ANALOG DEVICES

Démystifier la cybersécurité industrielle

VISIT ANALOG.COM/CYBERSECURITY

PROTÉGER LA PÉRIPHÉRIE INTELLIGENTE DE L'USINE NUMÉRIQUE DE NOUVELLE GÉNÉRATION

Véritable catalyseur de changement dans de nombreux pans de l'industrie, la transformation numérique génère de plus en plus de données qui facilitent la prise de décisions en temps réel dans l'optique d'augmenter le niveau d'automatisation et d'améliorer l'efficacité des processus. Pour maximiser l'exploitation de ces données, les entreprises numériques sont de plus en plus connectées, ce qui nécessite la convergence des réseaux opérationnels (OT) et informatiques (IT). Cette rapide évolution technologique a libéré la puissance de l'intelligence en périphérie de réseau (l'intelligent edge), rendant possibles des connexions fluides et transparentes entre la périphérie et le cloud (edge to cloud). Compte tenu de l'adoption croissante de la connectivité numérique — une technologie qui augmente la bande passante et permet d'accéder à des informations pertinentes collectées aux quatre coins des usines de traitement des matières premières et des ateliers —, il convient d'anticiper une hausse des cybervulnérabilités. En outre, l'adressabilité IP de chaque nœud et la suppression des passerelles qui caractérise les nouvelles infrastructures technologiques basées sur le protocole Ethernet industriel, la sécurisation des appareils et des systèmes contre les risques de cyberattaque s'avère primordiale. Au-delà d'un coût potentiellement extrêmement élevé, ces attaques peuvent également mettre en danger des vies humaines dans le cas des systèmes de contrôle liés à la sécurité.

Aujourd'hui, les entreprises doivent réfléchir à la manière dont elles vont opérer dans un monde où les systèmes d'automatisation et de contrôle industriels (IACS — Industrial Automated Control Systems) peuvent résister aux cyberattaques. Les systèmes de contrôle gèrent les commandes, régulent le comportement d'autres appareils et, en cas de cyberagression, constituent une menace pour l'ensemble de l'infrastructure de production. Les cyberattaques peuvent être invasives ou non invasives. Dans le premier cas, un cybercriminel ouvre le boîtier de l'appareil dans le but de manipuler le contenu stocké en mémoire, de remplacer le micrologiciel (firmware) ou d'analyser les empreintes sur des circuits imprimés. Pour leur part, les attaques non invasives sont généralement effectuées à distance par l'intermédiaire des ports de communications et ciblent les failles de sécurité dans le micrologiciel de l'appareil.

