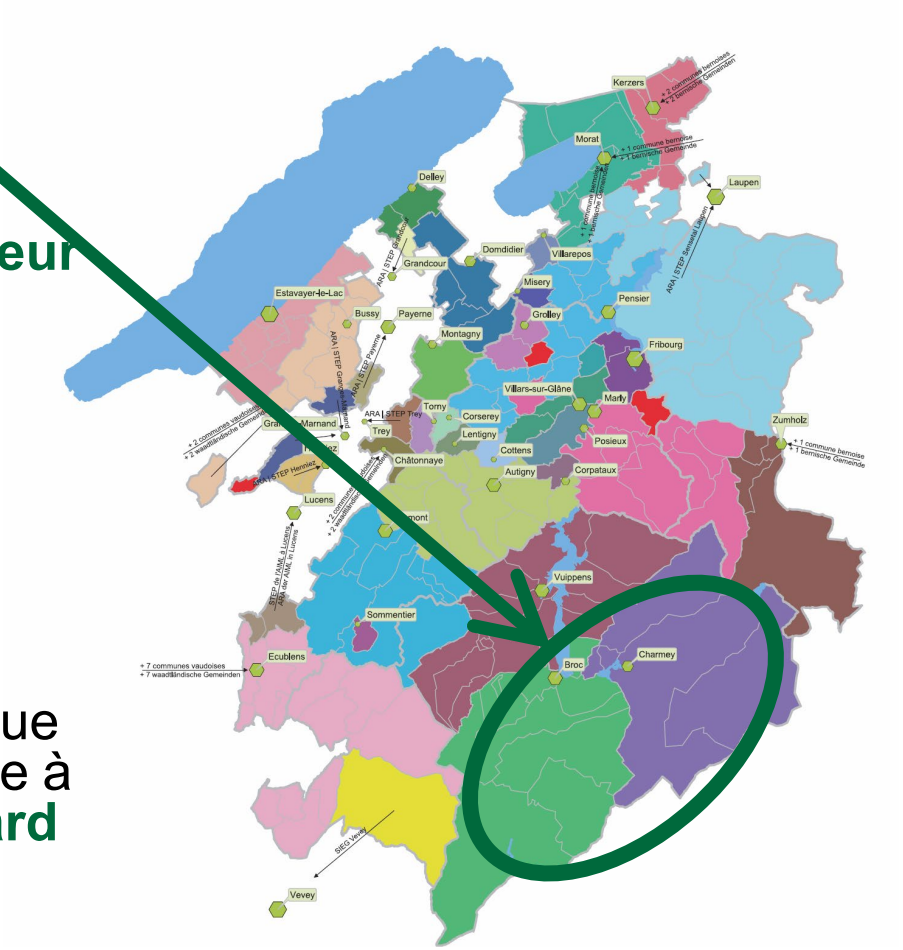
STEP de **Villars-sur-Glâne** :
- Projet **extension et réhabilitation** STEP 2045
- 50'000 EH : AVP fin 2021
- Raccordement **STEP Posieux** : 2025



Planification cantonale de l'épuration

Région Haute Gruyère
STEP Broc, Charmey

- Les 2 associations concernées (AECE et AICG) étudient **le meilleur tracé possible** pour ce raccordement.
- Une nouvelle **clef de répartition** commune aux deux STEP a été **établie.**

