
Digital Doorman
Remote Service requires high security standards
worldline

Worldline

an Atos Company

worldline

an atos company

Worldline is one of Atos expert brands to pave your way to digital transformation

Atos

We are a leader in digital services serving a global client base. Atos is the masterbrand of the Group, providing the fundamental values and identity that the sub-brands are based on.

Bull
atos technologies

Bull is the Atos brand for its technology products and value-added software which assist clients in their digital transformation, specifically in the areas of Big Data and Cyber-security. Bull is the European leader in HPC.

UNIFY
atos collaboration solutions

Unify is the Atos brand for unified communication and real time capabilities enhancing social collaboration, digital transformation, and business performance of its clients.

Canopy
atos cloud

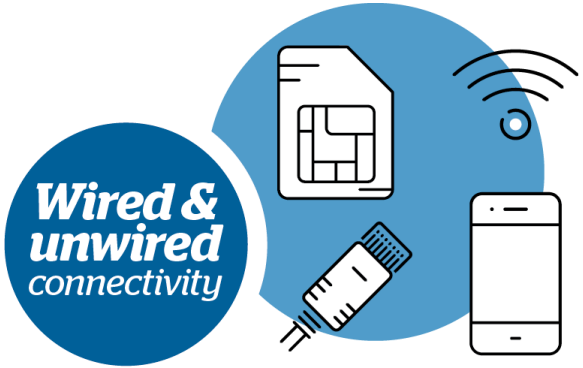
The Atos brand for cloud, Canopy is a cloud services integrator, enabling customers to drive business transformation through open, orchestrated cloud services.

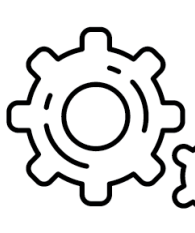
Worldline
atos e-payment services

Worldline is the Atos brand for payments and transactional services. Worldline's innovations and new-generation services enable its customers around the world to engage end consumers and process their transactions securely and efficiently.