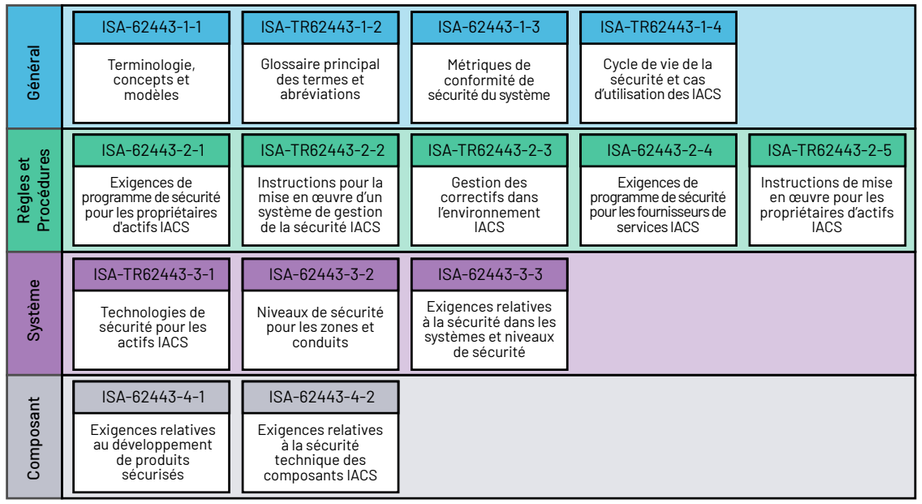
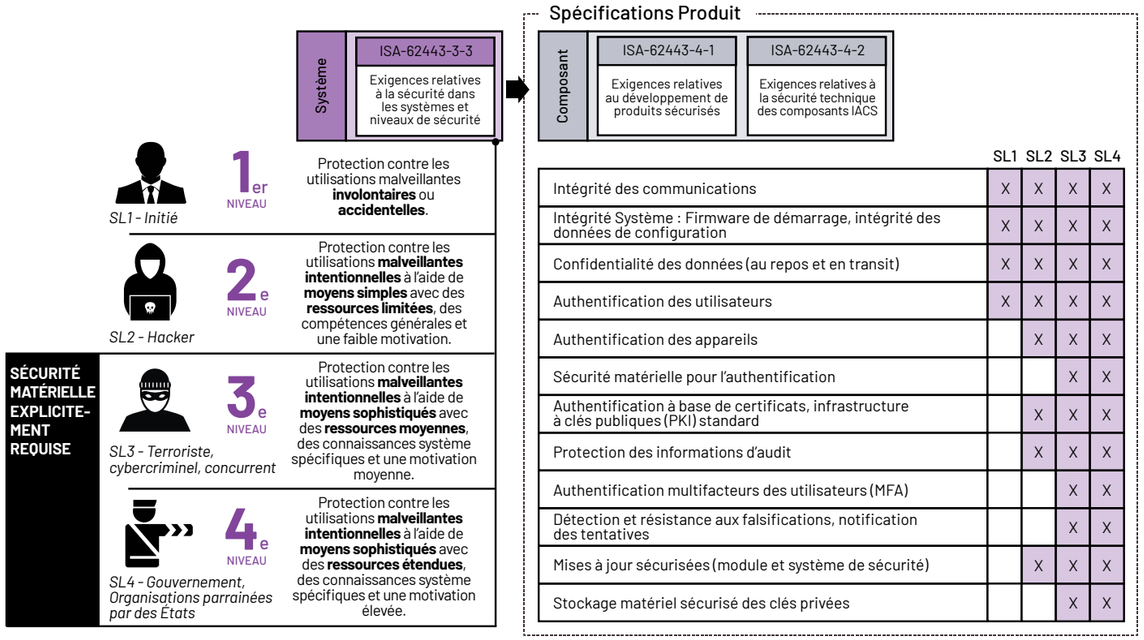


Figure 1 : *Norme de sécurité de la série CEI 62443*

Le nouveau règlement européen sur la cyberrésilience (CRA) régit la cybersécurité des produits numériques vendus dans l'espace économique européen (EEE) avec un impact global sur les fabricants, les développeurs et les fournisseurs de « produits comportant des éléments numériques » (PDE — Products with Digital Elements) destinés au marché de l'UE, avec notamment l'apposition obligatoire du marquage CE sur les produits d'ici à 2027. Cette législation vise à prioriser l'intégration des considérations de sécurité en amont des cycles de développement de nouveaux produits, faute de quoi les nouveaux articles créés actuellement ne seront pas conformes aux normes en vigueur lors de leur commercialisation en Europe après 2027.

Pour en savoir plus, lisez l'article consacré par ADI à la norme CEI 62443 : *"The IEC 62443 Series of Standards: How to Defend Against Infrastructure Cyberattacks"*

Pour faciliter l'adoption des dispositions du règlement CRA, l'Agence de l'Union européenne pour la cybersécurité (ENISA) a calé ses exigences sur la norme CEI 62443-4. La série de normes CEI 62443 a pour objectif de gérer la cybersécurité des technologies opérationnelles (OT) au sein des processus d'automatisation et de contrôle. Cette norme de premier plan représente une couche de sécurité étendue dont le rôle est de prévenir les attaques et d'en atténuer les effets. Elle est organisée en quatre niveaux et catégories : le niveau « général » qui regroupe les sujets communs à l'ensemble de la série ; les « règles et procédures » qui englobent les méthodes et processus associés à la sécurité des systèmes d'automatisation et de contrôle industriels (IACS) ; le niveau « système » qui décrit les exigences au niveau système ; et le niveau « composant » qui fournit des exigences détaillées pour les systèmes d'automatisation et de contrôle industriels IACS.



