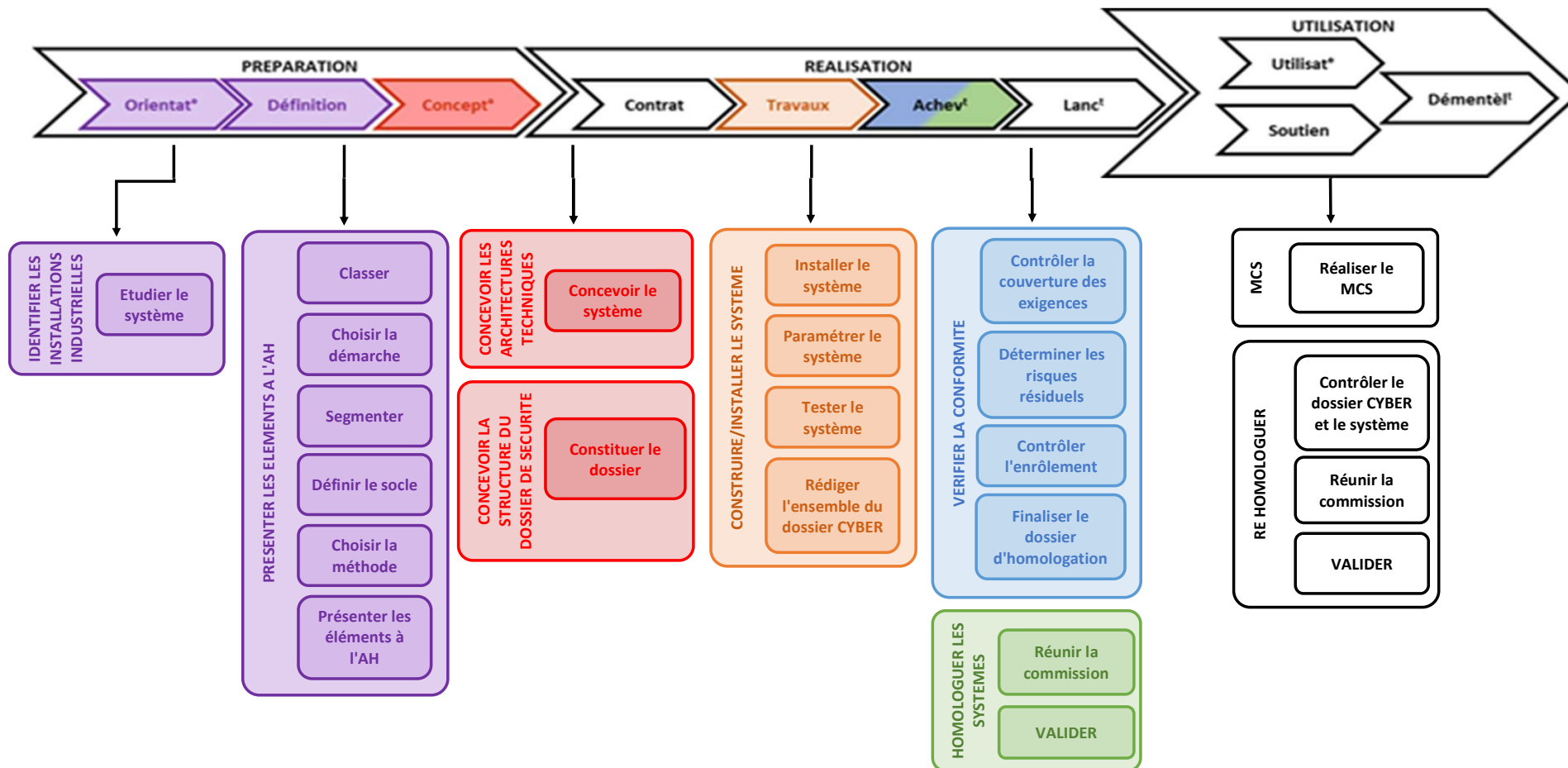