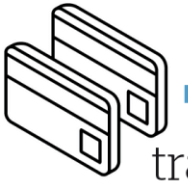
We are the leader for IoT transactions

Objects connected in over **130** countries





+20 protocols managed



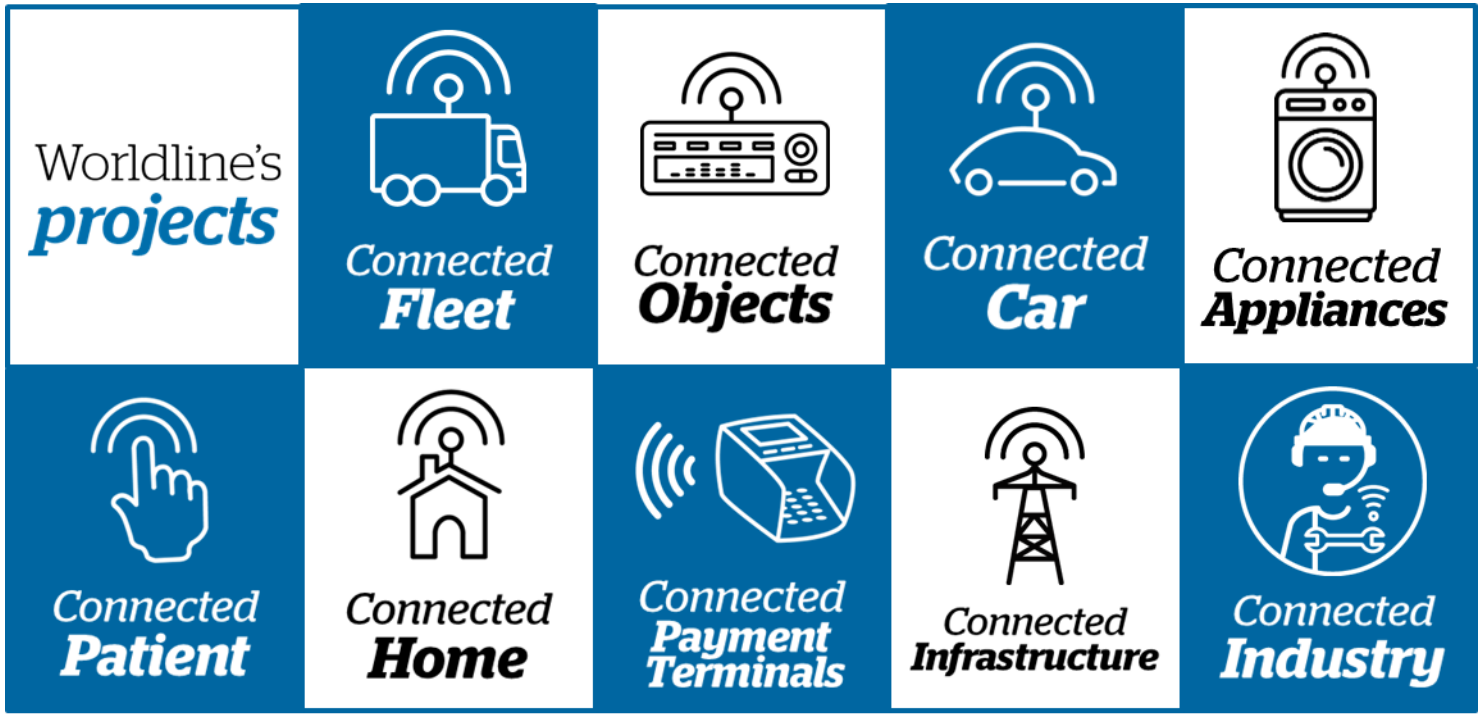
+70M transactions per day

100K messages/sec. in Real-time

More than **2M** objects connected

Worldline figures 2016

A proven experience in managing critical Transactional Services



Selected clients

MICHELIN solutions
RENAULT Passion for life
gorenje
B/S/H/
Dräger
Parrot
EDF
SIEMENS

unlock the power of IoT

worldline

Codex Communication Platform

powered by Worldline

worldline

an atos company

Our Communication Platform: a bilateral secure data tunnel

Backend system (Data Analytics, ERP, CRM, PLM, …)

Codex Communication Platform powered by Worldline

Hosting in Worldline data centers or other partners' data centers

Real-time error detection allowing fast problem fixing

Highly secure data tunnel

Upload of monitoring data, log files etc.

Download of updates, patches, etc.

