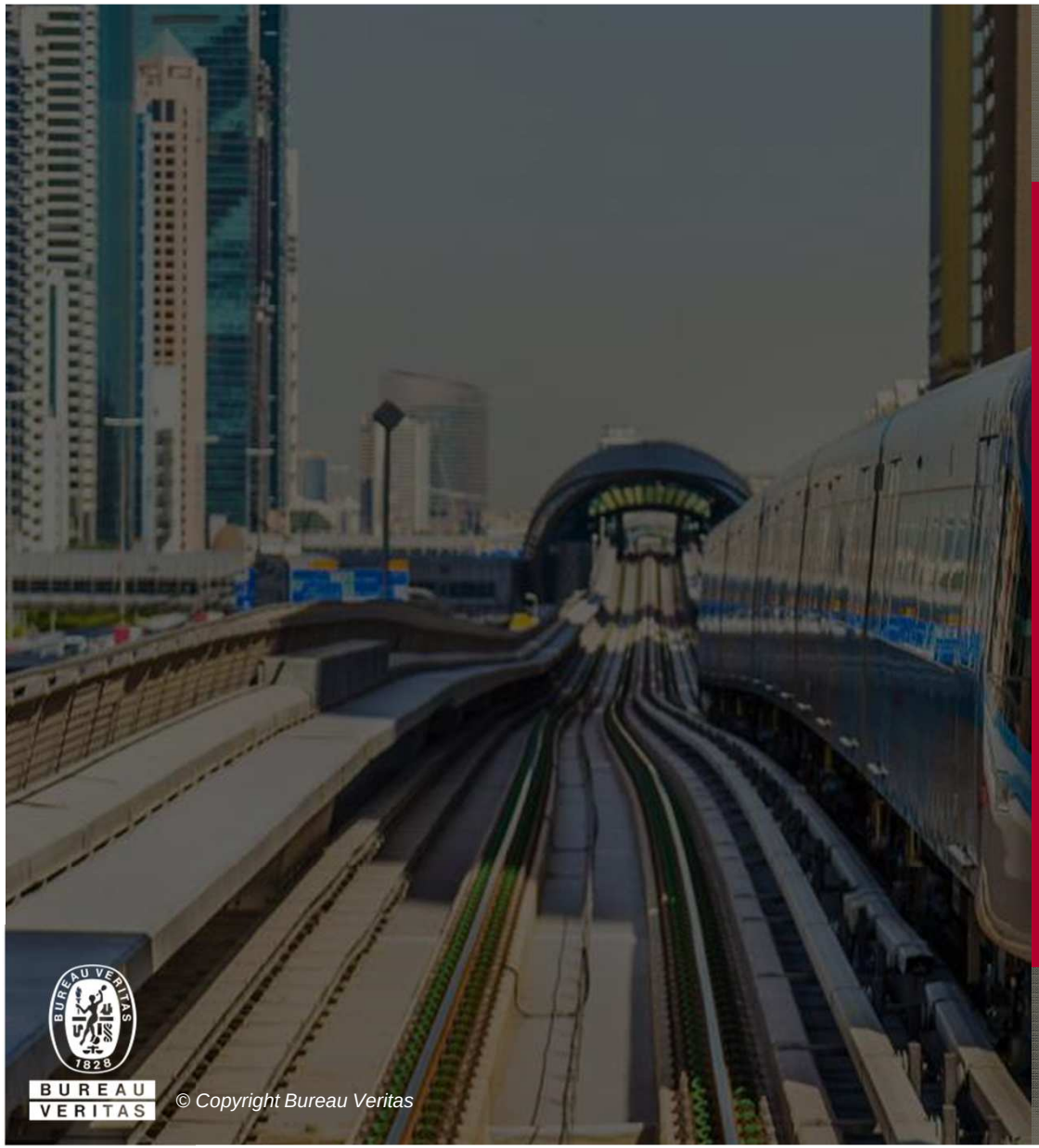
# RAIL

## QUALITY AND SAFETY THROUGHOUT THE LIFECYCLE

BARBARA SCAGLIONE – OQA T3

BENJAMIN SENECHAL – EVALUATEUR T3 IB

# SOMMAIRE



# 01

## Acceptation d’activités d’évaluations assurées par d’autres organismes

# CONTEXTE

## OBJET DE LA PRÉSENTATION

Les projets de rénovation ou de construction de systèmes ferroviaires peuvent impliquer l'utilisation d'équipements électroniques programmables répondant aux exigences de niveaux de SIL de la norme CEI 61508 et certifiés selon cette norme.

***Présenter les conditions d'acceptation d'un équipement certifié selon la norme CEI 61508 pour une utilisation en sécurité.***

01

# ACCEPTATION D'ACTIVITÉS D'ÉVALUATIONS ASSURÉES PAR D'AUTRES ORGANISMES

## RECENSEMENT DES DIFFÉRENTES SITUATIONS QUI SE PRÉSENTENT

**Possibilités**

- Le dossier de sécurité du composant a été l'objet d'une évaluation indépendante de produit ou d'application générique (au sens de la norme EN 50129 § 5.5.1) dans le cadre d'une certification par un organisme **accrédité et/ou reconnu** ;
- L'organisme est reconnu mais l'application générique (EN 50129 § 5.5) concernée peut apparaître **hors du domaine** prévu d'application ;
- Le dossier de sécurité du composant a été l'objet d'une évaluation indépendante par un organisme **non reconnu**, par exemple dans le cadre d'une homologation ;
- *Le dossier de sécurité du composant a été l'objet d'une évaluation indépendante dans le cadre d'une certification selon la norme* **CEI 61508** *par un organisme* ***reconnu*** *;*

> *L'existence d'un certificat établi par un organisme accrédité et/ou reconnu permet de dégager la responsabilité de l'évaluateur sur ces parties couvertes par d'autres organismes*

# ACCEPTATION D'ÉVALUATIONS CEI 61508 ASSURÉES PAR D'AUTRES ORGANISMES

## VALIDITÉ D'UN CERTIFICAT OU D'UNE ÉVALUATION INDÉPENDANTE

**Organisme certificateur**

- **Doit disposer d'une accréditation par un organisme signataire d'un accord de reconnaissance mutuelle (membre du IAF ou du EA : http://www.cofrac.fr/fr/international/accords.htm).**