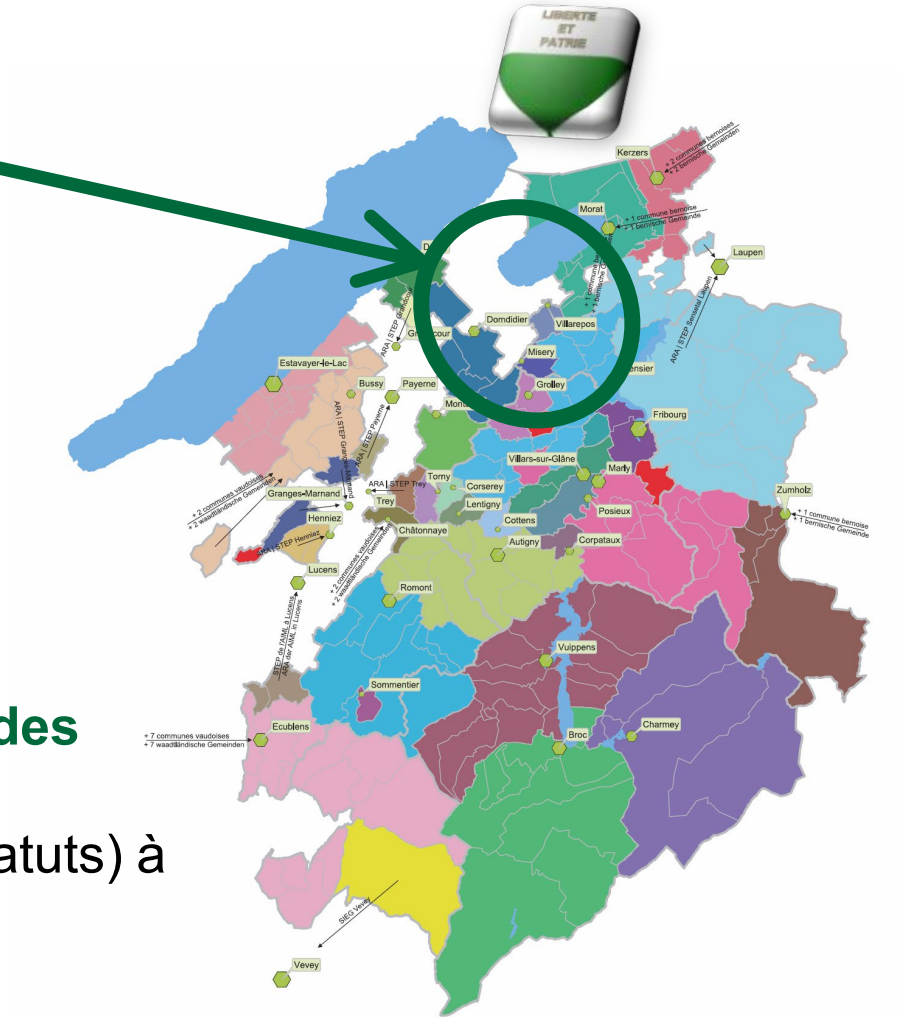


Planning **:**

- Selon la planification, il est prévu que la STEP de Charmey soit raccordée à celle de Broc **d'ici 2035 au plus tard**