New instructions for assets

Real-time assistance to service technicians

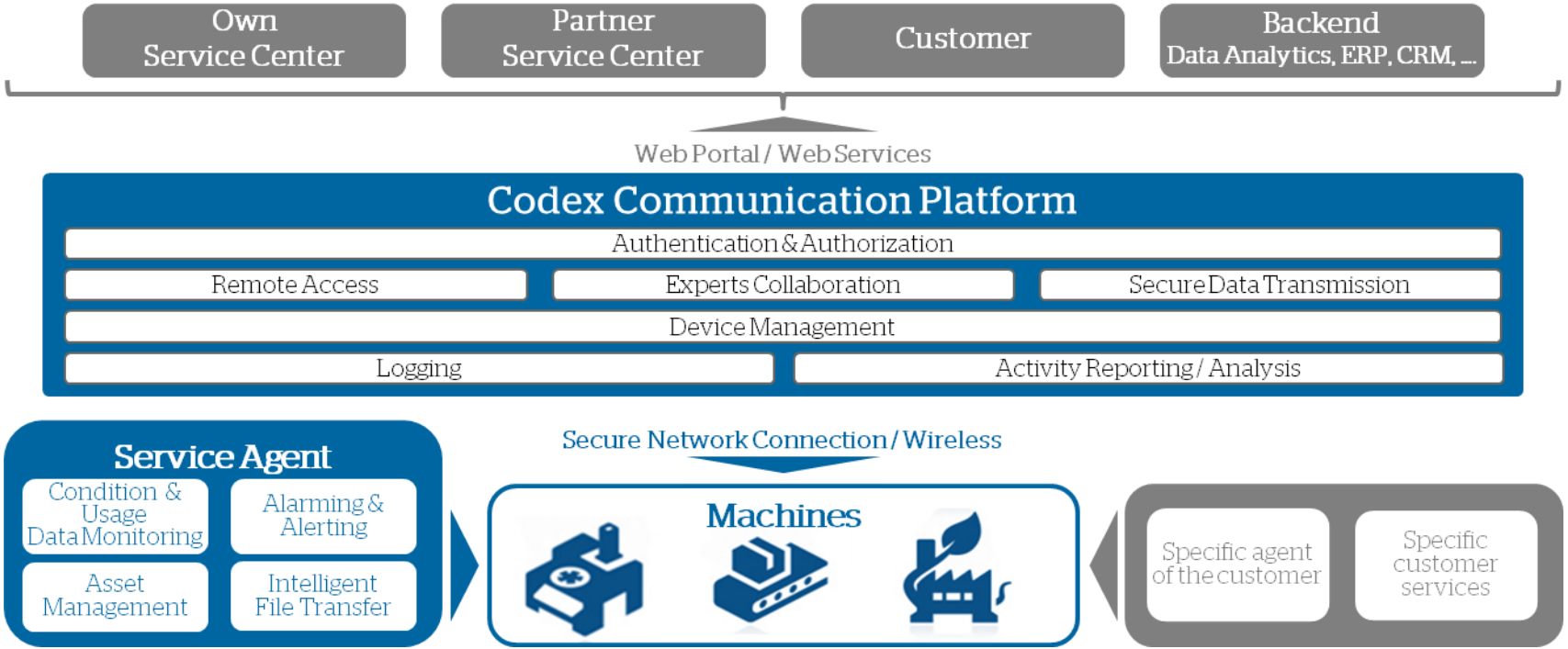
Remote direct intervention on machines in case of emergency

Worldline Service Agent

- Monitoring of assets
- Pre-analysis of results
- Transfer of results to backend

Assets connected locally

The architecture of Worldline's Communication Platform



unlock the power of IoT

worldline

Security of your data is paramount

Security of data collected is a priority

- Respecting customers' security policies
- Increasing security standards
- Reducing risk of production downtime
- Protection of sensitive sites