- **Le composant certifié est utilisé correctement c'est-à-dire dans des environnements couverts par le certificat et associé à un traitement correct des réserves éventuelles ou des clauses particulières d'utilisation**

**Critères de Réutilisation**

**Pour le matériel** : Limitation possible de qualification au-delà de $10^6$ heures de service (50 129) – Défaut Systématique.
**Pour le logiciel** : Justification de la capacité du logiciel à satisfaire les exigences de Sécurité et à ne pas interférer négativement sur les autres parties du système.

**Le point essentiel de la réutilisation d'un composant est de maîtriser totalement son comportement lors de son intégration et de son utilisation.**

- **L'ensemble des exigences de sécurité obtenues à partir de l'analyse des défaillances potentielles. Vis-à-vis de toutes les défaillances possibles, l'analyse de sécurité qui doit être présentée – y compris sur un composant réutilisé – doit donner lieu à une mise en relation entre les protections et les défaillances.**
- **La validation doit porter sur l'ensemble du produit intégrant le composant réutilisé et couvrant les mécanismes de protection associés au composant à intégrer.**
- **Concernant les niveaux d'intégrité de sécurité de ces équipements, et les mesures cibles de défaillances pour une fonction de sécurité, il y a nécessité de vérifier que le niveau de SIL présenté reste conforme au tableau 3 (et non le tableau 2) du §7.6.2.9 de la norme IEC 61508-1 (Le mode de fonctionnement applicable aux équipements ferroviaires doit être le mode « demande élevée ou continue». Dans ce cas, les tableaux de niveaux de SIL des normes EN 50129 Annexe A et IEC 61508-1 tableau 3 sont considérés comme acceptables – objectif de défaillance.**