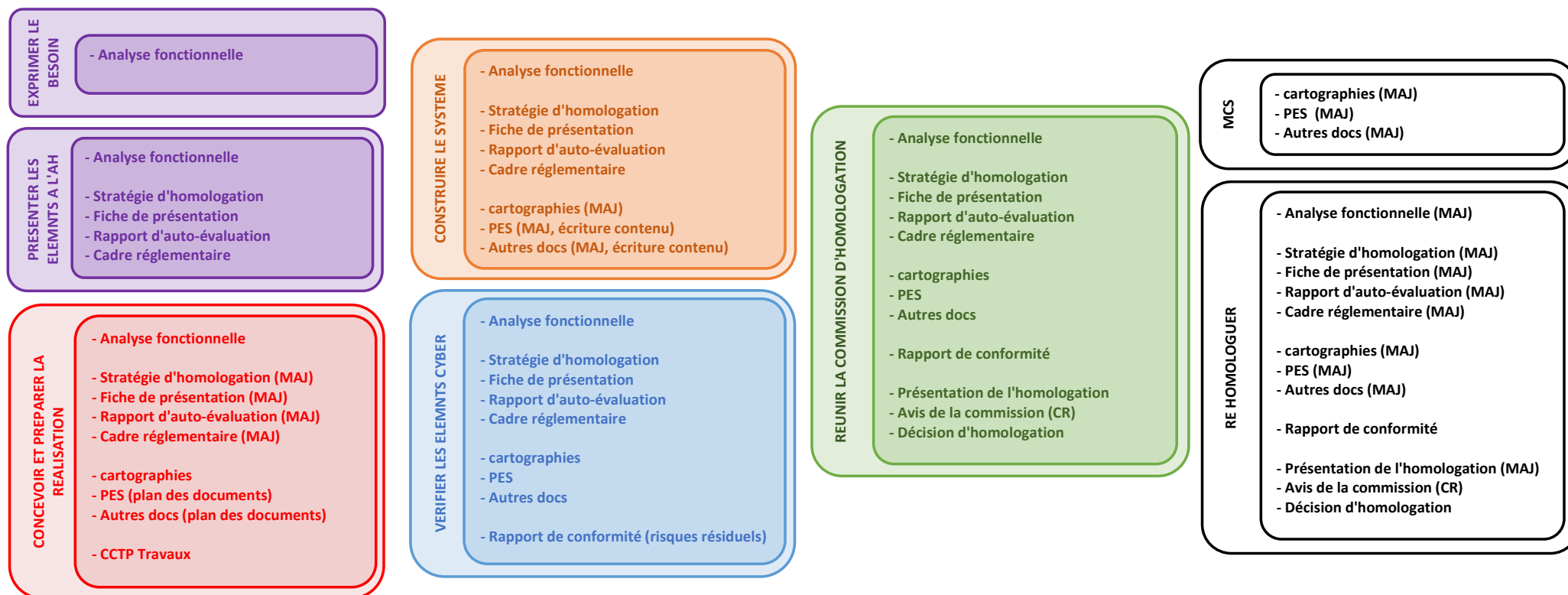