Exposition to cyber-risk is not an option!
Choose the right trusted partner

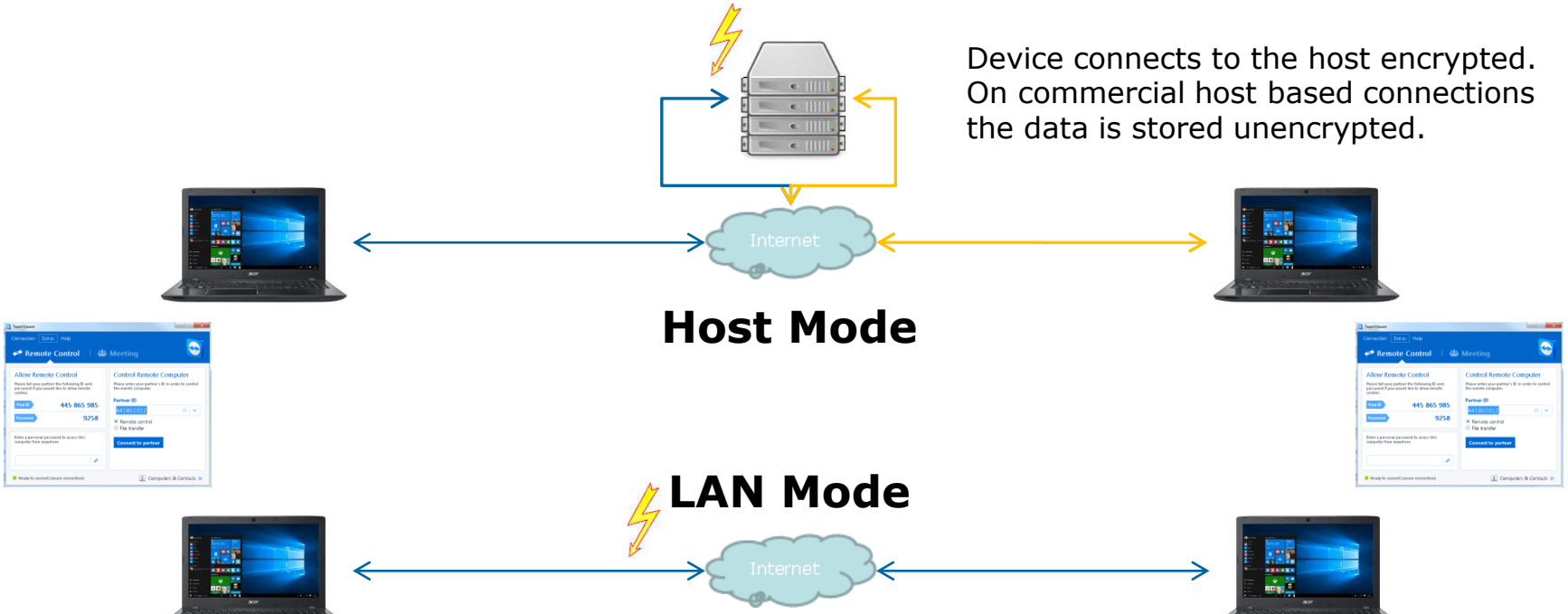
Remote Service

requires high security standards

worldline

an atos company

Architecture of commercial host based connections



Device connects to the host encrypted.
On commercial host based connections the data is stored unencrypted.

Direct connection between the devices.
IP has to be known.

End 2 End security – the last mile

What is it good for?

A lot of threads cannot be prevented or mitigated by transport encryption. Only E2E security implements individual security methods and defines a “security area”.

That means

- Datalinks between E2E secured systems need no additional security mimic
- Connections between systems can be operated unencrypted, without putting the security level at danger
- Intermediate Systems, that route or transfer data have no possibility to read or change the data

End 2 End security – the last mile

What does it regulate – by what is it driven?

- **E2E Security regulates**
  - Data ownership
  - Authenticity of the data
  - Authenticity of all components of the security area which prevents
    - Attacks by feigned participants in the security area
    - Usage of the system by not authenticated persons, systems or components
- **IT/OT convergence will be a driver of security**
  - The security in the IT/OT convergence has to ensure that messages are transmitted authorized and identity-checked between identified partners
- **Preventive/Prescriptive maintenance will be a driver of security**
  - Machines have to be always online and must cope with more dangers

IT-Security Act in the BRD

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015

§8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 **angemessene organisatorische und technische Vorkehrungen** zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen **Kritischen Infrastrukturen** maßgeblich sind.

Dabei soll der **Stand der Technik** eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

Source: https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/it-sicherheitsgesetz.pdf?__blob=publicationFile

IEC* 62443 will very likely become mandatory for Remote Service when used for critical infrastructure