*Bureau Veritas considère que les normes actuelles (CENELEC ) développent assez peu les aspects liés à l'utilisation de COTS. L'approche ne peut pas rester purement « boite noire » dans les systèmes critiques*

# ACCEPTATION D'ACTIVITÉS D'ÉVALUATIONS CEI 61508 ASSURÉES PAR D'AUTRES ORGANISMES

## NIVEAUX D'EXIGENCES SELON NIVEAU DE SÉCURITÉ

SIL Ferroviaire (CENELEC) est différent du SIL (CEI 61508)

Niveau 0 | Niveau 1 | Niveau 2 | Niveaux 3 | Niveaux 4

- **La norme EN 50128 utilise les niveaux SIL (« System Integrity Level ») de criticité des systèmes, plus la criticité est élevée, plus les tâches, les vérifications et validations à effectuer seront nombreuses, dans ce cadre les activités à réaliser pour les niveaux SIL 1 et SIL 2 sont identiques, tout comme pour les niveaux SIL 3 et SIL 4**
- **Au sein de l'EN 50129, le niveau de SIL se définit de manière analogue à CEI 61508: suivant la criticité d'une défaillance pour les utilisateurs ou l'environnement du système, et un taux de diminution de défaillance souhaité. Il est noter que pour le logiciel (EN 50128 / CEI 61508), la définition du niveau de SIL ne fait pas référence aux taux de défaillance.**

> *L'évaluation d'un produit (système ou logiciel) consiste à évaluer la conformité de ce produit par rapport aux exigences d'un référentiel.*

# ACCEPTATION D'ACTIVITÉS D'ÉVALUATIONS CEI 61508 ASSURÉES PAR D'AUTRES ORGANISMES

## NIVEAUX D'EXIGENCES SELON NIVEAU DE SÉCURITÉ CENELEC

### Exigences de Bureau Veritas

**Niveau 0**

- **Prouver qu'il ne réalise pas de fonction de sécurité**
- **Prouver l'innocuité/indépendance du composant par exemple par l'analyse des effets des défaillances**