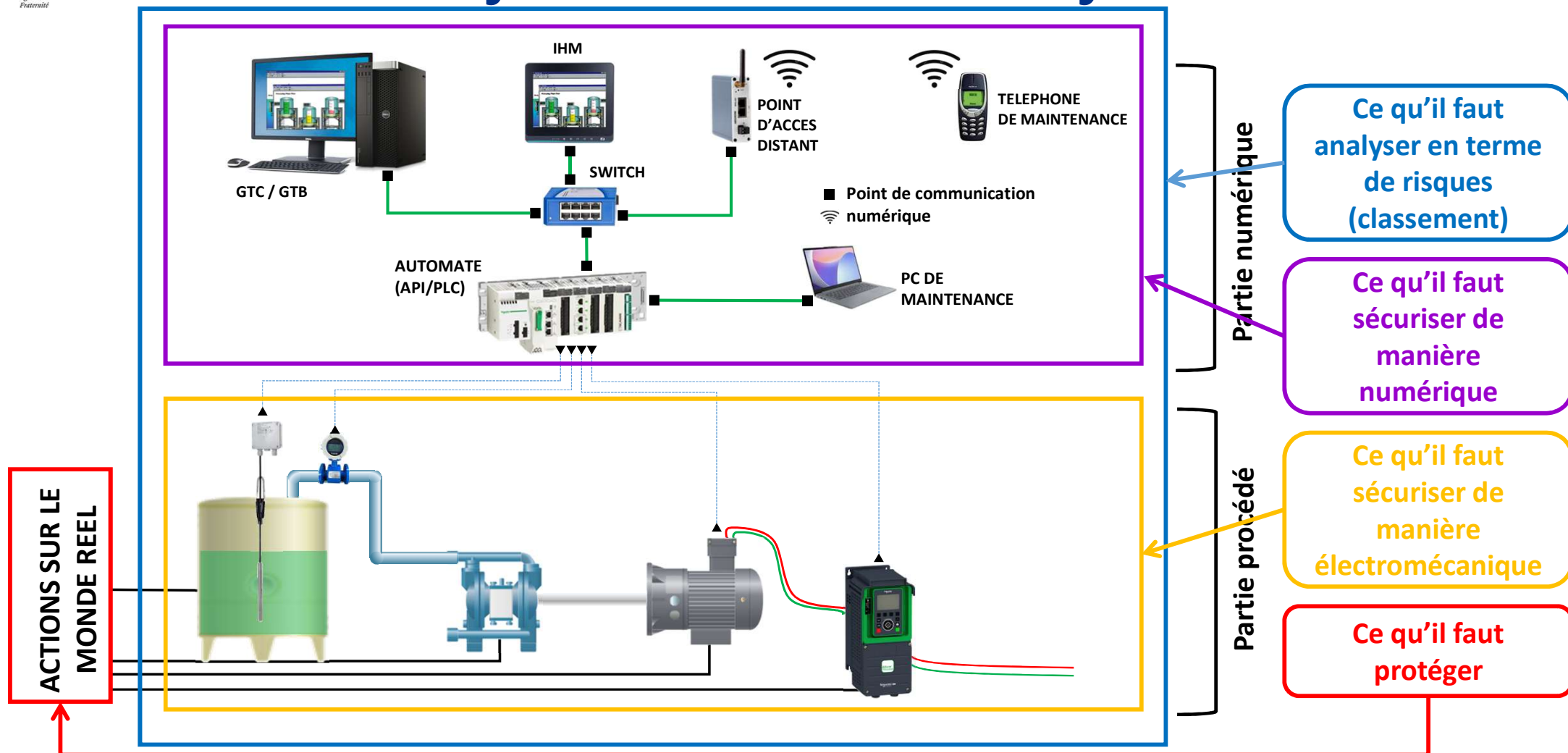
Homologation : le déroulé d'une opération