Planification cantonale de l’épuration

Région Avenches
STEP Belmont-Broye, Villarepos, Grolley, Delley-Portalban, + VD

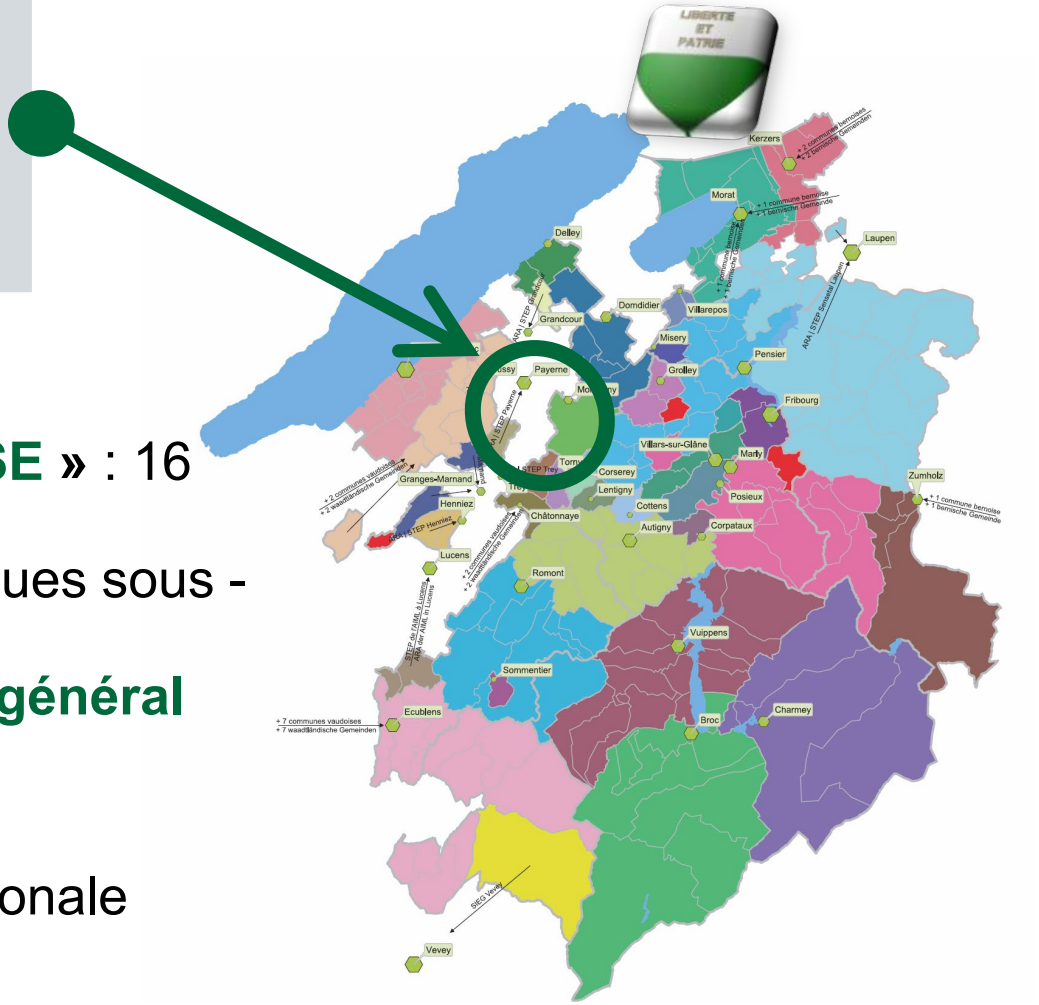


Constitution d’un **COPil régional** :
- choix d’un **BAMO**
- un **site** a été **identifié**

Planning 2021-2022**:**
- Affectation **du site** et suite des **études techniques**
- **Processus politique** constitutif (statuts) à horizon **2022**

Planification cantonale de l'épuration

Région Payerne : STEP de l'EPARSE (49'000 EH)
STEP Bussy, Torny, Montagny, VD



Depuis **2019 :**

- **Nouvelle association intercommunale « l'EPARSE »** : 16 communes (7 VD, 9 FR)
- Poursuite des études techniques sous - l'égide d'un **CODIR**
- Sélection d'un **planificateur général**

Planning **:**

- «Dans **53 mois**, la STEP régionale devrait être en fonction»