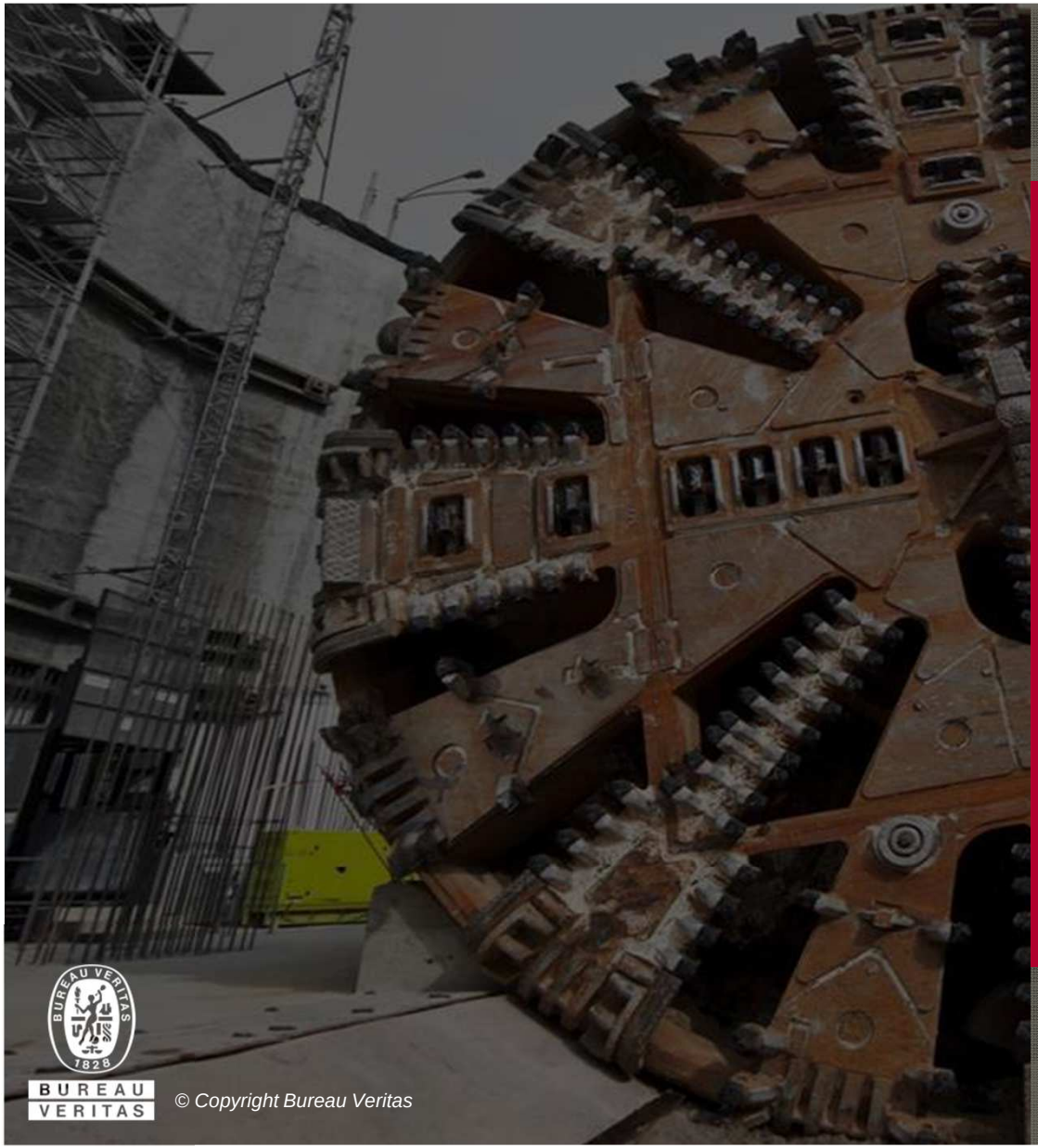
**Niveaux 1 ou 2**

- **Composant à inclure dans le processus de validation et être clairement identifiés et documentés - Traçabilité documentaire**
- **Identifier les fonctions du COTS non utilisées, et les mesures prises pour que ces fonctions n'interfèrent pas avec les fonctions utilisées**
- **Exhaustivité des rapports d'anomalies : l'historique en service peut être exploité pour compenser les non-conformités avec des contraintes (parades) strictes lorsque celles-ci sont possibles. Adéquation totale des environnements d'utilisation précédente avec celui de la nouvelle application**

**Niveaux 3 ou 4**

- **En plus des exigences du niveaux 1 et 2**
- **Analyse des défaillances potentielles dans le système qui inclut le composant réutilisé**
- **Stratégie de détection des défaillances et de protection du système (à définir et valider)**
- **Les composants doivent avoir documentation suffisante et disponible pour évaluation**
- **Inclure la documentation du composant dans le dossier de sécurité**

*"La notion de preuve à l'utilisation antérieure nécessite une documentation suffisante pour couvrir les pannes systématiques."*



