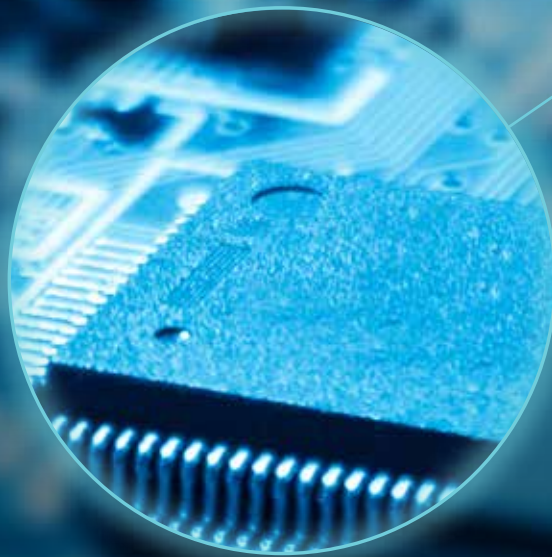


IndustrialProtect™

PROTECTION DES DONNÉES DANS LES INFRASTRUCTURES CRITIQUES.



Applied Intelligence

BAE SYSTEMS
INSPIRED WORK

LE PROBLÈME

Grâce à Internet et aux progrès quotidiens de la science et de la technologie, la société et notre mode de vie ne cessent d'évoluer. La technologie transforme tout et la connectivité entre les personnes, les entreprises et les systèmes devient omniprésente. Pourtant, les systèmes au cœur des industries qui sont aussi au centre de toutes nos sociétés - pétrole, gaz, eau, électricité, usines chimiques, fabrication, centrales nucléaires, etc. - reposent généralement sur des systèmes de commandes industriels conçus dans l'optique de l'efficacité opérationnelle et de la fiabilité plus que de la cyber sécurité.

Il est inquiétant de noter qu'à une époque où la connectivité est très présente, les systèmes industriels critiques qui n'ont pas été conçus à l'origine avec des fonctions de sécurité aptes à résister aux logiciels malveillants ou aux cyber attaques, sont aujourd'hui connectés à Internet, les uns avec les autres par le biais des réseaux TCP/IP et cloud.

Face aux menaces et aux risques qui étaient autrefois insignifiants, mais qui mettent aujourd'hui en péril l'infrastructure dont dépend la société, il convient de trouver des solutions de sécurité qui pourront être mises en œuvre dans les systèmes critiques sans affecter leur fonctionnement.

LA SOLUTION

IndustrialProtect est une de ces solutions capables d'aider ceux qui sont chargés d'élaborer et de mettre en place des mesures de sécurité efficaces dans la technologie opérationnelle qui contrôle les systèmes industriels.

IndustrialProtect™ permet un échange d'informations fiable entre les systèmes de technologie opérationnels et le service informatique de l'entreprise.



IndustrialProtect est construit sur l'hypothèse selon laquelle, si l'on parvient à préserver une séparation sécurisée entre les réseaux informatique et de technologie opérationnelle (OT), le risque et l'impact de toute cyber attaque seront réduits. L'objectif de cette solution est de fournir un échange d'informations sécurisé entre des réseaux segmentés afin que les processus opérationnels puissent continuer à fonctionner entre les réseaux au-delà de leurs frontières propres. Il permet à un réseau de supervision distant de communiquer en toute sécurité avec les éléments du système de commandes ou des systèmes de terrain et de les contrôler, et facilite les communications sécurisées entre les systèmes industriels et les réseaux professionnels, le réseau LAN de l'entreprise ou de l'organisation.

Avec les systèmes industriels, il est indispensable que les commandes envoyées par les réseaux de supervision en vue de contrôler, réguler et recueillir des données soient authentiques et autorisées. Il est également essentiel que les informations envoyées par les systèmes de contrôle vers les réseaux de supervision et au-delà dans l'entreprise ou la société, proviennent de sources connues et autorisées, ce qui garantira qu'aucune donnée non autorisée ou peu fiable ne pourra être introduite dans ces réseaux.

Dans chaque secteur d'activité, les langages et protocoles de contrôle utilisés pour communiquer entre périphériques au sein de réseaux industriels sont spécifiques et parfois uniques aux applications et aux périphériques contrôlés. En garantissant en outre que les communications entre les systèmes et les périphériques sont au format, à la fréquence, dans une structure et un protocole connus et contiennent uniquement un contenu pertinent et autorisé pour la communication entre ces périphériques et systèmes, les personnes chargées de la sécurisation des réseaux industriels peuvent réduire considérablement le risque de mise en péril de leur technologie opérationnelle.