Planification cantonale de l’épuration

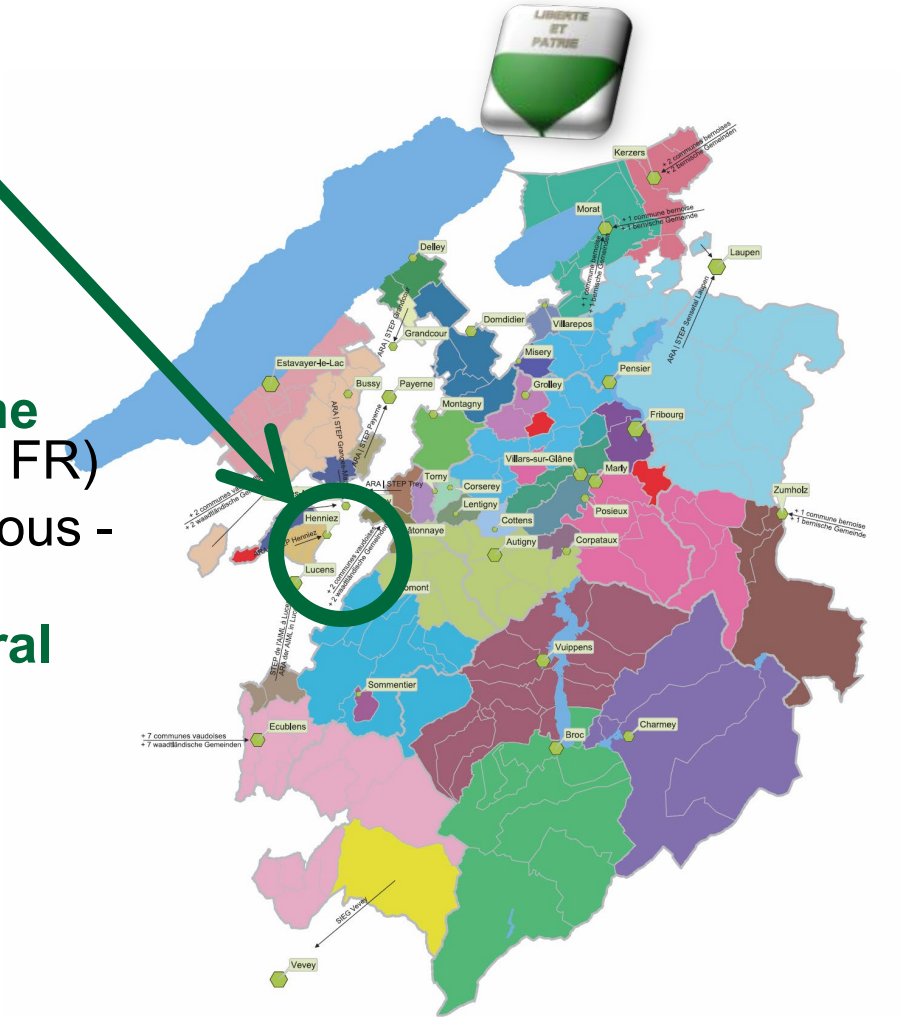
Région Lucens (60’000 EH),
STEP Châtonnaye + VD

Depuis **2019** :

- **Nouvelle association intercommunale « Eaux Moyenne Broye»** : 28 communes (22 VD, 6 FR)
- Poursuite des études techniques sous - l’égide d’un **CODIR**
- Sélection d’un **planificateur général**

Planning :