# 02

Principe d’évaluation d’un constituant déjà évalué – Projet **T3 IB**

02

# PRINCIPE D'ÉVALUATION D'UN CONSTITUANT DÉJÀ ÉVALUÉ – PROJET T3 IB

## CONTEXTE

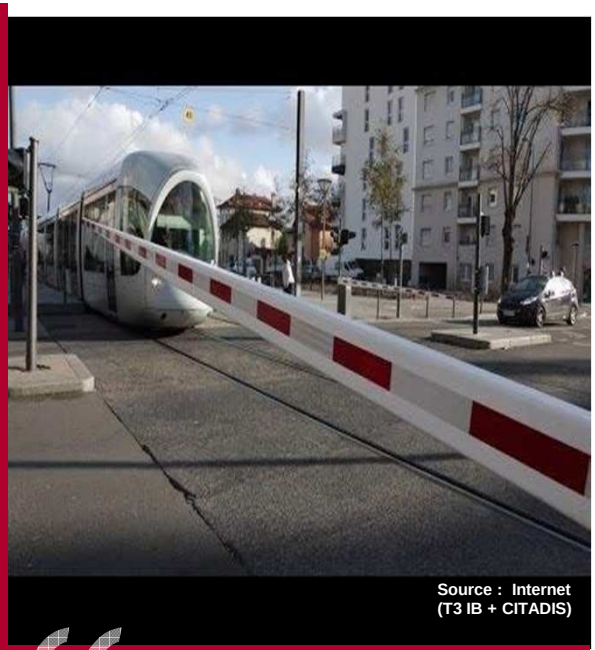
La ligne T3 du réseau de transports Lyonnais présente la particularité d'être équipée d'intersections barriérées (IB), permettant la sécurisation des croisements entre véhicules ferroviaires et usagers de la voie publique (VP)

Cette présentation porte sur le dossier « la remise à niveau des intersections barrièrées (IB) de la ligne T3» dans le cadre du projet de l'aménagement de la ligne T3 du tramway.

Ce projet de refonte du fonctionnement des IB consistait à réaliser des:

- **modifications des principes de signalisation ferroviaire;**
- **modifications de la signalisation routières des IB.**

*Dans ce cadre, l'OQA suite à l'évaluation du dossier d'intention « « Refonte des IB version 0.6 » a considéré nécessaire que les risques résiduels des feux antagonistes (SF, R24) et de la remontée intempestive des barrières devraient être traités, de manière à obtenir un niveau équivalent à celui offert par un contrôleur de carrefour (SIL3 ou supérieur).*



Source : Internet (T3 IB + CITADIS)

*« La récupération d'un certificat pour l'automate générique permet de ne pas réitérer le processus d'évaluation (voir critère 6.4.4.2 de la norme EN50128:2011). »*

02

# PRINCIPE D'ÉVALUATION D'UN CONSTITUANT DÉJÀ ÉVALUÉ – PROJET T3 IB

## CONTEXTE

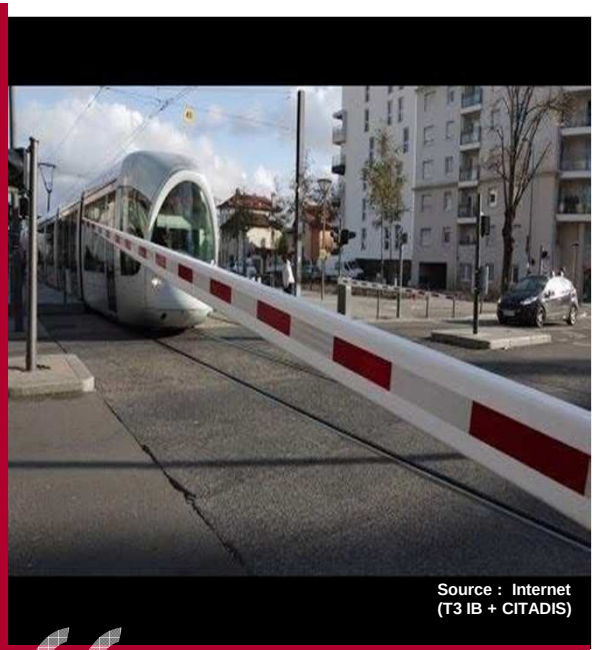
CEGELEC Mobility a assuré la réalisation et l'implémentation des **28 logiciels spécifiques** de sécurité des intersections barriérées (IB) de la ligne 3 du tramway de Lyon, implémentées **dans l'automate de sécurité** SIEMENS SF-315F (**plateforme générique**).