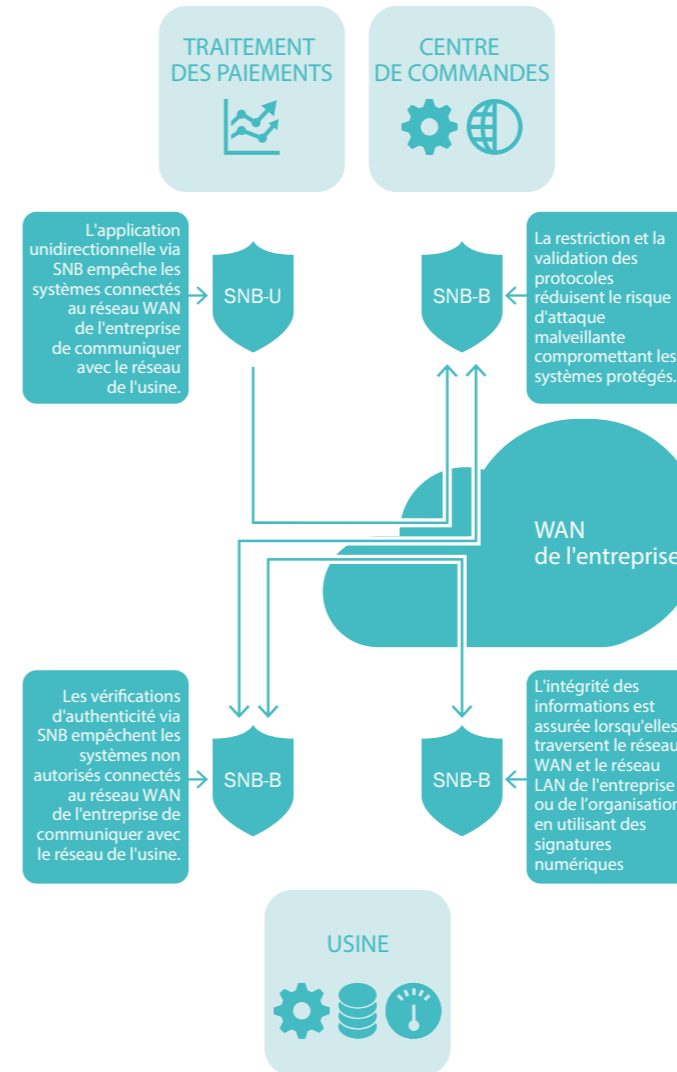
Au cœur de la solution BAE Systems IndustrialProtect se situe une solution (Secure Network Bridge - SNB) qui peut être déployée aux frontières entre segments du réseau : autrement dit, un SNB à la frontière du réseau de commande de supervision ou du système de commandes dans une usine et un autre sur le réseau LAN de l'entreprise.

Le sens de circulation des données au-delà d'un réseau peut être défini pour permettre un transport unidirectionnel ou bidirectionnel des données.

Lorsque les données franchissent la passerelle entre segments du réseau, l'appareil se comporte comme un proxy pour la communication et reconditionne les données dans un format vérifiable, appliquant une rupture complète du protocole. Il analyse ensuite le type, le contenu et la structure de ces données et après les avoir comparées à une liste blanche des communications autorisées, bloque toute communication qui n'est pas acceptée, pertinente ou correctement formatée. Il signe ensuite numériquement la communication, afin de fournir l'assurance de l'autorisation et de l'intégrité du message avant de quitter le système.

Lorsque les données arrivent de l'autre côté de la frontière, le SNB du destinataire extrait les données, les inspecte pour vérifier qu'elles proviennent d'une source connue et vérifie que les données n'ont pas été modifiées depuis qu'elles ont quitté cette source. Il vérifie que les informations sont conformes à une liste blanche avant de les accepter dans ce segment.

Une fonction importante de cette passerelle tient au fait que les fonctions de sécurité sont mises en œuvre dans le matériel et sont par conséquent à l'abri des attaques logicielles. Ces fonctions de sécurité garantissent que les communications entre les passerelles sont résistantes à de nombreux types de cyber attaques, y compris les attaques de type intermédiaire et les attaques par injection de contenu malveillant, qui sont des vecteurs d'attaque courants pour ce type de système.



