OPEN INDUSTRY 4.0
ALLIANCE

Open Industry 4.0 Alliance – Putting secure Industry 4.0 into reality

Nils Herzberg
Chairman/ Spokesperson of the Board, Open Industry 4.0 Alliance
SVP, Global Head - Strategic Partnerships I Digital Supply Chain & Industrie 4.0, SAP SE

OPEN INDUSTRY 4.0
ALLIANCE

=

Industry 4.0 relevant companies – with their interoperable solutions and services – committed to deliver customer value

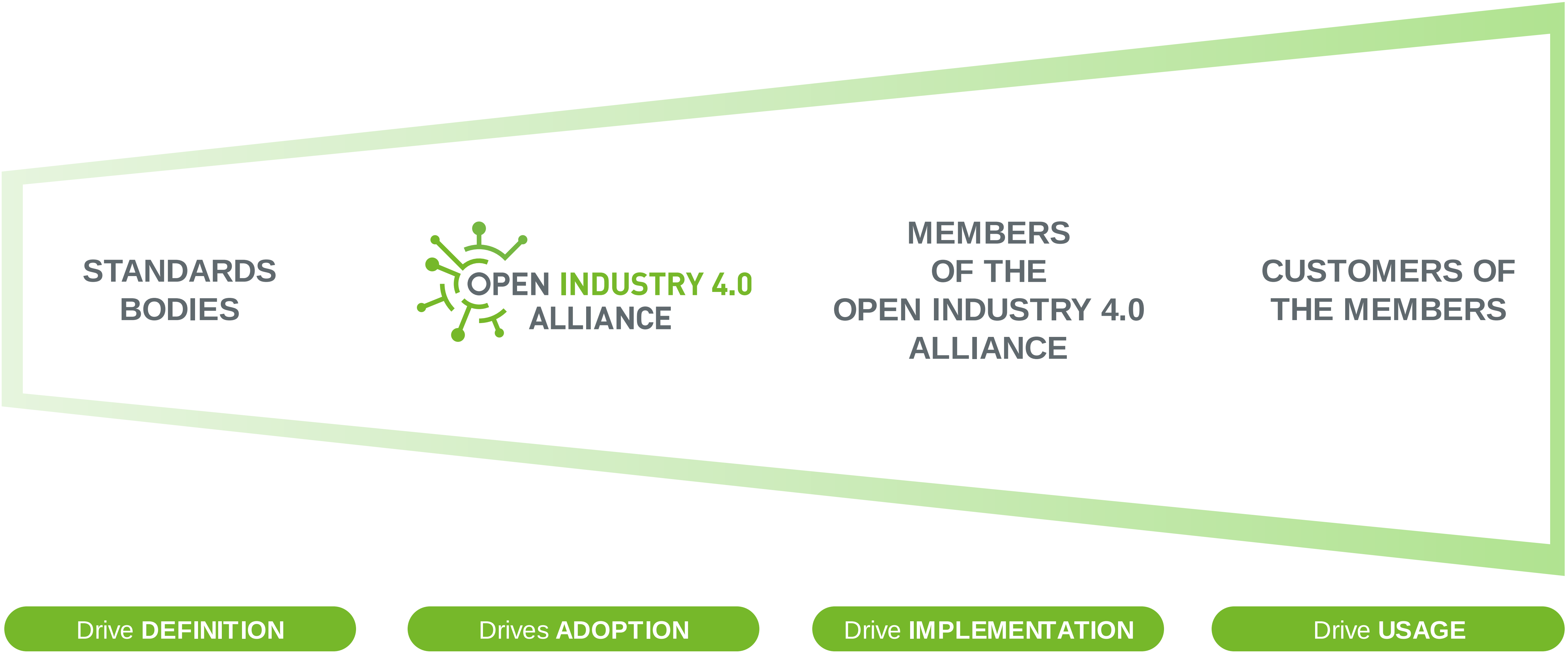
At this time the Open Industry 4.0 Alliance comprises 70+ companies