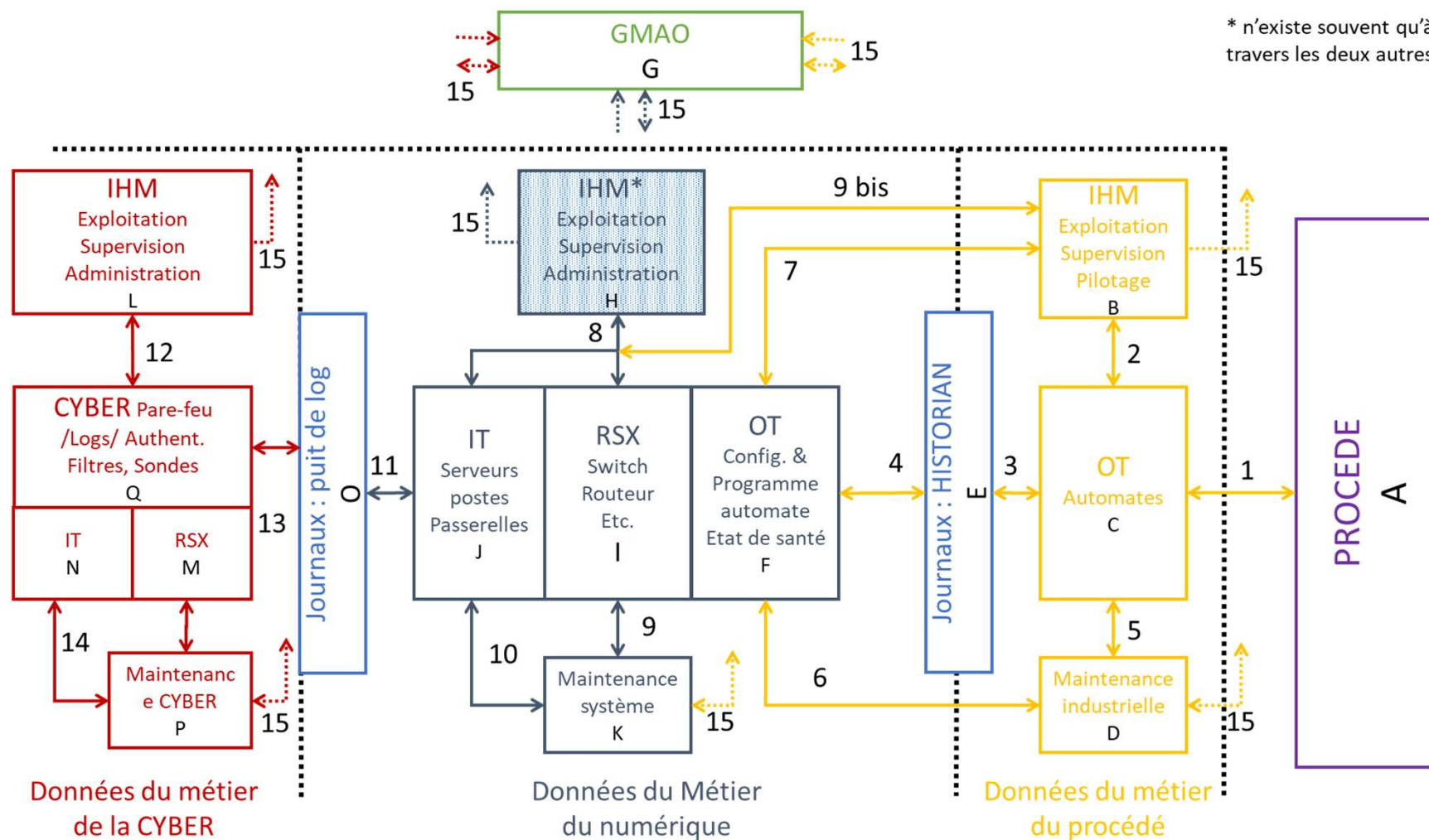
Homologation : les livrables



Classement cyber : Périmètre d'analyse



Sensibilité des données présentes dans les S2I



Sensibilité des données présentes dans les S2I

Type Equipement	Données
A	Valeur analogique, position du contact (contact sec), valeur numérique, Composant assurant l'interaction avec le monde physique
B	données de paramétrages de l'IHM (firmware/OS)
C	données de paramétrages, règles d'automatisme
D	données de paramétrages de l'équipement (firmware/OS/logiciel métier)
E	données de paramétrages de l'équipement (firmware/OS/logiciel métier)
F	données de configuration des équipements, programme automate et concernant l'état de santé de l'automate
G	données de paramétrages de l'équipement (OS/logiciel métier), donnée de la gestion technique du patrimoine (non alimenté par le système)
H	données de paramétrages de l'équipement (firmware/OS/logiciel métier), données d'administration des équipements I+J+F (niveau 2)
I	données de paramétrages des équipements réseaux, échange des données OT/IT et IT/IT
J	données de paramétrages des équipements de supervision (niveau 2)
K	données de paramétrages de l'équipement (firmware/OS/logiciel métier), donnée d'administration des équipements I+J+F (niveau 2)
L	données de paramétrages de l'équipement (firmware/OS/logiciel métier), données d'administration de équipement M
M	supervision des paramétrages des équipements réseaux I, ensemble des paramétrages des équipements réseaux M, échange des données IT/IT cyber
N	supervision des paramétrages des équipements de J+I+F, ensemble des paramétrages des équipements M et N
O	données de paramétrage du serveur des journaux des événements
P	paramétrages de l'équipement (firmware/OS/logiciel métier), donnée d'administration des équipements M + N

