
01/12/2017
Auteurs : Hubert Tardieu
Publication European Cyber Week - Cybersécurité de l’Internet des objets
OAI : oai:www.see.asso.fr:20892:20895
DOI : Document accessible sous conditions - vous devez vous connecter ou vous enregistrer pour accéder à ou acquérir ce document.
- Accès libre pour les ayants-droit

Abstract

Authors

Hubert Tardieu


Metrics

Downloaded: 17
Viewed: 0
Size: 1.75 MB
Type: application/pdf
URI: bitcache://16e3b222531e23610cf28b0b2904873b5e7f4762
La SEE (Société de l'Electricité, de l'Electronique et des Technologies de l'Information et de la Communication – Association reconnue d’utilité publique, régie par la loi du 1er juillet 1901) met à la disposition de ses adhérents et des abonnés à ses publications, un ensemble de documents numériques accessibles à partir de son portail des publications. Ces documents incluent notamment les articles des revues REE, 3 EI et e-STA disponibles sous forme numérique ainsi que des publications additionnelles regroupées dans l’espace eREE. Les présentes conditions précisent les conditions de diffusion et d’utilisation de ces documents et des informations qu’ils contiennent. L’accès à ces documents, qu’il se fasse de façon gratuite ou dans le cadre d’abonnements ou d’achats faits à titre onéreux, implique l’acceptation sans restriction de ces dispositions.

Droits de propriété et de diffusion des contenus téléchargés sur le portail des publications

Les contenus rendus accessibles sur le portail des publications sont, en règle générale, protégés par le droit d’auteur. En tant que producteur, et le cas échéant d’auteur, des informations rassemblées dans les contenus accessibles par ce portail, SEE se réserve l'exclusivité des droits de copie et de diffusion de tout ou partie de ces contenus.

Les contenus sont rendus accessibles à titre individuel, pour les besoins de la personne en détenant des droits d’accès en cours de validité. Aussi, la modification, la reproduction et/ou la diffusion via Internet ou le Web, intranet, extranet ou toute autre forme numérique ou imprimée, de tout ou partie des contenus téléchargés sont interdites. Une tolérance est consentie quant à la reproduction d’extraits limités de ces contenus, dans le cadre de travaux ou d’activités auxquels ils sont utiles, à la condition que l’origine de ces reproductions partielles soit mentionnée de façon lisible et sans ambiguïté. Figureront en particulier : la REE (ou toute autre revue accessible sur le portail) en tant que la source, la référence de la publication et le nom de l’auteur (s’il figure dans la revue).

Ces dispositions s’appliquent également aux figures, illustrations, logos ou images.

Publication externe des contenus du portail des publications

Tout extrait des contenus du portail destiné à être utilisé dans des publicités, des communiqués de presse ou du matériel de promotion nécessite un accord préalable écrit de la SEE. Une version préliminaire du document proposé contenant ces extraits doit accompagner chacune de ces demandes. SEE se réserve le droit de refuser un tel usage externe pour quelque raison que ce soit.

Responsabilités

La SEE apporte tout le soin possible à la préparation des informations délivrées dans les contenus produits. Cependant elle ne peut être tenue pour responsable d’aucune perte ou frais qui pourrait résulter d'imprécisions, d’inexactitudes, d’erreurs ou de possibles omissions portant sur des informations publiées, ni des résultats obtenus par l'utilisation et la pratique des informations délivrées.
Utilisation des informations recueillies lors du téléchargement de contenu

Le portail des publications est susceptible d'utiliser des « cookies » afin notamment de permettre l'utilisation de paniers d'achat et de personnaliser les parcours sur le site. SEE se réserve la possibilité d'utiliser les informations recueillies lors des téléchargements pour ses besoins internes et notamment pour l'amélioration de ses services, sans qu'elles puissent être cédées à des partenaires commerciaux. Conformément à la loi "informatique et libertés" du 6 janvier 1978, chaque utilisateur du portail dispose d'un droit d'accès et de rectification aux informations qui le concernent. Pour exercer ce droit, les utilisateurs doivent s'adresser à SEE – 17 rue de l'amiral Hamelin – 75783 Paris Cedex 16, par simple lettre ou en utilisant le formulaire de contact disponible sur son site.