	SL1	SL2	SL3	SL4
Intégrité des communications	X	X	X	X
Intégrité Système : Firmware de démarrage, intégrité des données de configuration	X	X	X	X
Confidentialité des données (au repos et en transit)	X	X	X	X
Authentification des utilisateurs	X	X	X	X
Authentification des appareils		X	X	X
Sécurité matérielle pour l'authentification			X	X
Authentification à base de certificats, infrastructure à clés publiques (PKI) standard		X	X	X
Protection des informations d'audit		X	X	X
Authentification multifacteurs des utilisateurs (MFA)			X	X
Détection et résistance aux falsifications, notification des tentatives			X	X
Mises à jour sécurisées (module et système de sécurité)		X	X	X
Stockage matériel sécurisé des clés privées			X	X

Figure 2 : *Norme CEI 62443. Choix des composants en fonction du niveau de sécurité souhaité pour le système.*

Pour concevoir un composant sécurisé, il convient dans un premier temps de définir le niveau de sécurité nécessaire en évaluant les risques potentiels. Le résultat permettra de déterminer si le composant doit résister aux attaques d'initiés qui correspondent généralement à des failles de sécurité involontaires ou accidentelles (niveau 1), de hackers qui cherchent à nuire intentionnellement avec des ressources limitées (niveau 2), de cybercriminels (niveau 3) et de gouvernements (niveau 4) dont l'objectif est de nuire en s'appuyant sur des ressources sophistiquées.

La combinaison de la norme ISA-62443-3-3 (« Exigences de sécurité des systèmes et niveaux de sécurité ») et des exigences au niveau des composants (ISA-62443-4-1 et ISA-62443-4-2) permet de concevoir des composants sécurisés capables de résister aux cyberattaques. En fonction du niveau de sécurité souhaité, il conviendra de prendre en compte certaines exigences au cours de la phrase de conception. Tous les niveaux exigent la confidentialité des données identifiées comme « sensibles ». L'authentification des composants est requise pour les niveaux de sécurité SL2 à SL4, tandis que le stockage sécurisé des clés privées au niveau matériel est spécifié pour tout composant devant atteindre les niveaux SL3 ou SL4. Le cycle de développement sécurisé des produits d'ADI est certifié selon la norme IEC-62441-4-1:2018.

COMPRENDRE LES VULNÉRABILITÉS INDUSTRIELLES

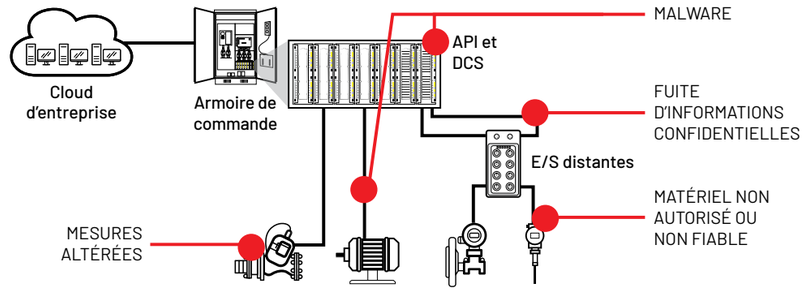


Figure 3 : *Vulnérabilités de sécurité courantes dans les applications industrielles.*

Dans les environnements industriels, plusieurs zones de vulnérabilité doivent être sécurisées en vue de garantir l'intégrité de l'infrastructure opérationnelle. Nous allons examiner quatre zones qui peuvent être protégées au moyen de circuits intégrés sécurisés disponibles clé en main, en intégrant des mécanismes essentiels tels que le stockage sécurisé des clés et en évitant aux développeurs de composants IACS de consacrer d'importantes ressources à la conception de primitives de sécurité complexes. L'ajout d'un circuit intégré sécurisé à un système non sécurisé élève le niveau de sécurité du système sans qu'il soit nécessaire de refondre l'architecture. Un tel composant doit intégrer de puissantes fonctions de chiffrement tout en étant suffisamment souple pour prendre en charge différentes fonctions de sécurité au niveau système. Se reporter aux tableaux de sélection pour des connaître les produits recommandés.

