



ESID de Bordeaux - Mai 2021

DESCRIPTION DES CARTOGRAPHIES

Le référentiel utilisé est celui de l'agence nationale de la sécurité des systèmes d'information (ANSSI) :

- <http://www.ssi.gouv.fr/>
- <http://www.ssi.gouv.fr/administration/guide/la-cybersecurite-des-systemes-industriels/>

Les cartographies comprennent :

- la cartographie physique du système industriel ;
- la cartographie logique des réseaux industriels ;
- la cartographie des applications ;
- la cartographie de l'administration et de la surveillance du système d'information.

Les cartographies doivent être présentées sous forme de tableaux et sont accompagnées de schémas améliorant la compréhension.

A. Cartographie physique du système industriel

Le point de vue physique correspond à la répartition géographique des équipements au sein des différents sites.

Elle devra comporter notamment les éléments suivants :

La liste des équipements communicants du système industriel :	<p>Cette liste comportera par exemple les automates, les entrées sorties déportées, les capteurs, les actionneurs, les variateurs de vitesse, les centrales de mesures, les disjoncteurs, les interrupteurs, les serveurs physiques, les postes de travail, les unités de stockage. Pour chaque élément, il devra être précisé :</p> <ul style="list-style-type: none"> - le nom ; - la marque ; - le modèle ou la référence^[1] ; - la version du firmware (software version) embarqué et la version du produit (product version) si pertinent ; - les caractéristiques matérielles (si pertinent) ; - l'emplacement physique (bâtiment, pièce, armoire, baie) ; - la liste des commutateurs reliés.
La liste des équipements des réseaux de communication	<p>Cette liste comportera par exemple les commutateurs, les routeurs, les passerelles protocolaires, etc. Pour chaque équipement, il devra être précisé :</p> <ul style="list-style-type: none"> - la marque ; - le modèle et la référence ; - la version du firmware embarqué. - l'emplacement physique (bâtiment, pièce, armoire, baie). - Dans le cas de commutateurs Ethernet, on précisera également les numéros de VLAN pour chaque port du commutateur.

Le schéma est la représentation des différents sites géographiques, faisant apparaître :

- les commutateurs, les numéros de VLAN associés ;
- les liens entre équipements ;
- en cas d'installation inter-sites, les identifiants d'interconnexion (MPLS, VPLS, numéros de téléphone) ;
- les équipements.

^[1] Certains équipements (les automates modulaires, par exemple) contiennent plusieurs références.

B. Cartographie logique des réseaux industriels

On s'intéresse ici à la topologie logique des réseaux (les plan d'adressage IP et non-IP, noms de sous-réseaux, liens logiques entre ceux-ci, principaux équipements actifs, etc.).

Elle devra comporter notamment les éléments suivants :

Les organisations :	Avec pour chacune d'entre elles le responsable.
La liste des plages d'adresses IP :	Avec pour chacune : <ul style="list-style-type: none"> - la liste des commutateurs en support ; - la description fonctionnelle de la plage IP ; - les interconnexions avec d'autres plages.
La liste des réseaux non-IP :	Avec pour chaque réseau <ul style="list-style-type: none"> - la liste des adresses MAC ou des adresses spécifiques à des protocoles industriels sur le réseau ; - la liste des commutateurs en support ; - la description fonctionnelle du réseau ; - les équipements connectés à d'autres réseaux (automates).
La liste des points d'accès non Ethernet	Avec pour chacun d'entre eux : <ul style="list-style-type: none"> - la liste des ports d'accès ; - l'adressage en cas de protocole spécifique ; - la liste des équipements connectés.
La liste des serveurs logiques et des postes de travail :	Avec pour chacun d'entre eux, lorsque cela s'applique, <ul style="list-style-type: none"> - l'adressage IP (réseau, masque, passerelle) ; - la version du système d'exploitation ; - le serveur physique en support ; - les applications métier et leur version ; - les services et versions ; les services et applications inutiles et que l'on pourrait supprimer sans remettre en cause le fonctionnement du système industriels ^[2] .
La liste des automates et équipements de terrain communicants ^[3]	Avec pour chacun <ul style="list-style-type: none"> - l'adressage IP (réseau, masque, passerelle), l'adressage MAC et réseau associé ou l'adressage spécifique le cas échéant ; - les applications métier ; - la liste des ports de communication (port ETHERNET, port série, etc...) présents, ceux qui sont activés et si cette activation est nécessaire au fonctionnement du système industriel.

Le schéma est la représentation des ensembles IP (réseaux et sous-réseaux) et de leurs interconnexions, faisant apparaître :

- la description fonctionnelle de la plage IP ;
- les interconnexions avec les autres plages IP ;
- les routeurs, commutateurs et pare-feu ;
- les équipements informatiques de sécurité (relais filtrant, sondes, IDS, etc.).

Cette cartographie doit faire apparaître en particulier les points d'interconnexion avec des entités « extérieures » (partenaires, fournisseurs de services, etc.) et l'ensemble des interconnexions avec Internet.

Si aucune interconnexion n'existe avec l'extérieur, cette absence de connexion devra être mentionnée explicitement.

^[2] Par exemple, sur une console SCADA, on peut supprimer la visionneuse de film Windows (Media-Player).

^[3] Entrées sorties déportées, capteurs/actionneurs intelligents, etc.

C. Cartographie des applications

Le point de vue applicatif correspond aux applications métier et aux flux de communication entre elles.

Elle devra comporter notamment les éléments suivants :

- le responsable ;
- le type d'application (application SCADA, programme automate, historique, etc.) ;
- le nombre d'utilisateurs ;
- les équipements (physiques ou logiques) supports ;
- les services en écoute sur le réseau et ports réseaux associés ;
- les flux applicatifs ;
- la version de l'application.

Le schéma est une représentation des composants des applications et des flux entre elles :

- les programmes des automates ;
- les applications de SCADA ;
- les services d'infrastructure (DNS, NTP, passerelle Internet, etc.) ;
- les services d'administration (service d'inventaires, d'administration à distance, etc.)
- la matrice de flux associée à chaque application et service.

D. Cartographie de l'administration et de la surveillance du système d'information

Cette dernière cartographie ne s'applique que si une gestion centralisée des droits d'administration sur les équipements a été mise en place. Dans le cas où les droits sur les équipements ne sont gérés que par des comptes locaux, cette cartographie se réduira à une liste des comptes et des droits associés pour chaque équipement.

La cartographie devra contenir :

- Les annuaires (voir plus bas) ;
- les infrastructures de gestion de clés ;
- les systèmes de mots de passe à usage unique ;
- les systèmes de gestion de journaux et d'événements de sécurité (collecteurs de journaux, SIEM) ;
- les systèmes de supervision (alarmes réseau, sondes de détection, etc.).

Le point de vue « domaines d'administration » représente le périmètre et le niveau de privilèges des administrateurs sur les ressources du parc informatique.

Cette cartographie contiendra :

- le cas échéant, un schéma « Active Directory » avec :
 - o les domaines Active Directory et leur description,
 - o les forêts Active Directory,
 - o les relations d'approbation avec les domaines externes à chaque forêt,
 - o les caractéristiques des relations d'approbation (bidirectionnelle, filtrée, etc.),
 - o les serveurs support des Active Directory ;
- sinon, la représentation de l'architecture d'administration avec :
 - o les zones de responsabilité des différents administrateurs,
 - o l'inventaire des secrets (mots de passe, clés, etc.) et droits associés à l'administration des ressources.

Ce point de vue permet, en cas de compromission d'un compte d'administration, d'identifier le niveau de privilège de l'attaquant et la portion du parc potentiellement affectée.