Flux	Données
1	Données de fonctionnement (Mesure d'un capteur, commande d'un actionneur)
2	Données d'exploitation (Report de valeurs, consignes de seuils, commande)
3	Données d'historisation du fonctionnement du procédé (Une valeur de capteur, une consigne passée)
4	Données d'historisation du fonctionnement de l'automate (Arrêt /marche de l'automate, dysfonctionnement système, etc.)
5	Données de maintenance du procédé (Configuration des entrées/sorties pour le procédé - points de fonction de l'IHM)
6	Données de maintenance de l'automate (configuration de l'automate, désactivation des services, configuration des applications de l'automate (i.e. serveur web), configuration du réseau, etc.)
7	Données de fonctionnement de l'automate (Passage en mode distant local, watchdog de l'automate)
8	Données d'exploitation du système -> i.e. supervision système et administration système (Trap SNMP pour la supervision, commande d'exploitation courante (administration) comme le blocage des ports sur un switch ou l'ajout ou la suppression des utilisateurs, etc.)
9	Données de maintenance des équipements réseaux (Chargement des firmwares, paramétrage des firmwares, configuration du réseau)
9 bis	Données de l'état du réseau
10	Données de maintenance des équipements informatiques (serveurs et postes de travail) -> i.e administration système (Installation d'applications, paramétrage d'applications, durcissement de l'OS, etc.)
11	Données de journalisation des équipements numériques (Espace disque, changement de configuration, etc.)
12	Données d'exploitation de la sécurité du système -> supervision et administration de la sécurité (alarme d'intrusion dans le système, filtrage en échec, paramétrage des règles de filtrage, de règles de firewall, gestion des comptes et mots de passe, souche antivirus, scan vulnérabilités, etc.)
13	Données de journalisation de la sécurité du système (Tous les traps d'alarme de sécurité, échec de connexion, etc.)
14	Données de maintenance des équipements de sécurité -> i.e. administration des serveurs de sécurité (Installation des firmwares, paramétrage des firmwares, durcissement des configurations, etc.)
15	Données d'intervention (Alarmes, élément pour générer l'ordre de travail, etc.)

Sensibilité des données dans le système

	NP mini, au-delà si état à protéger	NP mini, au-delà si état à protéger ou programme (secret indus)	Dépend du procédé, NP interne mini	DR mini
Caractérisation des données dans le procédé	A - E	C - F	B - D	
Caractérisation des données dans les flux liés au procédé	1 - 3 - 4		2 - 5 - 6 - 7	
Caractérisation des données dans le système qui conduit le procédé			H - I - J - K - O	
Caractérisation des données dans les flux liés au système qui conduit le procédé			8 - 9 - 9bis - 10 - 11	
Caractérisation des données de sécurisation du système qui conduit le procédé				L - M - N - P - Q
Caractérisation des données dans les flux liés à la sécurisation du système qui conduit le procédé				12 - 13 - 14
Caractérisation des données dans la gestion de la maintenance (GMAO S2I)				15 ¹ - G

[1] Peut-être NP si anonymisation des données

Note N°502162/ARM/SGA/DCSID/DIR du 01/09/2025

1. LISTE DE LA SENSIBILITE MINIMUM DES DOCUMENTS DU DOSSIER D'HOMOLOGATION

- Fiche de détection => NON PROTÉGÉ
- Fiche de présentation du périmètre => DIFFUSION RESTREINTE
- Rapport de questionnaire de classe => DIFFUSION RESTREINTE
- Stratégie d'homologation (SH) => DIFFUSION RESTREINTE
- Socle de sécurité => DIFFUSION RESTREINTE
- Analyse de risques et la fiche d'expression rationnelle des objectifs de sécurité (FEROS) => DIFFUSION RESTREINTE SPÉCIAL FRANCE
- Procédures d'exploitation de sécurité (PES) => DIFFUSION RESTREINTE
- Plan de continuité informatique et plan de reprise informatique (PCI/PRI) => DIFFUSION RESTREINTE
- Rapport de conformité => DIFFUSION RESTREINTE SPÉCIAL FRANCE
- Rapport d'audit => SECRET
- Fiche de synthèse => DIFFUSION RESTREINTE
- Avis de la commission => DIFFUSION RESTREINTE SPÉCIAL FRANCE
- Support de présentation de la commission => DIFFUSION RESTREINTE SPÉCIAL FRANCE
- Décision d'homologation => DIFFUSION RESTREINTE
- Synthèses de projets et agrégats indicateurs sur les dossiers d'homologation => DIFFUSION RESTREINTE