PRISE EN CHARGE DU PROTOCOLE

Les protocoles utilisés pour communiquer varient selon le secteur d'activité, l'application et le système de commandes. IndustrialProtect prend actuellement en charge les protocoles OSISoft PI et JDBC et des protocoles supplémentaires devraient être ajoutés en 2015 et au-delà. Notre architecture Protocol Connector facilement extensible permet d'ajouter rapidement de nouveaux protocoles, sans avoir besoin d'apporter de changements importants aux éléments d'application de la sécurité du produit.

MISE EN ŒUVRE ET ENTRETIEN

La mise en œuvre de solutions de sécurité dans les opérations et les systèmes de commande existants de l'usine peut être dangereuse. IndustrialProtect comprend une série de services qui garantissent à nos clients qu'ils pourront bénéficier pleinement de la solution avec un minimum de perturbations de fonctionnement : cela comprend le conseil et la prise en charge de la conception, l'installation et la transition vers les opérations en direct, avec un ensemble géré d'assistance et de maintenance qui correspond à la criticité des systèmes que nous protégeons.

AVANTAGES DE LA SOLUTION

- Réduit le risque de mise en péril d'ICS sans perturber les processus professionnels existants
- Permet un flux sécurisé et bidirectionnel des informations, réduisant le besoin de recourir à des processus locaux manuels
- Peut être simplement étendue pour d'autres protocoles de systèmes de commandes
- Interface de gestion centralisée pour simplifier les déploiements à grande échelle et faciliter la gestion simple et la maintenance des systèmes distants
- Conçue pour être simple à installer et à intégrer pour un déploiement rapide

PROTOCOLES PRIS EN CHARGE :

- Applications de base de données
 - JDBC
- SCADA
 - OSISoft PI
- Surveillance
 - SNMP
 - Syslog

À PROPOS DE NOUS

BAE Systems Applied Intelligence propose des solutions qui aident nos clients à protéger et à renforcer leurs actifs critiques dans un monde connecté. Les plus grandes entreprises et les organismes gouvernementaux utilisent nos solutions pour protéger et renforcer leur infrastructure physique, leur nation et leur population, leurs systèmes stratégiques, leur précieuse propriété intellectuelle, les informations de leurs entreprises, leur réputation et leurs relations avec les clients, sans oublier leur avantage concurrentiel et leur réussite financière.

Nous intervenons dans quatre principaux domaines d'expertise :

- Cyber Sécurité – aider nos clients tout au long du cycle de vie des risques pour la cyber sécurité
- Criminalité financière – identification, lutte et prévention des menaces financières, des risques, des préjudices ou des pénalités
- Renseignement sur les communications – fourniture de renseignements de pointe sur les réseaux, protection et contrôles
- Transformation numérique – création d'un avantage concurrentiel et amélioration de la performance opérationnelle grâce à l'exploitation des données et de la connectivité numérique

Nous permettons aux entreprises de devenir plus souples, d'améliorer leur fiabilité et d'opérer de manière plus confiante. Nos solutions contribuent à renforcer la sécurité et la résilience nationales, pour un monde plus sûr. Elles permettent aux entreprises de gérer les risques professionnels, d'optimiser leurs opérations et de se conformer à leurs obligations réglementaires.

Nous faisons partie de BAE Systems, une entreprise mondiale travaillant pour les secteurs de la défense, de l'aérospatiale et de la sécurité, et proposant toute une gamme de produits et de services, parmi lesquels des solutions avancées dans les domaines de l'électronique, de la sécurité et des technologies de l'information.

Victime d'une cyber-attaque ? Contactez notre équipe d'intervention d'urgence aux coordonnées suivantes :

Pour plus d'informations, veuillez contacter :

Royaume-Uni : 0808 168 6647
Australie : 1800 825 411
International : +44 1483 817491
E-mail : cyberresponse@baesystems.com



Certified Service



Cyber Incident Response



Global Headquarters

BAE Systems Applied Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
Royaume-Uni
T : +44 (0) 1483 816000

BAE Systems Applied Intelligence Australia

Level 12
20 Bridge Street
Sydney NSW 2000
Australie
T : +612 9240 4600

BAE Systems Applied Intelligence Dubai

Dubai Internet City
Building 17
Office Ground Floor 53
PO Box 500523
Dubai
T : +971 4369 4369

BAE Systems Applied Intelligence Malaysia

Level 28
Menara Binjai
2 Jalan Binjai, 50450
Kuala Lumpur
Malaisie
T : +60 3 2191 3000

BAE Systems Applied Intelligence USA

265 Franklin Street
Boston
MA 02110
USA
T : +1 (617) 737 4170
E-mail : learn@baesystems.com
Site Web : www.baesystems.com/ai



www.twitter.com/baesystems_ai



www.linkedin.com/company/baesystemsai