*IEC: International Electrotechnical Commission

IEC 62443: Definitions and Scope

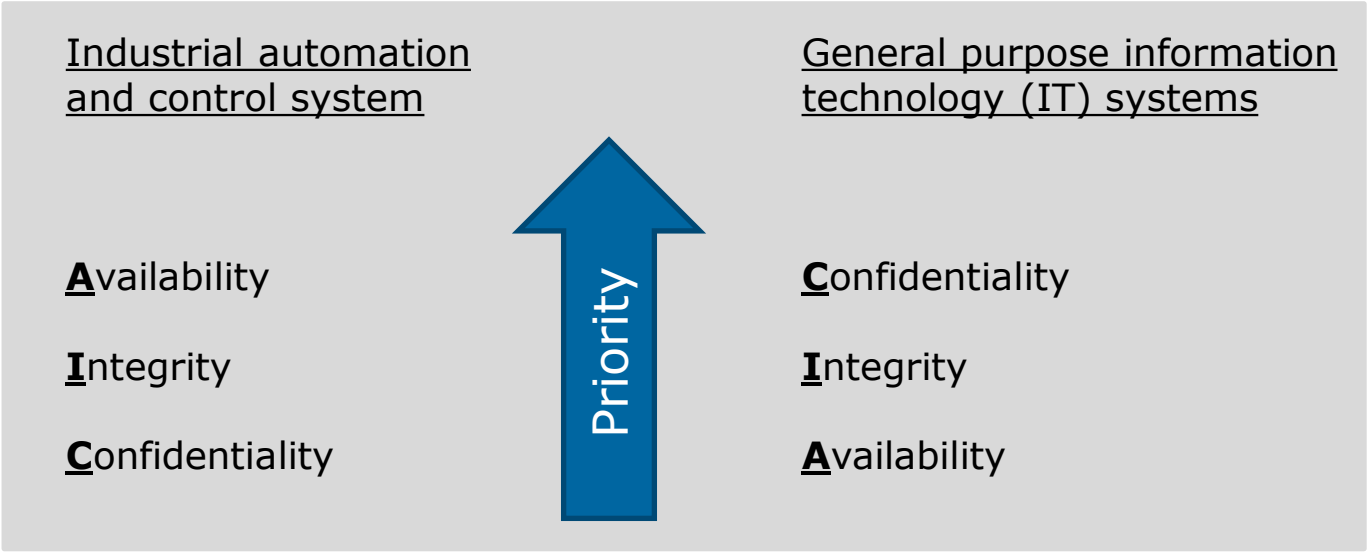
Industrial communication networks – Network and system security

Scope 62443-1-1:

This part of the IEC 62443 series is a technical specification which defines the **terminology, concepts and models for Industrial Automation and Control Systems (IACS) security**. It establishes the basis for the remaining standards in the IEC 62443 series.

The term "**Industrial Automation and Control Systems" (IACS)**, includes control systems used in **manufacturing and processing plants** and facilities, building environmental control systems, geographically dispersed operations such as utilities (i.e., electricity, gas, an water), pipelines and petroleum production and distribution facilities, and other industries and applications such as transportation networks, that use automated or **remotely controlled or monitored assets**.

General Purpose IT-Systems vs. Industrial Automation and Control Systems



Comparison of objectives between IACS and general IT systems

Source: IEC 62443-1-1, Figure 1

IEC 62443: Definitions and Scope

Industrial communication networks – Network and system security

Scope of IEC 62443-3-3:

This part of the IEC 62443 series provides detailed technical control **system requirements (SRs)** associated with the seven **foundational requirements (FRs)** described in IEC 62443-1-1 including defining the requirements for control system capability security levels, SL-C(control system). These requirements would be used by various members of the industrial automation and control system (IACS) community along with the **defined zones and conduits for the system under consideration (SuC)** while developing the appropriate control system target SL, SLT (control system), for a specific asset.

IEC 62443 – Security Levels

Security levels provide a qualitative approach to addressing security for a zone

SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Source: Industrial Security nach ISA 99/IEC 62443 Tagung zur Funktionalen Sicherheit IEC 61508 (VDE 0803), 13.03.2013 Erfurt Dr. Pierre Kobes

When do we have „enough“ security?

- Security is **not a goal that can be reached**
  - New vulnerabilities every day
  - Threats evolve
  - Weak points in the system change → new points of attack

- Security is **an ongoing process** / an attitude → we are all involved
  - „All trust is limited“
  - Motivation / knowledge of attackers
  - Weak points in the system are more likely to be attacked
  - Security may be achieved / lost incrementally

Thanks

For more information please contact:

Dr. Robin Just
Head of Industrial IoT

M: +49 151 11453782
robin.just@worldline.com
Max-Stromeyer-Str. 116
D-78467 Konstanz