2. LISTE DE LA SENSIBILITE MINIMUM DES AUTRES DOCUMENTS EN LIEN AVEC LES S2I

- Analyse/architecture fonctionnelle => NON PROTÉGÉ
- Architecture fonctionnelle de sécurité => DIFFUSION RESTREINTE
- Schéma technico-opérationnel (STO) => DIFFUSION RESTREINTE
- Cartographies:
 - Physique => DIFFUSION RESTREINTE
 - Logique => DIFFUSION RESTREINTE
 - Plan d'adressage S2I classe brute 1 => DIFFUSION RESTREINTE
 - Plan d'adressage S2I autres classes => DIFFUSION RESTREINTE SPÉCIAL FRANCE
 - Applications => DIFFUSION RESTREINTE
 - Administration et surveillance => DIFFUSION RESTREINTE
- Traduction du socle de sécurité en CCTP => NON PROTÉGÉ
- Plan de test => NON PROTÉGÉ
- Résultats des tests => DIFFUSION RESTREINTE
- Matrice de traçabilité des exigences => NON PROTÉGÉ
- Spécifications fonctionnelles, IHM et autres interfaces => NON PROTÉGÉ
- Notices équipements S2I => DIFFUSION RESTREINTE
- Dossier des ouvrages exécutés (DOE) partie description des S2I et câblages divers => DIFFUSION RESTREINTE
- Dossier d'exploitation et maintenance (DEM) => DIFFUSION RESTREINTE
- Dossier justification de définition (DJD) => DIFFUSION RESTREINTE
- Dossier de définition (élément de conception) (DD) => DIFFUSION RESTREINTE
- CR de réunion de l'AMO => NON PROTÉGÉ
- Preuve de sensibilisation cyber => NON PROTÉGÉ
- Preuve certification diverses => NON PROTÉGÉ

ANNEXE 2	SENSIBILITE DES FLUX ET DES DONNEES STOCKEES D'UN S2I
-----------------	--

Les lettres et chiffres nommés dans le tableau sont définis dans l'annexe 3.

	=> NON PROTÉGÉ mini, au- delà si état à protéger	=> NON PROTÉGÉ mini, au-delà si état à protéger ou programme (secret indus)	Dépend du procédé, => NON PROTÉGÉ interne mini	=> DIFFUSION RESTREINTE mini
Caractérisation des données dans le procédé	A E	C F	B D	
Caractérisation des données dans les flux liés au procédé	1 - 3 - 4		2 - 5 - 6 - 7	
Caractérisation des données dans le système qui conduit le procédé			H - I - J - K - O	
Caractérisation des données dans les flux liés au système qui conduit le procédé			8 - 9 - 9bis - 10 - 11	
Caractérisation des données de sécurisation du système qui conduit le procédé				L - M - N - P - Q
Caractérisation des données dans les flux liés à la sécurisation du système qui conduit le procédé				12 - 13 - 14
Caractérisation des données dans la gestion de la maintenance (GMAO S2I)				15 ¹ - G

¹ Peut-être NP si anonymisation des données

Un système de remplissage d'un réservoir composé d'une pompe et de son régulateur.

Ce dispositif est contrôlé par un automate programmable. Ce dernier est piloté en local via un IHM et par une supervision, via un SCADA qui peut piloter également d'autres automates.

L'ensemble des moyens informatiques (supervision, SCADA, HISTORIAN, équipement réseau) est administré via une console d'administration.

Une zone de sécurité segmentée derrière un firewall assure la surveillance cyber de l'installation.

Un poste de GMAO permet de suivre la maintenance de l'installation.

Dans un automate, la sensibilité des données reçues par les capteurs et la sensibilité de sa programmation peuvent être différentes. Il est donc schématisé par 2 lettres C et F.

Dans l'idéal, un réseau possède ; un PC (interface) pour la surveillance et la gestion du procédé (B), 1 PC pour administrer le système industriel (H), 1 PC pour gérer la cyber sécurité (L) et éventuellement 1 écran tactile au plus près de l'automate principal (B).

Le matériel de supervision, exploitation et pilotage (B) et le matériel SCADA ont 2 volets de sensibilité de données comme l'automate : le programme et les données du procédé. Il est donc schématisé par 2 lettres B et J.

Définition des périmètres OT et IT

L'IT, ou technologie de l'information, désigne l'ensemble des technologies, outils et systèmes utilisés pour gérer, traiter, stocker et transmettre les données numériques. L'IT est axée sur les systèmes d'information et la communication numérique.

L'OT, ou technologie opérationnelle, regroupe les systèmes et technologies utilisés pour surveiller et contrôler les équipements, processus ou infrastructures physiques. L'OT est centrée sur le monde physique et la gestion des opérations industrielles en temps réel.

Définition des niveaux présents :

Les niveaux indiqués correspondent aux niveaux CIM (Computer Integrated Manufacturing) de l'ISA/IEC 62443, qui structurent la gestion des flux d'information et la segmentation des systèmes en couches.