Le rôle de **Automate Programmable de Sécurité - APS** est d'assurer la gestion du franchissement de l'IB au travers des fonctions de sécurité.

- **Les fonctions logicielles sécuritaires développées dans l'APS répondent à l'objectif de sécurité SIL2.**
- **Les fonctions de sécurité nécessitant un niveau de sécurité supérieur ne sont pas réalisées par l'APS.**

Cet automate a été certifié **SIL3** selon la norme **CEI 65108** par un autre organisme accrédité, en tant que plateforme générique. Il contient :

- **Logiciel et l'environnement de développement – F-STEP7 SAFETY ADVANCED , incluant le TIA Portal et le compilateur ;**
- **Les blocs logiciels de base;**
- **La séparation stricte des exécutions des fonctions sécurité;**
- **Mode de repli sécuritaire en cas de défaut;**



Source : Internet (T3 IB + CITADIS)

*"Bureau Veritas, par ce processus, accepte d'etendre l'application du critère 6.4.4.2 de la norme EN50128:2011 afin d'inclure un certificat CEI 61508."*

BUREAU VERITAS

02

# PRINCIPE D'ÉVALUATION D'UN CONSTITUANT DÉJÀ ÉVALUÉ – PROJET T3 IB

## FONCTIONS DE SECURITE

**Le rôle de l'APS est d'assurer la gestion du franchissement de l'IB au travers des fonctions de sécurités suivantes:**

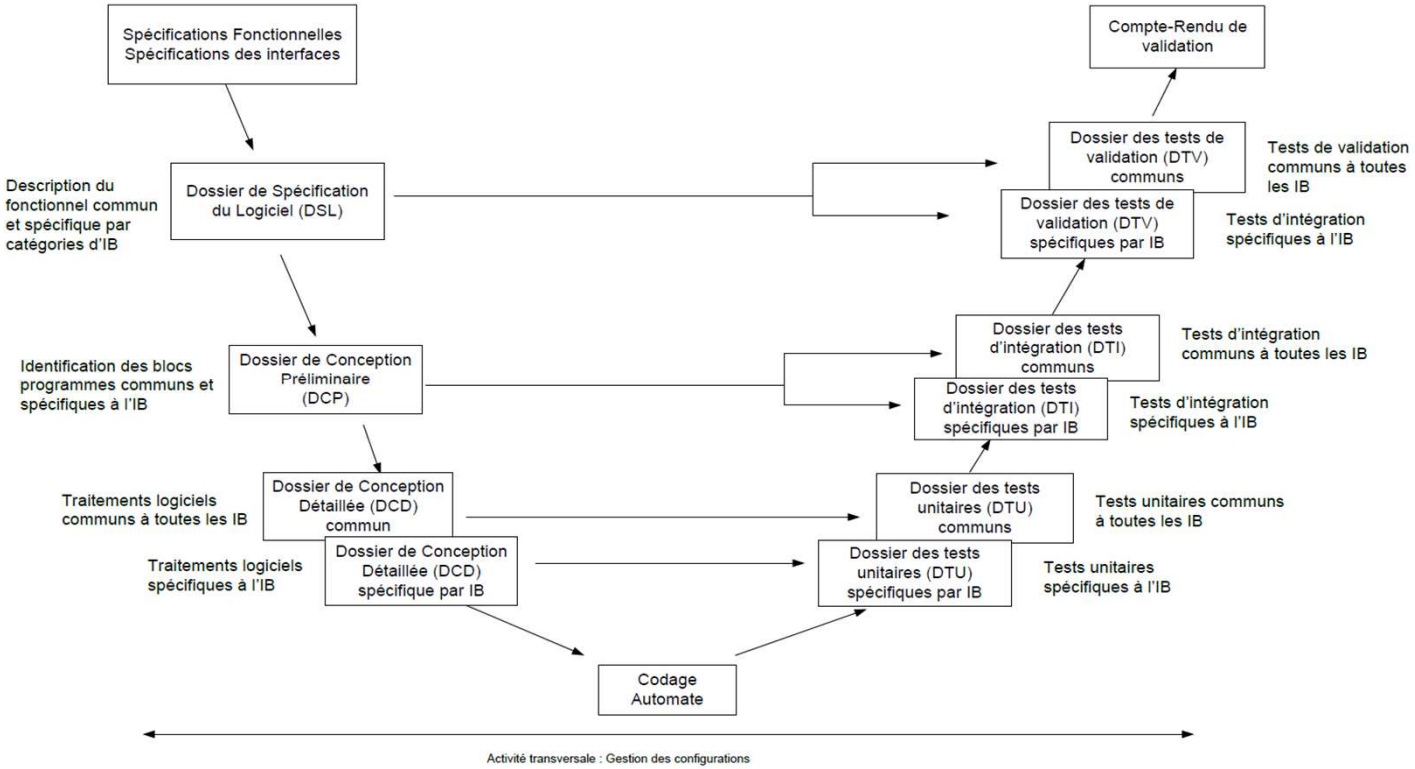
| | |
|---|---|
| ▪ **F1 : Détecter les tramways**<br>▪ F1-2 : Détecter les tramways en zone de sécurité<br>▪ F1-2-1 : Détecter les tramways en ZS1<br>▪ F1-2-2 : Détecter les tramways en ZS2<br>▪ F1-2-3 : Détecter les tramways en ZS3 | **Module « Détection TW »** |
| ▪ **F2 : Gérer le fonctionnement de l'intersection**<br>▪ F2-1 : Gérer les demandes de passage (gestion des échanges avec l'API)<br>▪ F2-2 : Gérer l'ouverture de l'intersection pour les tramways | **Module « Gestion passage IB »** |
| ▪ F2-3 : Gérer la fermeture de l'intersection pour les tramways | **Module « Fermeture IB»** |
| ▪ **F3 : Signaler l'état de l'intersection**<br>▪ F3-1 : Signaler l'état de l'intersection aux usagers VP<br>▪ F3-2 : Signaler l'état de l'intersection aux agents de conduite | **Module « Commande SF»** |
| ▪ **F6 : Gérer l'interface SIGF-ZdM (acquisition des zones de sécurités)** | **Module « Détection TW »** |