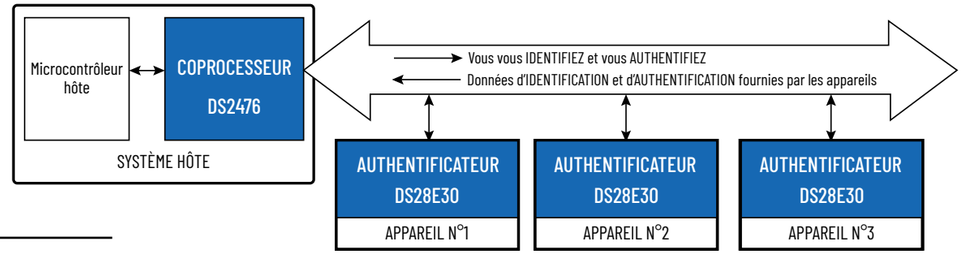


Figure 4 : *Comment les authentificateurs et coprocesseurs sécurisés simplifient le chiffrement.*

MATÉRIEL NON AUTORISÉ OU NON FIABLE

L'établissement de la confiance entre les différents appareils s'effectue au moyen d'un processus d'authentification par défi-réponse qui repose sur une clé secrète partagée (authentification symétrique) ou une paire de clés privée/publique (authentification asymétrique). Si la clé publique est par définition conçue pour être connue publiquement, la clé secrète et la clé privée présentent toutes deux un risque pour la sécurité : en cas de vol, l'ensemble du réseau est exposé à des menaces.

S'il n'est pas nécessaire que la clé publique soit tenue secrète, il est important de savoir qu'elle est authentique. La clé publique d'un composant et son identifiant (ID) peuvent être certifiés par une autorité de certification indépendante qui délivre un certificat numérique. Au cours du processus d'authentification des clés, la clé publique de l'autorité de certification peut être utilisée pour vérifier son authenticité.

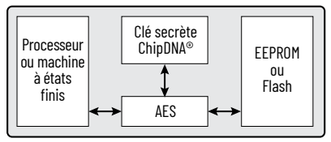
L'authentification par défi-réponse repose sur la capacité à générer un flux de bits réellement aléatoire, appelé « nonce ». L'utilisation d'un nonce aléatoire fort à chaque échange assure une protection contre la possibilité d'une « attaque par relecture » (replay attack). Les outils d'authentification sécurisés peuvent être utilisés comme solutions clés en main capables d'effectuer une authentification par défi-réponse.

DIVULGATION DE DONNÉES SENSIBLES

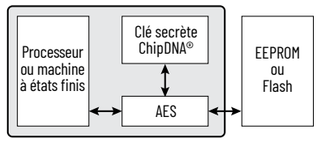
La protection des données au repos dans un appareil ou en transit en cas d'échange avec d'autres systèmes connectés au réseau dépend du chiffrement. L'utilisation de méthodes éprouvées telles que le standard AES (Advanced Standard Encryption) permet d'éviter la divulgation de données sensibles.

Dans les situations où les attaques ont lieu au niveau de l'appareil et où les données sont considérées comme étant au repos, le stockage sécurisé en mémoire garantit que même en cas d'accès à la mémoire, toutes les données sont chiffrées à l'aide de méthodes utilisant les caractéristiques aléatoires propres à chaque appareil lors de sa fabrication pour créer une fonction physiquement non clonable (PUF — Physically Unclonable Function). Dans les systèmes d'authentification sécurisée ChipDNA® d'Analog Devices dotés d'une fonction PUF, chaque clé est générée sous la forme d'une caractéristique analogique précise du circuit intégré et n'est jamais stockée en mémoire, ce qui l'immunise à tous les outils et fonctionnalités d'attaque invasive connus.

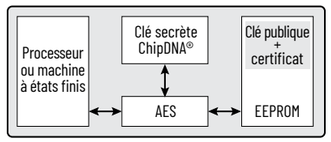
Lorsqu'un message est en transit, le chiffrement des données garantit qu'aucune information sensible ne sera divulguée à quiconque « écoute » le réseau. Le protocole TLS (Transport Layer Security) est le plus couramment utilisé pour protéger les données en transit ; il assure en effet l'authenticité, l'intégrité et la confidentialité des échanges.



Chiffrement sur mémoire interne



Chiffrement sur mémoire interne



Génération de clés d'authentification

Figure 5 : *Configurations de sécurité du circuit ChipDNA® PUF*

LOGICIELS MALVEILLANTS

Tout appareil connecté à un réseau non sécurisé tel qu'Internet est vulnérable aux attaques de logiciels malveillants (malware). Les appareils qui nécessitent des mises à jour de la part de leur fabricant doivent être capables de vérifier que ces dernières sont autorisées et qu'elles n'ont pas été modifiées. Les signatures numériques garantissent que seuls les firmwares vérifiés sont acceptés. Les appareils dotés d'une fonction de démarrage sécurisé (secure boot) garantissent l'authentification du micrologiciel lors de la mise sous tension. Si un firmware modifié est injecté dans l'appareil, le système refusera de démarrer dans la mesure où le micrologiciel ne reconnait pas la méthode de chiffrement initialement mise en œuvre par le fabricant, et la signature numérique est invalide.