- Mise en service **fin 2026**

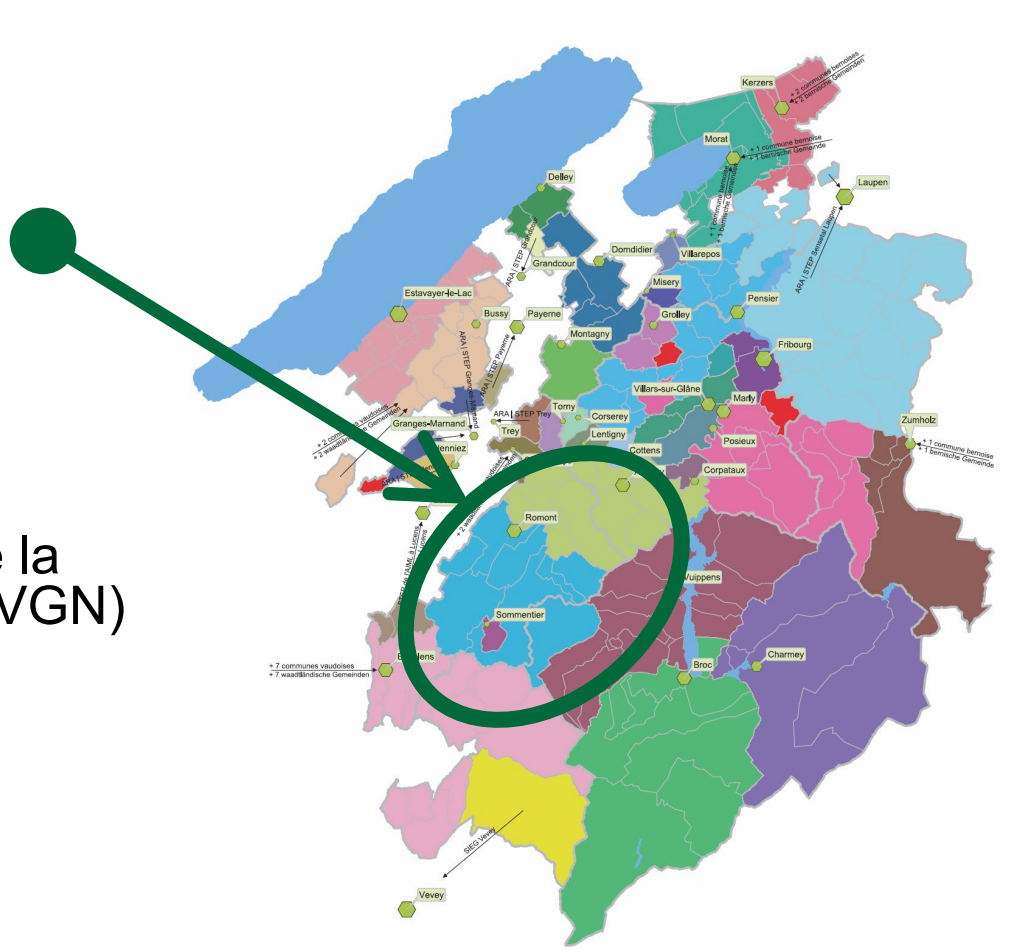


Planification cantonale de l'épuration

Région Glâne
STEP Romont, Autigny

Etude de base terminée :
- STEP **64'000 EH**

En **2020/21** :
- choix d'un **BAMO**
- Elaboration **des statuts** de la **nouvelle association** (ABVGN)



Planification cantonale de l'épuration

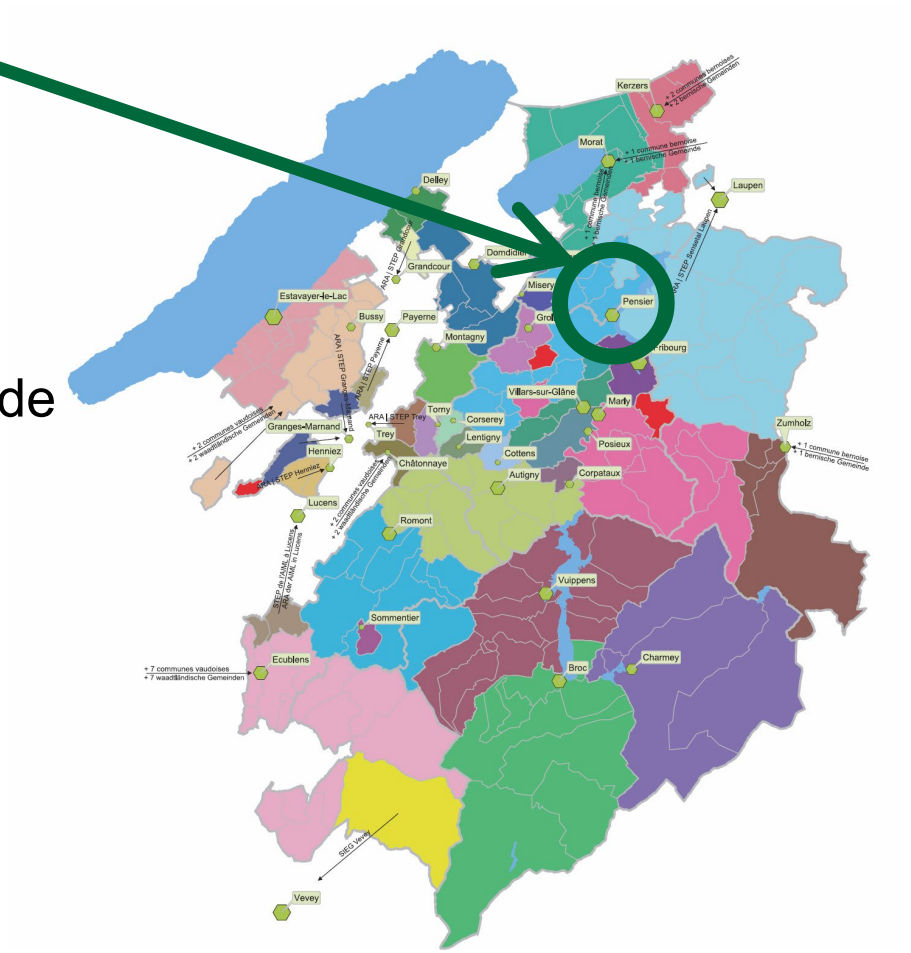
Pôle d'importance régionale
STEP de l'AESC + Misery-Courtion + Corserey