SCHMIDTSCHE SCHACK ARVOS GROUP	schneider	AUCOTEC	awinia software consulting & development	BALLUFF	BECKHOFF	Beijer ELECTRONICS	BIZERBA	CAPTRON Sensortechnologie
CAXperts	cedalo	CoreTigo	Cybus Independent Industrial IoT	DATAGROUP	diva e	dunkermotoren	DSC Fascination with Integration	EMERSON AVENTICS
Endress+Hauser People for Process Automation	FESTO	FORCAM smart factory experts	FUJITSU	Gallarus Industry Solutions Connection to Innovation	gebhardt	GERMAN EDGE CLOUD	GFT	handtmann Ideen mit Zukunft.
HENGSTLER FORTIVE	HENSOLDT Detect and Protect.	hilscher COMPETENCE IN COMMUNICATION	ifm	itelligence NTT DATA Business Solutions	IT4BI	janztec Industrial Computing Architects	KAESER KOMPRESSOREN	komax
KUKA	MACHIQ	SOFTWARE M&M BY PEOPLE WITH PASSION Member of WAGO Group	mongoDB.	mpdv	MULTIVAC BETTER PACKAGING	MURR ELEKTRONIK stay connected	MHP A PORSCHE COMPANY	NOVATEC
NRX AssetHub Powered by HubHead	PEPPERL+FUCHS	PHOENIX CONTACT	PROSYS OPC	q.beyond	roundSolutions FOR A WIRELESS WORLD	[SO:It] SALT SOLUTIONS Part of Accenture	samson	SAP
schiwa	schmid Engineering GmbH	SCHUNK	SICK Sensor Intelligence.	SMC	software AG Freedom as a Service	SVA	TeamViewer	TREBING HIMSTEDT
VEGA	VOITH	UREASON Responding to your environment	WAGO	weber	WIKA	YOKOGAWA Co-innovating tomorrow	3dSignals	… and recruiting continues

Status: 31.12.2020

Open Industry 4.0 Alliance

Members implement a coherent subset of relevant standards for the benefit of the customer



STANDARDS BODIES

OPEN INDUSTRY 4.0 ALLIANCE

MEMBERS OF THE OPEN INDUSTRY 4.0 ALLIANCE

CUSTOMERS OF THE MEMBERS

Drive **DEFINITION**

Drives **ADOPTION**

Drive **IMPLEMENTATION**

Drive **USAGE**

Open Industry 4.0 Alliance Principles

“ONE” and “OPEN”