MESURE ALTÉRÉE

La manipulation des données, ou l'altération des mesures effectuées en périphérie de réseau, peut provoquer des perceptions fausses quant à l'état d'un système. Un nombre croissant de systèmes étant automatisés, il est vital de s'assurer que des décisions fondées sur des données peuvent être prises à partir de mesures fiables. Si un acteur malveillant tente d'influencer le fonctionnement d'un appareil connecté en périphérie de réseau ou de falsifier les messages d'état, la vérification des commandes par le biais de signatures élimine le risque que des mesures altérées affectent le bon fonctionnement.

PRINCIPALES CONCLUSIONS

Pour qu'un système soit sécurisé, les appareils doivent être capables de créer des connexions de confiance en utilisant un mécanisme d'authentification. Ils doivent assurer la confidentialité des informations en utilisant les techniques de chiffrement et déchiffrement, et être en mesure de vérifier l'intégrité des commandes afin de limiter le nombre de points d'attaque potentiels qu'un acteur malveillant peut exploiter pour prendre le contrôle des processus industriels. Les CI sécurisés clés en main que commercialise ADI réunissent ces fonctionnalités, augmentant ainsi la sécurité du système sans qu'il soit nécessaire de modifier l'architecture de l'IACS.

CERTIFICATS NUMÉRIQUES ET PROVISIONNEMENT

Un message validé par la signature numérique de l'expéditeur peut être utilisé pour prouver qu'il a bien été envoyé par l'expéditeur et qu'il n'a pas été modifié. Cependant, une signature numérique ne suffit pas pour prouver l'identité de l'expéditeur. Cette preuve est apportée par un certificat numérique qui contient une clé publique et des informations d'identification (ID) permettant de vérifier à qui appartient la clé. Les certificats et les clés peuvent être programmés par ADI pour le compte du client en tant que service. En s'appuyant sur les certificats numériques et les pratiques de provisionnement de la sécurité, les entreprises industrielles peuvent améliorer de manière significative la protection de leur infrastructure de cybersécurité en vue de garantir l'intégrité, la confidentialité et l'authenticité de leurs systèmes et données critiques.

Certification numérique

Un document numérique vérifie à qui appartient la clé

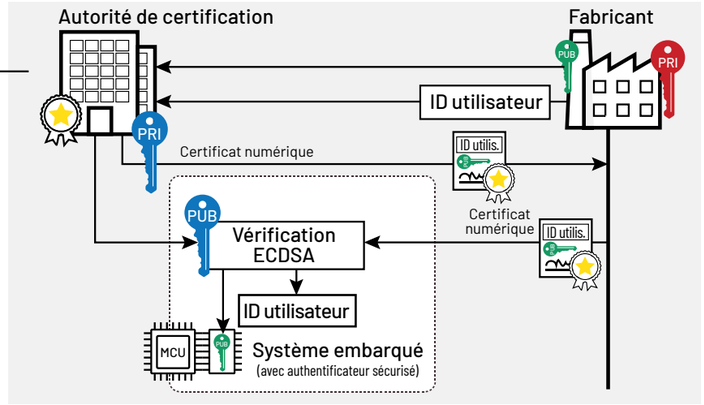


Figure 6 : *Utiliser une autorité de certification pour générer un certificat numérique*

MISE À JOUR DU FIRMWARE

Les mises à jour critiques du firmware peuvent être déployées sur le terrain à l'aide de messages signés, ce qui en garantit à la fois l'authenticité et l'intégrité.