Projet **AESC 2045** :

- étude d'**extension** et **mise en conformité** (**~50'000 EH**)
- Traitement **biologique** au moyen de **biofiltres**
- Traitement des **MP** par **ozonation** suivi d'une **filtration sur sable**

Planning :

- Mise à l'enquête **printemps 2022**
- Début travaux **fin 2022**



Planification cantonale de l’épuration

Pôle d’importance régionale
STEP ERES

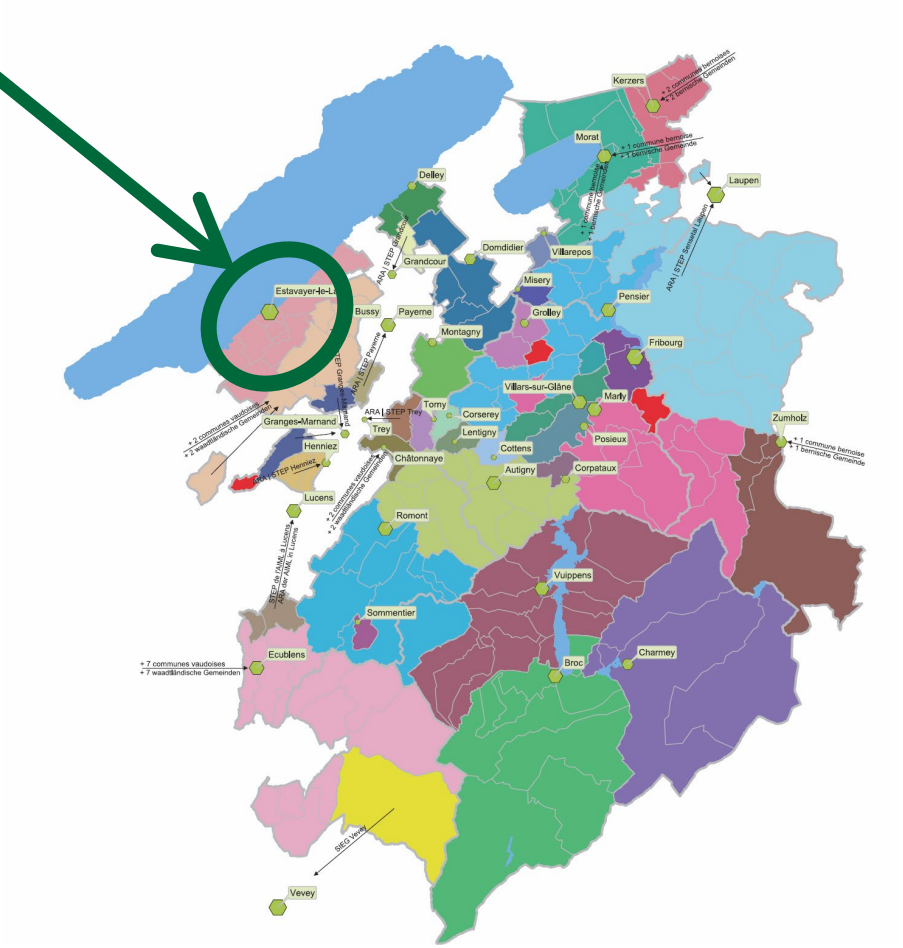
STEP d’Estavayer 2050 (80’000 EH)