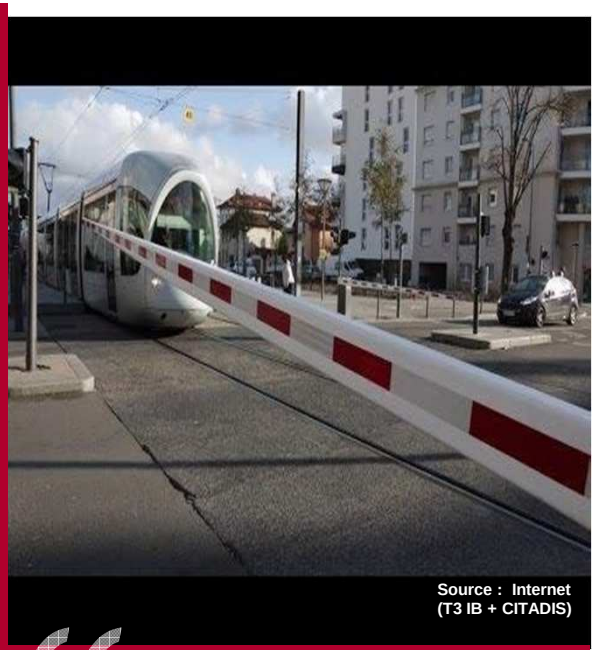
Source : Internet (T3 IB + CITADIS)

*"Les automates de gestion IB (AP-IB) sont constitués d'une partie API (Automate Programmable Industriel non sécuritaire) et d'une partie APS (Automate Programmable de Sécurité) et des specificités par IB"*