Messages signés

Assurent l'authenticité et l'intégrité des informations

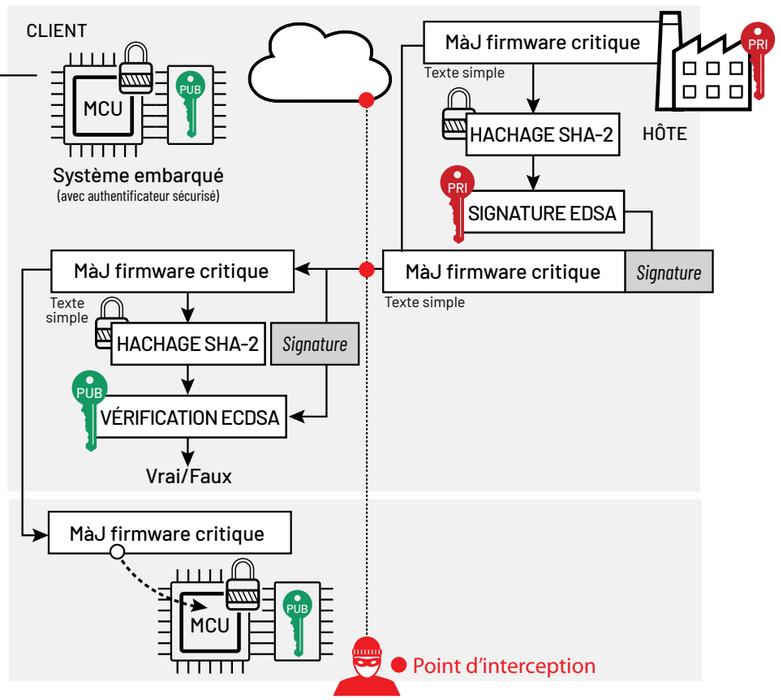


Figure 7 : *Processus de mise à jour du firmware.*

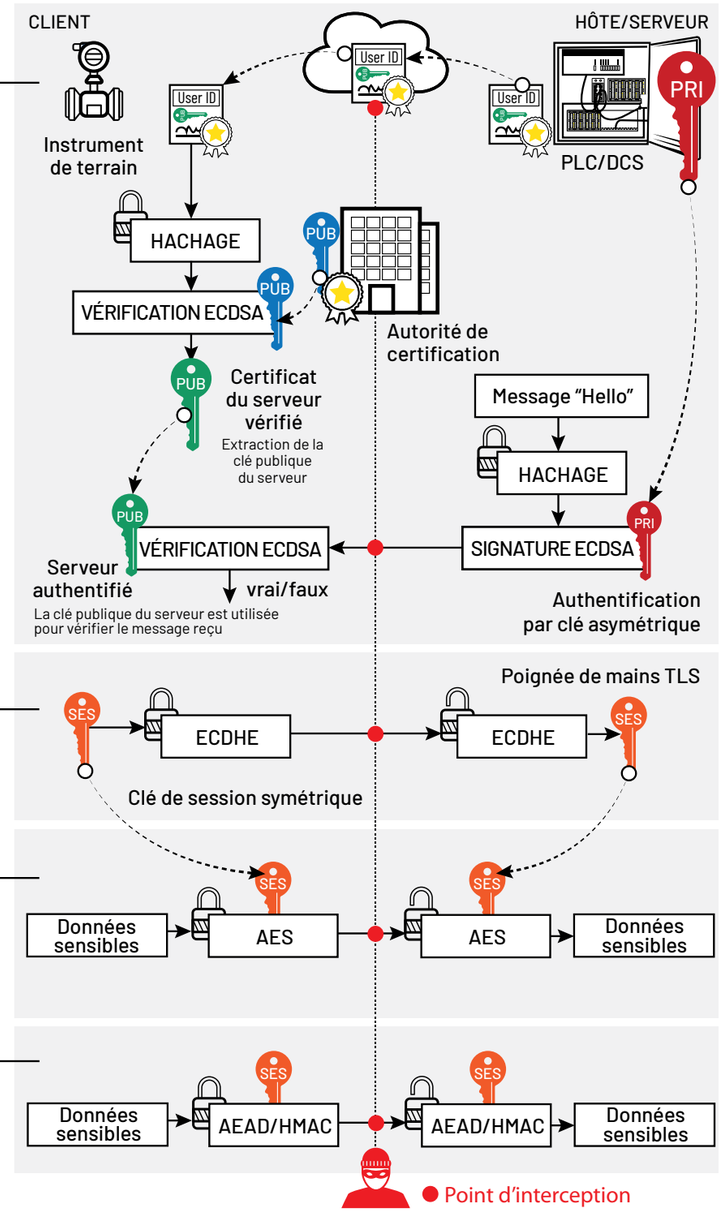
AUTHENTIFICATION DU MATÉRIEL ET COMMUNICATIONS SÉCURISÉES

Le processus d'authentification matérielle commence par l'échange de paires de clés entre un hôte (automate programmable industriel — API) et un client (instrument de terrain). L'illustration ci-dessous représente un processus d'authentification par certificat en deux étapes : dans un premier temps, le client vérifie le certificat hôte/serveur avec la clé publique délivrée par l'autorité de certification, ce qui permet de l'utiliser en toute confiance. La clé publique est ensuite utilisée pour vérifier la signature d'un nonce (dans ce cas, les données « Hello » échangées précédemment) après calcul par l'hôte. Avec le protocole TLS, une clé de communications partagée (également appelée « clé de session ») est créée après que le serveur a été authentifié à l'aide d'un algorithme symétrique (ECDH ou ECDHE). Cette clé de session est alors appliquée pour chiffrer les données « utiles » et permettre au serveur et au client d'échanger des informations confidentielles. Le protocole TLS garantit l'intégrité des échanges, soit par chiffrement authentifié (clé AES-GCM ou AES-CCM), soit en ajoutant une clé de hachage HMAC (Hash-based Message Authentication Code). Une fois la communication achevée, les clés de session sont détruites.

Figure 8 : *Processus d'authentification et de communications du matériel.*

Authentification Serveur TLS

Vérification et authentification du certificat du serveur



Les termes les plus couramment utilisés dans le domaine de la cybersécurité sont expliqués dans ce glossaire.