- étude de **modernisation** et **d’assainissement** du traitement **biologiques, boues et gaz**

- étude de **variantes** (biofiltres et hybrides)

Planning :

- à **l’étude**



Planification cantonale de l’épuration

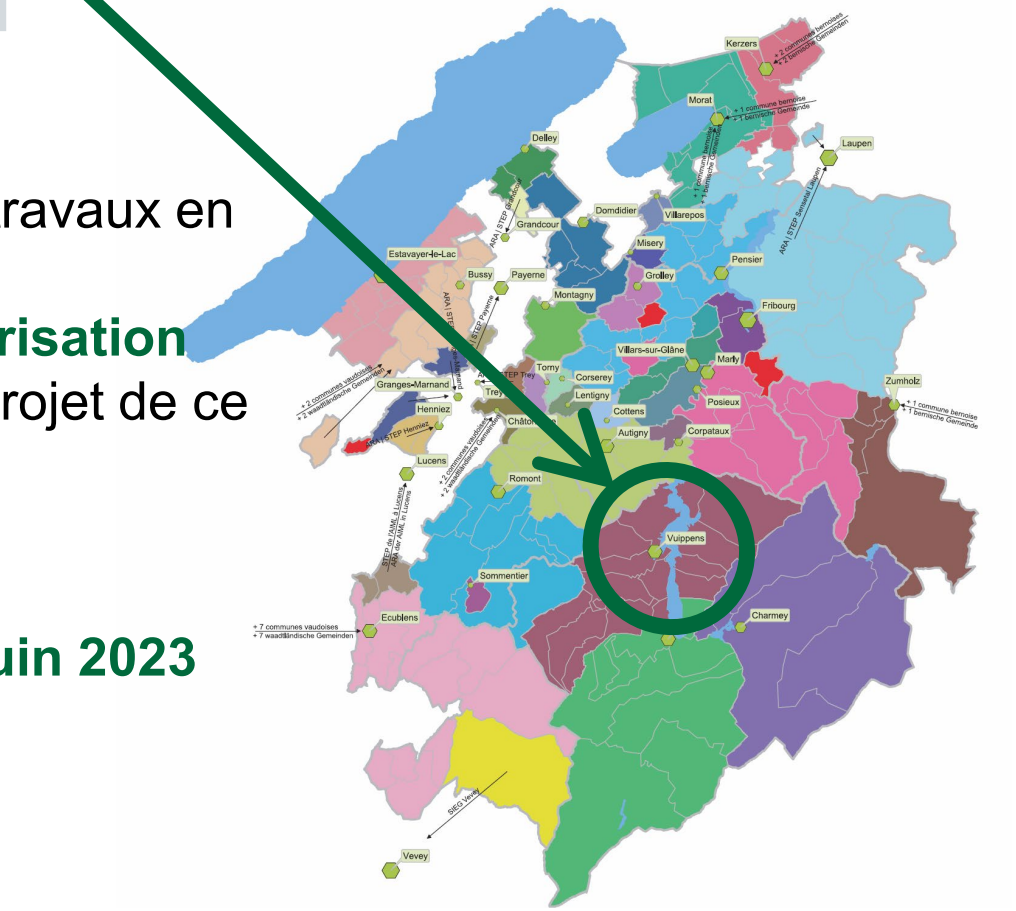
Pôle d’importance régionale
STEP AIS

STEP Vuippens (80’000 EH) :