Paris, le 28 avril 2013

Sponsors

 metadata Datacite XML candidate:

<resource xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns="http://datacite.org/schema/kernel-4"
  <identifier identifierType="DOI">10.23723/20892/20895</identifier>
  <creators>
    <creator>
      <creatorName>Hubert Tardieu</creatorName>
    </creator>
  </creators>
  <titles>
    <title>La sécurité de l'IoT pour l'analytique prescriptif : « Common Communication Platform » et « Machine Intelligence »</title>
  </titles>
  <publisher>SEE</publisher>
  <publicationYear>2017</publicationYear>
  <resourceType resourceTypeGeneral="Text">Text</resourceType>
  <dates>
    <date dateType="Created">Mon 4 Dec 2017</date>
    <date dateType="Updated">Mon 4 Dec 2017</date>
    <date dateType="Submitted">Sun 4 Aug 2019</date>
  </dates>
  <alternateIdentifiers>
    <alternateIdentifier alternateIdentifierType="bitstream">16e3b222531e23610cf28b0b2904873b5e7f4762</alternateIdentifier>
  </alternateIdentifiers>
  <formats>
    <format>application/pdf</format>
  </formats>
  <version>35295</version>
  <descriptions>
    <description descriptionType="Abstract"></description>
  </descriptions>
</resource>

dd-mm-yyyy La sécurité de l'IoT pour l'analytique prescriptif : « Common Communication Platform » et « Machine Intelligence » Hubert Tardieu Conseiller du Président 1 Décembre 2017 2 20 Mio proactive accesses per month 5 Mio reactive accesses per month data transfer in reactive mode: 8 TB / month Multivendor-capability open for all suppliers data transfer in system management mode: 25 TB / month more than 30.000 users Hard facts about the running version of the solution Developed in co-investment and co-owned IP Rights More than 400.000 configured systems 3 Example of devices connected to our Platform Energy Healthcare Industry • Paper machines • Ships • Cranes • SIPLACE mounting machines • Building technology (e.g. building automation systems, fire detectors, cameras) • Traffic systems (e.g. traffic computers, traffic light systems, traffic management systems) • GAS Analysis • Train Rail
Multi-factor Authentication Industrial System Vendor Customer A Use Case

App Layer Human-facing IAM services

Multi-factor Authentication, Social Media

IT/OT: Bring Strong authentication & Access control to OT environment

IIoT Service Partner

Secure IAM Services – Multi-tenant, Federation, Open Standards, architectures and blueprints

Machine Intelligence for Prescriptive Security Analytics

Seamless integration of IT, OT and IoT into Security Analytics

IAM for Technologies (quantum crypto, Blockchain)

Resilience to attacks and security breaks (adaptive security)

Seamless IT, OT and IoT Security with prescriptive technologies into OT environment

Identity and Access Management for OT devices

Lightweight Identity and Access Management for OT and IoT from the Edge

Cognitive Security

Prescriptive Security for IT/OT/IoT

Resilient & Agile Cybersecurity aaaS

Extend classic IT security into all regional markets

Large, switches with large number of ports

Investment life cycle

Min 5 to 15 years

Every 2 to 3 years

IT-Security

Industrial Security

Additive Manufacturing/3D Printing

Connected objects

Data IT/OT connections

Intellectual engineering company.

Siemens Energy

Global remote service 7

Traffic System Support Center

Reliable solution that protects traffic systems and customer networks in cities Siemens is an integrated technology company with activities in the fields of industry, energy and healthcare. It is the largest Europe-based electronics and electrical engineering company. Siemens Mobility

Global remote service for traffic systems Business Challenges Our solution Benefits 6 Drägerwerk AG & Co. KGaA, one of the world’s leading manufactures of medical and safety technology • 1889 founded in Germany • headquarter in Lübeck • family owned company • ca. 14,000 employees global • Accessibility of medical devices in hospitals • Ensuring the highest security requirements • Central administration and support • Dynamic scalability • Use of the common Remote Service Platform • Adaptation to individual requirements through customizing • Complete operating model for infrastructure and solution • Extending possibilities into all regional markets • Ensure all required services • Fulfillment of all, also regional specific security requirements • Focusing on core business thanks to full-service model • Extending services possible at any time • No restrictions regarding expansion (volume, regions, etc.) Business challenges Our solution Benefits Dräger Global remote service Business challenges • Remote Service Platform operated as a service • Automated connection process, remote session sharing, extensive logging and reporting • Redundant DMZ infrastructure and fallback configuration • Application of world-class security standards (VPN, encryption, authentication and authorization, data integrity...) Our solution • Standardized processes and worldwide access to system data and information about system conditions for optimal scheduling of service activities and efficient spare parts planning • Facilitating condition monitoring and thus reducing unplanned downtimes significantly which saves more than 80% of time and cost • Shared platform model with usage-based prices guarantee economic remote service and cost transparency Benefits • Providing a remote service interface for remote expert and specialists in Power Diagnostic Centers in Germany and USA as well as for local technicians worldwide • Connecting systems spread all over the globe, like gas and steam turbines • Supporting a wide range of different protocols • Enabling intelligent system diagnostics based on self learning techniques for condition-based maintenance Siemens is an integrated technology company with activities in the fields of industry, energy and healthcare. It is the largest Europe-based electronics and electrical engineering company. Siemens Energy Global remote service 7 The challenge of Manufacturing Industry Increasing Vulnerability & Cyber Attacks targeting IT & OT: IT-Security Industrial Security IT-Security Industrial Security Additive Manufacturing/3D Printing Connected objects Data IT/OT connections Intellectual Property Access to system and applications What is it all about? Exponentially increasing number of incidents and attacks to companies – with both IT and OT as main targets The challenge of Manufacturing Industry Increasing Vulnerability & Cyber Attacks targeting IT & OT: IT-Security Confidentiality Integrity