CIM 0 - Processus physique : correspond à la production réelle, incluant les machines, équipements, capteurs et actionneurs.

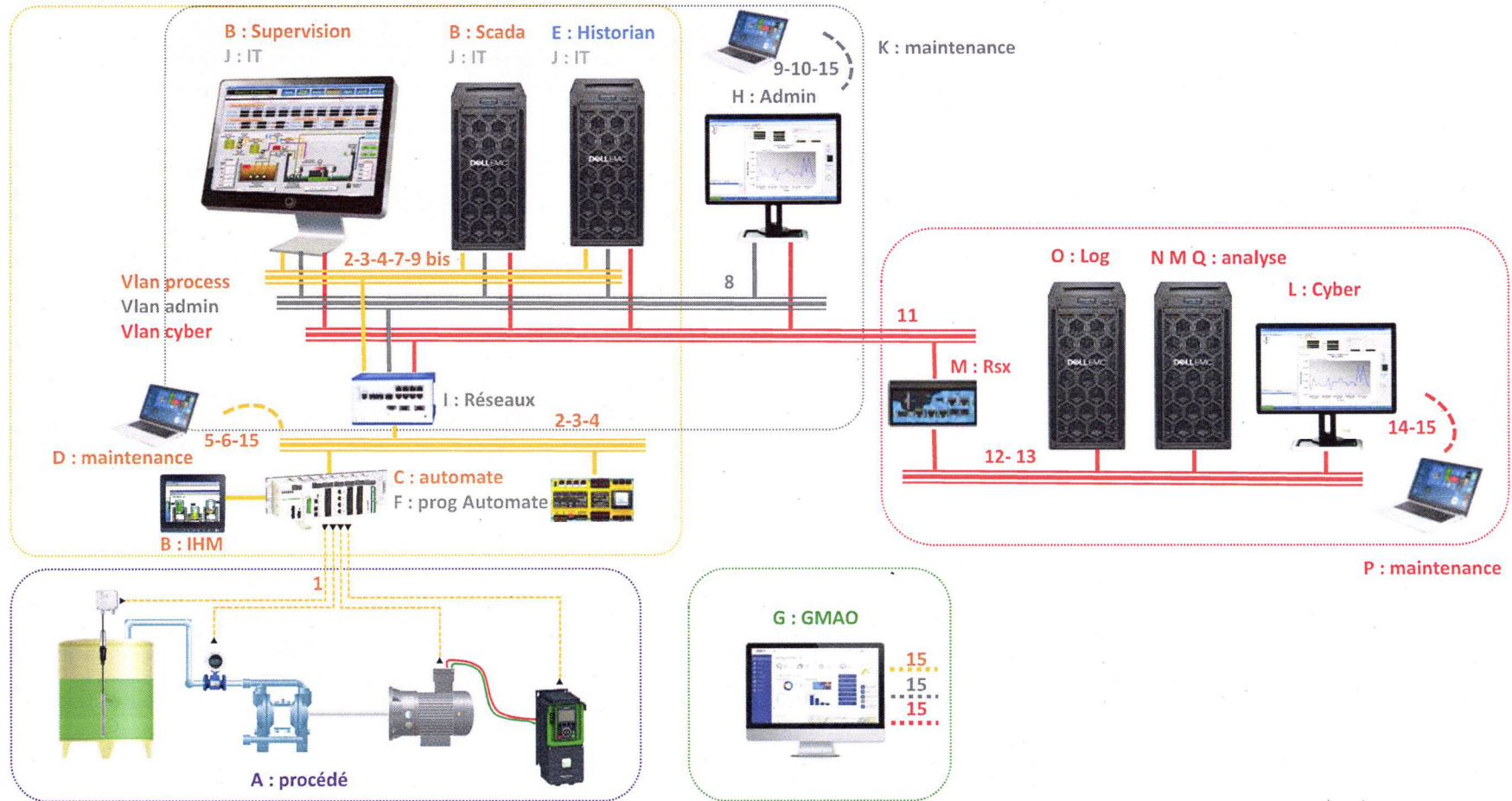
CIM 1 - Contrôle des processus : inclut les équipements permettant de contrôler les processus physiques : Automates Programmables Industriels (PLC).