- Agrandissement **file boues** : travaux en cours
- Centrale thermique avec **valorisation chaleur eaux polluées** : 1er projet de ce type dans canton

Planning :

- File boues : mise en service **juin 2023**
- Traitement MP : étude des **variantes en cours**



Planification cantonale de l’épuration

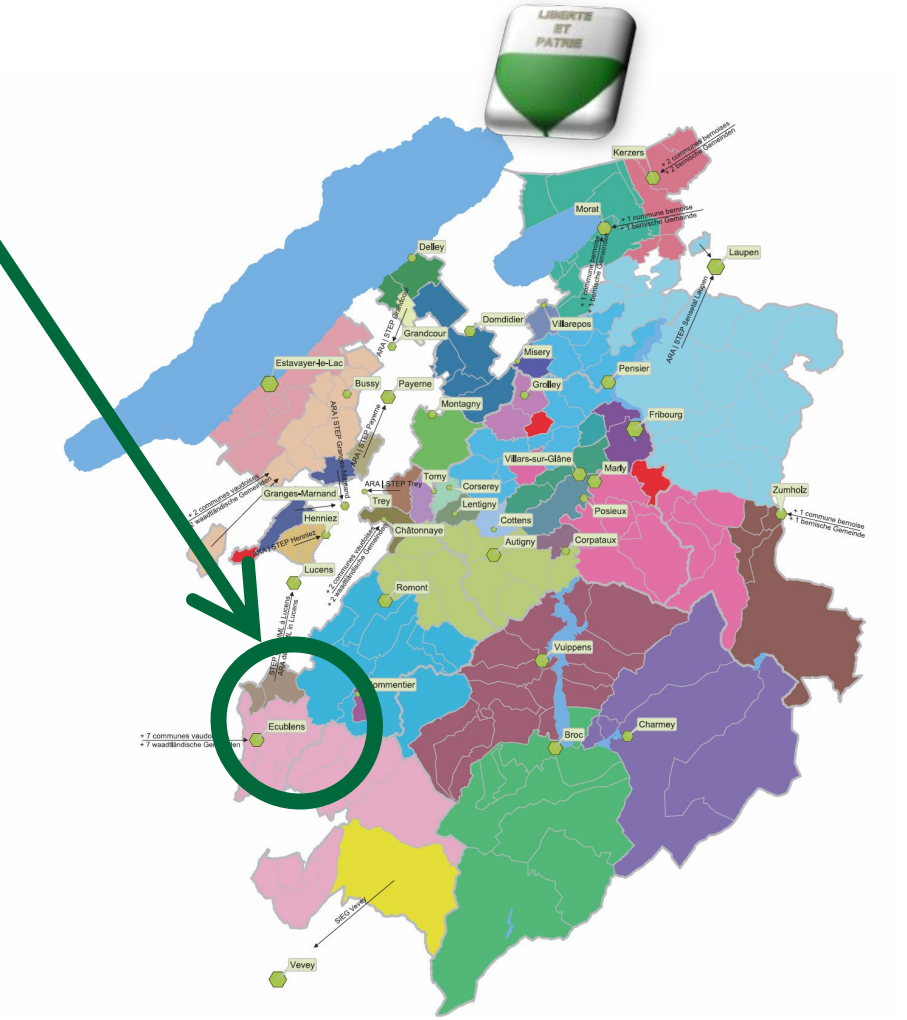
Pôle d’importance régionale
STEP VOG

Projet **VOG :**

- agrandissement de la STEP **à 48’750 EH**

Planning :

- 1ère STEP du canton **à traiter les micropolluants** (Charbon actif)
- mise en service : Juin **2022**



Questions ?