Avec sa suite de produits **ADI Assure™**, Analog Devices assure une protection robuste contre les cybermenaces avec à la clé une résilience persistante. Nos solutions de protection en périphérie de réseau Trusted Edge rapprochent la ligne de sécurité de l'origine des données, ce qui augmente le niveau de confiance accordé à leur authenticité et à leur fiabilité. ADI s'engage à aider ses clients à se mettre rapidement en conformité avec les normes et standards cybersécurité et les règlementations en vigueur dans l'industrie, ainsi qu'à renforcer leurs défenses contre des cybermenaces en constante évolution tout au long de la durée de vie de leurs produits. Nos technologies de pointe, telles que le circuit **ChipDNA®** avec fonction physiquement non clonable PUF, le stockage de clé inviolable et les algorithmes de chiffrement avancés, améliorent les architectures de sécurité et renforcent le niveau de résistance aux attaques invasives et non invasives. Notre vaste portefeuille de solutions de sécurité évolutives et flexibles, avec racine de confiance matérielle et services logiciels, assure une protection durable et une grande facilité d'intégration dans l'optique de sauvegarder les systèmes et d'accélérer le processus de certification de la cybersécurité tout en garantissant une résilience à long terme.

CHOISIR LE BON COMPOSANT D'AUTHENTIFICATION MATÉRIELLE, DE LUTTE CONTRE LA CONTREFAÇON, D'ÉTALONNAGE ET DE CONTRÔLE DE L'UTILISATION

AUTHENTIFICATEUR	Clé secrète SHA-2	Clé secrète SHA-3	Clé publique ECDSA	Clé secrète SHA-2 & Clé publique ECDSA
I2C	DS28C22	DS28C50* DS28C16	DS28C36* DS28C39*	DS28C40
1-Wire	DS28E(L)25 DS28E(L)22 DS28E(L)15	DS28E50* DS28E16	DS28E38* DS28E39* DS28E30	DS28E36 DS28E40
NFC	MAX66240 MAX66242	MAX66250		
COPROCESSEUR				
I2C	DS2465	DS2477*		DS2476 DS2478
NFC	MAX66300	MAX66301		

** ChipDNA® PUF Technology*

CIRCUIT INTÉGRÉ SÉCURISÉ DE DÉMARRAGE, DE MISE À JOUR DU FIRMWARE, DE COMMUNICATIONS ET DE PRISE EN CHARGE DU PROTOCOLE TLS

SECURE ELEMENT		ECDSA	ECDH	AES 128/256	Certificats	Protocole TLS
SPI	DS28S60*	X	X	X	Custom	
SPI	MAXQ1065*	X	X	X	x.509	OpenSSL, mbedTLS, WolfSSL

** ChipDNA® PUF Technology*

ANALOG DEVICES

VISIT ANALOG.COM/CYBERSECURITY