# PRINCIPE D'ÉVALUATION D'UN CONSTITUANT DÉJÀ ÉVALUÉ – PROJET T3 IB

## CYCLE DE VIE – PAR GROUPE D'IB



Source : Internet (T3 IB + CITADIS)

*"Les fonctions de sécurité nécessaires à l'exploitation en sécurité d'une IB sont réalisées suivant les règles décrites dans les documents qualité; intégrant les principes de mise en oeuvre de l'outil S7 Safety Advanced spécifiées par le constructeur."*

02

# PRINCIPE D'ÉVALUATION D'UN CONSTITUANT DÉJÀ ÉVALUÉ – PROJET T3 IB

## LES ACTIVITÉS TOUT AU LONG DU PROCESSUS D'ÉVALUATION

Les études de sécurité ont démontré un besoin de sécurité **SIL 2** pour certaines fonctions qui sont assurées par la solution logicielle et matérielle basée sur les automates de sécurité SIEMENS S7.

**Dans ce cadre, les activités ci-dessous ont été réalisées:**

- **Evaluer tout autre document (du fournisseur ou du certificateur) afférant au produit ou sous-système réutilisé et qui serait nécessaire pour acquérir la confiance suffisante pour l'acceptation d'utilisation du produit.**
  - Le système possède un certificat de sécurité pour le niveau d'intégrité de sécurité défini (validité, restrictions et conditions d'utilisation) ;
  - Le système répond aux besoins spécifiés au titre de l'opération y compris son parametrage ;
  - Le système bénéficie d'un retour d'expérience en exploitation dans un contexte équivalent;
  - La démonstration de sécurité et les hypothèses associées du système proposées sont applicables dans le contexte de l'opération.
- **Evaluer la démonstration du respect des préconisations d'utilisation du fournisseur afin de confirmer que les interactions matériel/logiciel sont maitrisées (manuel de sécurité conforme CEI 61508). En cas de non respect, pouvoir démontrer l'acceptation par l'organisme d'évaluation et/ou le fournisseur de l'écart.**
  - Evaluer la définition et formalisation des exigences de sécurité qui concernent l'automate y compris environnementalles.
  - Utilisation conforme des outils certifiés (Compilateur, environnement de test, etc)
  - Evaluer la conception et réalisation (Architecture, Codage, Traçabilité des exigences).
  - Evaluer le processus et activités de vérification et validation incluant bien l'automate, ainsi que les résultats d'intégration.
  - Evaluer la maîtrise de la configuration et des modifications ainsi que la traçabilité documentaire.

Source : Internet (T3 IB + CITADIS)

*« Bureau Veritas évalue le respect des critères de la EN NF 50128:2011 § 8 « Développement de données d'application ou d'algorithmes d'application : systèmes configurés par des données d'application ou par des algorithmes d'application »*

# 03

## Conclusions

# CONCLUSION

## UTILISATION D'UN AUTOMATE CERTIFIE – CEI 61508

*Bureau Veritas considère qu'il est acceptable d'utiliser un automate certifié selon la norme CEI 61508 si la démonstration inclut les aspects suivants :*

- Définition du niveau de SIL des fonctions (incluant l'automate) conforme à la norme EN NF 50129.
- Certificat valide émis par un organisme signataire d'un accord de reconnaissance mutuelle (membre du IAF ou EA).
- Niveau de SIL de l'automate selon le §7.6.2.9 de la norme IEC 61508 – Demande élevée ou Continue.
- Suffisance du retour d'expérience (environnement similaire), recommandé.
- Respect des conditions d'application (inclus l'environnement et l'utilisation de l'outillage) et/ou restrictions telles que définies dans le manuel de sécurité (CEI 61508).
- Respect des critères de la norme EN NF 50128:2011 § 8 pour le développement logiciel « Développement de données d'application ou d'algorithmes d'application : systèmes configurés par des données d'application ou par des algorithmes d'application » ainsi que la traçabilité documentaire.

BUREAU VERITAS

# 04

Questions


BUREAU
VERITAS

*Move Forward with Confidence*