CIM 2 - Supervision et contrôle : correspond aux systèmes de supervision (HMI - Interfaces Homme-Machine) et SCADA (Supervisory Control and Data Acquisition).

CIM 3 - Gestion des opérations industrielles : correspond dans notre contexte aux GMAO.

CIM 4 - Gestion de l'entreprise : rarement mis en œuvre dans nos systèmes industriels d'infrastructure.

EXEMPLE D'ARCHITECTURE TECHNIQUE



1. DEFINITION DES FONCTIONS

1.1.1. A. Procédé (CIM 0)

- **Définition** : Composant physique assurant l'interaction directe avec le monde réel. Il inclut des capteurs et des actionneurs qui transmettent ou exécutent des commandes.
- **Exemple** : *Un capteur de niveau mesure la hauteur d'eau dans le réservoir. Une commande est envoyée à la pompe pour démarrer ou arrêter le remplissage.*

1.1.2. B. Interface Homme-Machine (IHM -CIM 2) : Exploitation, Supervision, Pilotage

- **Définition** : Interface utilisateur permettant de surveiller et de contrôler le procédé via des réglages spécifiques adaptés à son fonctionnement.
- **Exemple** : *Un écran tactile permet à un opérateur d'ajuster le niveau de seuil pour arrêter la pompe lorsque le réservoir est plein.*

1.1.3. C. Technologies Opérationnelles (OT) - Automates (CIM 1)

- **Définition** : Automates industriels qui appliquent des règles logiques pour gérer les données issues du procédé et déclencher des actions.
- **Exemple** : *Un automate programmable logique (PLC) gère l'arrêt automatique de la pompe lorsque le capteur signale que le niveau d'eau atteint le seuil prédéfini.*

1.1.4. D. Maintenance industrielle

- **Définition** : Gestion des réglages et des logiciels de l'équipement pour garantir son bon fonctionnement.
- **Exemple** : *Ajustement des paramètres du capteur de niveau pour compenser l'usure ou les erreurs de mesure.*

1.1.5. E. Journaux HISTORIAN (CIM 2)

- **Définition** : Système d'enregistrement des données de fonctionnement du procédé pour une analyse historique.
- **Exemple** : *Stockage des valeurs mesurées par le capteur de niveau toutes les minutes pour une consultation ultérieure.*

1.1.6. F. Configuration et Programme automate (CIM 1)

- **Définition** : Paramètres définissant le comportement des automates, incluant l'état de santé du système.
- **Exemple** : *Programmation d'un redémarrage automatique de la pompe après une panne.*

1.1.7. G. Gestion de la Maintenance Assistée par Ordinateur pour les S2I (GMAO – CIM 3)

- **Définition** : Outil de gestion des données techniques et administratives liées à l'entretien des équipements.

- **Exemple** : Génération d'un ordre de maintenance lorsqu'une alarme signale un dysfonctionnement de la pompe.

1.1.8. H. IHM Exploitation Supervision Administration

- **Définition** : Interface dédiée à l'administration avancée des équipements, comme la gestion des utilisateurs.
- **Exemple** : Ajout d'un utilisateur pour accéder aux données de la pompe et du capteur.

1.1.9. I. Réseaux (Switch, Routeur)

- **Définition** : Infrastructure de communication permettant les échanges de données entre les équipements OT et IT.
- **Exemple** : Transmission des données du capteur de niveau vers l'IHM via un réseau industriel.

1.1.10. J. Serveurs, postes et passerelles IT

- **Définition** : Équipements informatiques supportant la supervision et la communication entre les systèmes.
- **Exemple** : Serveur central recevant les données de la pompe et envoyant des rapports aux opérateurs.

1.1.11. K. Maintenance système

- **Définition** : Administration et mise à jour des équipements informatiques et réseaux.
(Nota la fonction station d'ingénierie est incluse dans cette fonction)
- **Exemple** : Mise à jour du firmware du serveur supervisant les niveaux d'eau.

1.1.12. L à Q : Cyber maintenance et sécurité

- **Définition** : Aspects liés à la supervision, journalisation et protection des systèmes face aux cybermenaces.
- **Exemple** : Un pare-feu filtre les accès aux données de la pompe pour prévenir des intrusions non autorisées.
- **Exemple** : Une sonde réseau type IDS
- **Exemple** : Un serveur de mise à jour antivirus