Confidentiality Integrity Availability

Availability Installation Topology Location of use Device density Network failure times < 300 ms Plant commissioning personnel Plant-specific Harsh environment Low, switches with fewer ports Second to minute range accepted Network specialists Star-shaped Climate-controlled offices Large, switches with large number of ports Investment life cycle Min 5 to 15 years Every 2 to 3 years IT-Security Industrial Security CY 2017


Extend classic IT security technologies into OT environment • Identity and Access Management for OT devices • Lightweight Identity and Access Management for OT and IoT from the cloud • Virtual Security Operations Center for IT, OT and IoT Atos & Siemens Joint R&D: From Classic IT Security to Resilient & Agile Cybersecurity IT/OT/IoT CY 2018 CY 2019+ Security ongoing Security outlook End-to-End Security for IT/OT and IoT as a Service Manage threats and create benefits from disruptive Technologies (quantum crypto, Blockchain)

Resilience to attacks and security breaks (adaptive security)

Seamless IT, OT and IoT Security with prescriptive security analytics

Identity and Access management on the shop floor between devices

Security blueprints for brownfield installations

Cloud security architectures and blueprints

Machine Intelligence for Prescriptive Security Analytics

Seamless integration of IT, OT and IoT into Security Analytics IAM for IT/OT: Bring Strong authentication & Access control to OT environment IoT Service Partner Secure IAM Services – Multi-tenant, Federation, Open Standards, Multi-factor Authentication Industrial System Vendor Customer A Use Case App Layer Human-facing IAM services (Multi-factor Authentication, Social Media
Connect... Core Service Layer Prescriptive Maintenance Remote Field Service PLM Optimization Mass Device Management Big Data Analytics SCADA Databases Connectivity Messaging Federated Expert Customer B Customer Z ... BACKEND SERVICES HUMANS Cloud Platform Orchestration App Mgmt RESTful API MISP Service and Technical User Connect Open Cloud IAM Standards (e.g. SAML) ... ... But this is only the one side of the story ... A fully integrated IAM service architecture must support the whole ecosystem down to the shop floor level IIoT Service Partner Secure IAM Services – Multi-tenant, Federation, Open Standards, Multi-factor Authentication Industrial System Vendor Customer A Use Case App Layer Core Service Layer Prescriptive Maintenance Remote Field Service PLM Optimization Mass Device Management Big Data Analytics SCADA Databases Connectivity Messaging Federated Expert Support Customer B Customer Z ... HUMANS Cloud Platform Orchestration App Mgmt RESTful API MISP Shop Floor Level - Gateways, Devices, Actuators, Sensors Secure IAM Services for Edge Devices /Gateways Engineering System MIS P MACHINES Agent MIS P Agent gateway New IIoT protocols, SDKs, RESTful (portable MISP) ... ... Human-facing IAM services (Multi-factor Authentication, Social Media Connect...) BACKEND SERVICES Service and Technical User Connect Open Cloud IAM Standards (e.g. SAML) ▶ The Siemens IAM architecture and blueprints are based on the following design principles:

- Standards-based: The interfaces of an IAM service component for authentication, authorization and user management must be based on standards. • Usage of Open Source: IAM service component should be based on Open Source components wherever possible. • Integration with existing infrastructure: Authentication must be integrated with existing infrastructure (e.g. enterprise security infrastructure where already user accounts are already managed). • Loose coupling: Possibility to use a system-specific IAM service component to decouple from OT external components to care for offline cases or scenarios with intermittent connections. Design Principles for IAM Architecture IAM is a common concern across OT products PREDICTIVE AUTOMATION ORCHESTRATION SUPERCOMPUTING 14 IT/OT Security Operation Centers Prescriptive Security Analytics Security Powered by Machine Intelligence: Why We Bring Security + Machine Intelligence Together Security is maintained through constant monitoring and alarming Monitoring capabilities are on the rise Data points describe events at particular points in time ▶ This generates lots of data to be reviewed for security We have many data points in the security cloud ... Machine Intelligence offers the right points to connect the dots efficiently The joint Atos/Siemens View: Better detection by interconnecting the IT and the OT security clouds Offering our customers more value by thwarting attacks better IT Data OT Data Big Data Security Analytics Advanced Correlation Engine Incident Handling Processes Threat Intelligence Info Collection Customer Interface Vendor Interface IT- Eco System IT-SIEM* Network • Applications • Behavior • Identities • Location • Endpoint Protection • DDoS • DLP • Encryption • Log Files Threat Intelligence for Detection Threat-DB OT/IT- Eco System • Technology based Security Data • Log Files • Behavior • Perimeter OT/IT-SIEM* Mindsphere Knowledge Base SOC – Graphical User Interface Siemens OT/IT Operation Interface Siemens CSOC Siemens Customer CERT Atos SOC Atos CSIRT/CERT Atos IT Operation Interface *) both are currently using Intel/McAfie SIEM Joint Process Integration (Ticketing, Asset Inventory, Knowledge Base, Data Bus, Process Definitions) DataLake Wave 2: Advanced Analytics Wave 1: Integrated Operational Model Threat Intelligence for Detection Threat-DB External TI External TI distributed distributed SvCZ1: Remote SOC Data Collector Zone & cRSP SvCZ1: OT/IT Field Device Zones & cRSP Advanced Correlation Engine Basic Correlation Engine Prescriptive SOC IT/OT Network of our Customer Prescriptive SOC IT/OT Machine Intelligence Use Cases Customer’s OT Networks In the Focus of the generated Value Proposition: Cross-IT/OT Attacks Machine Intelligence powered Attack Detection and Incident Response Customer’s IT Networks IT to OT Example 1 Detecting Blackenergy & CrashOverride Multi-domain Example 3 Detecting WannaCry OT to IT Example 2 Detecting the crossplatform Malware Value Proposition • Coverage: Various Use Cases addressing main market segments • Automation: Advanced Machine Intelligence methods allow to efficiently identify relevant events, coping with immense data volume • Tangible Offerings: Develop concrete backend tools for productive use in service Attacks across OT/IT borders | dd-mm-yyyy | Author | © Atos - For internal use GBU | Division | Department 18 CCP a joint Siemens/Atos Investment for Next Generation IoT CCP will gradually replace cRSP with the following objectives: • Reduce by an order of magnitude cost and time to connect new equipments and applications • Allow dual way communication to enable prescriptive analytics • Connect 10’s of Millions of objects • Be the only communication channel between the cloud and equipments including for: • mass device management • security policy management • distributed analytics • machine intelligence | dd-mm-yyyy | Author | © Atos - For internal use GBU | Division | Department 19 CCP is a secure and flexible connectivity service to be integrated into IoT environments Codex Communication Platform (CCP) IPSec Reactive Service • Service Engineer with Service Application accesses remote device / system e.g. TeamViewer, RDP, VNC • File Transfer • Device Management Machine to Machine • Messaging • File Transfer • Data Ingestion • Property/Device Monitoring Client-less Devices (e.g. in a hospital network) Websocket Secure Client-less Devices (via connectivity box) Device Client (on single device) • Master Data Management (e.g. Devices, IP Addr., Credentials, Security Policies) • Access Control (Authentication / Authorization) • File Transfer (e.g. support of Amazon S3 Storage), Scheduling, Order Book, Directory Synchronization • Device Management (e.g. Properties, Alerting) • Logging / Audit Trail • Support of the most important Industrial Security Standards e.g. IEC 62443 SSL VPN Device Client (on single device) | dd-mm-yyyy | Author | © Atos - For internal use GBU | Division | Department CCP Backend Components A component architecture with open interfaces enables control of features by ext. applications CCP GUI Master Data Management RESTful API with JSON Optional Components, eventually substituted by customer components File Transfer Audit Authentication Authorization Device Management Remote Access Messaging 20 System/ Device Client | dd-mm-yyyy | Author | © Atos - For internal use GBU | Division | Department CCP Backend Engineering Tool Device Client Remote Access Client Messaging Device Device Client Remote Access Client Messaging Client A messaging channel is used to request, authorize and manage data channels through the CCP proxy framework One or more data channels are opened through the CCP
proxy framework to route the Engineering Tool protocol to the device 1 2 22 Atos, the Atos logo, Atos Codex, Atos Consulting, Atos Worldgrid, Worldline, BlueKiwi, Bull, Canopy the Open Cloud Company, Unify, Yunano, Zero Email, Zero Email Certified and The Zero Email Company are registered trademarks of the Atos group. November 2017. © 2017 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos. Thanks

https://www.see.asso.fr/en/node/20895/landing