ONE Data Semantics and Asset Network

ONE asset repository

ONE attitude to data custodianship

ONE unified approach to security

ONE Catalogue of Members’ OI4 components

ONE Alliance – meaning “no one is dominant”
– everyone has a say

OPEN to all types & bands of equipment

OPEN to all manufacturers & operators

OPEN to run on major hyperscalers

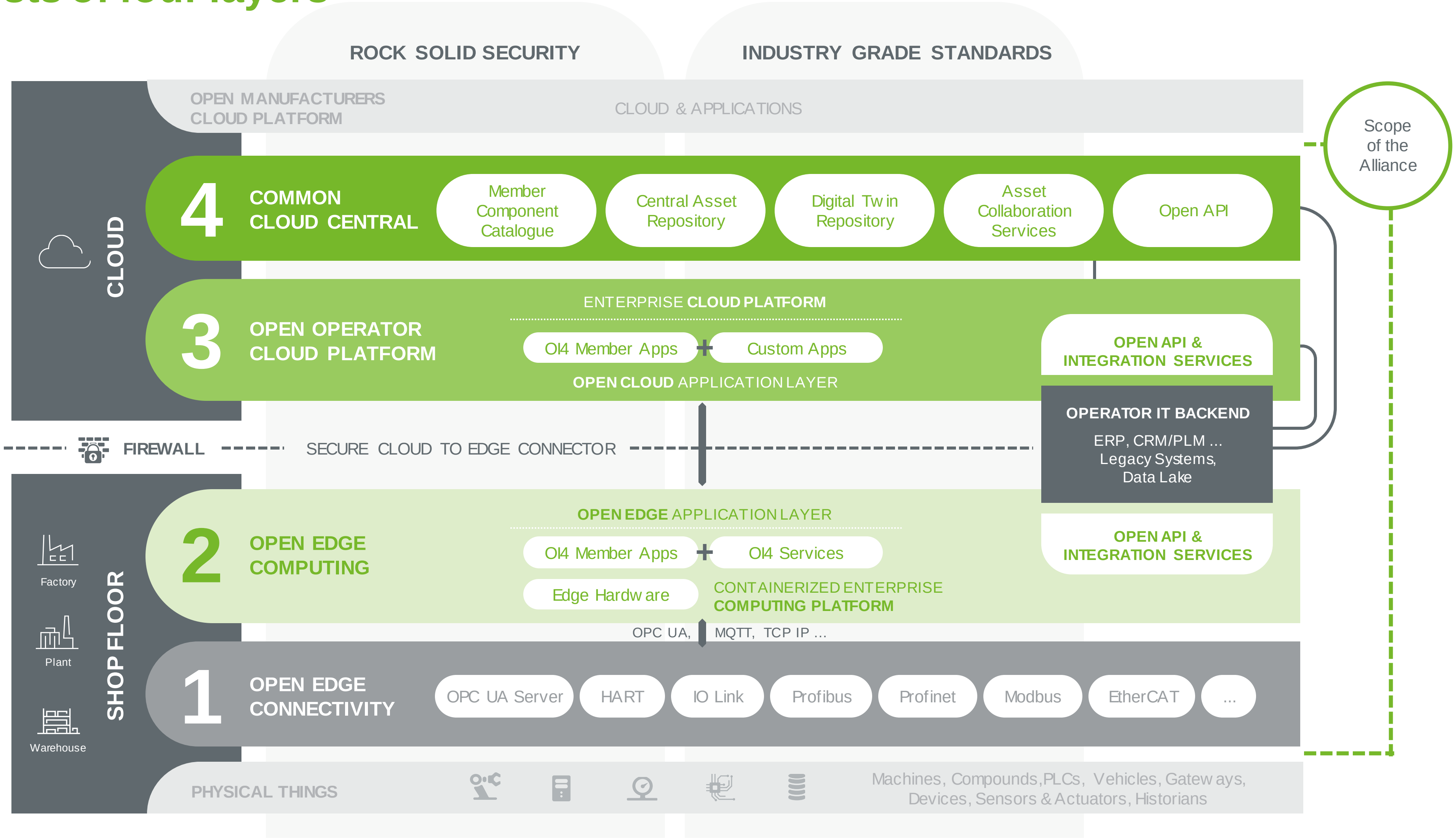
OPEN to all integrators and software providers

OPEN to fair rules-based collaboration across the network

OPEN to embrace Industry 4.0 standards

Open Industry 4.0 Alliance´s Solution Reference Architecture

… consists of four layers



ROCK SOLID SECURITY

INDUSTRY GRADE STANDARDS

OPEN MANUFACTURERS CLOUD PLATFORM

CLOUD & APPLICATIONS

Scope of the Alliance

CLOUD

4 COMMON CLOUD CENTRAL

- Member Component Catalogue
- Central Asset Repository
- Digital Twin Repository
- Asset Collaboration Services
- Open API

3 OPEN OPERATOR CLOUD PLATFORM

ENTERPRISE **CLOUD PLATFORM**

OI4 Member Apps + Custom Apps

OPEN CLOUD APPLICATION LAYER

OPEN API & INTEGRATION SERVICES

OPERATOR IT BACKEND

ERP, CRM/PLM …
Legacy Systems,
Data Lake

FIREWALL

SECURE CLOUD TO EDGE CONNECTOR

SHOP FLOOR

Factory

Plant

Warehouse

2 OPEN EDGE COMPUTING

OPEN EDGE APPLICATION LAYER

OI4 Member Apps + OI4 Services

Edge Hardware

CONTAINERIZED ENTERPRISE **COMPUTING PLATFORM**

OPEN API & INTEGRATION SERVICES

OPC UA, MQTT, TCP IP …

1 OPEN EDGE CONNECTIVITY

- OPC UA Server
- HART
- IO Link
- Profibus
- Profinet
- Modbus
- EtherCAT
- …

PHYSICAL THINGS

Machines, Compounds, PLCs, Vehicles, Gateways, Devices, Sensors & Actuators, Historians

Customer (Operator) Needs assume Security and Data Sovereignty as given

For deriving insights and business benefits from data generated on the shopfloor

Safeguard investment

A low-risk commitment with **strong support** to solve IIoT challenges

Leverage existing brownfield stack

Full **interoperability** with existing operational setup, a **standardized collaboration** platform

Tangible business impact

An **improvement** in availability, performance, output, and quality indexes of operation

No operational disruption

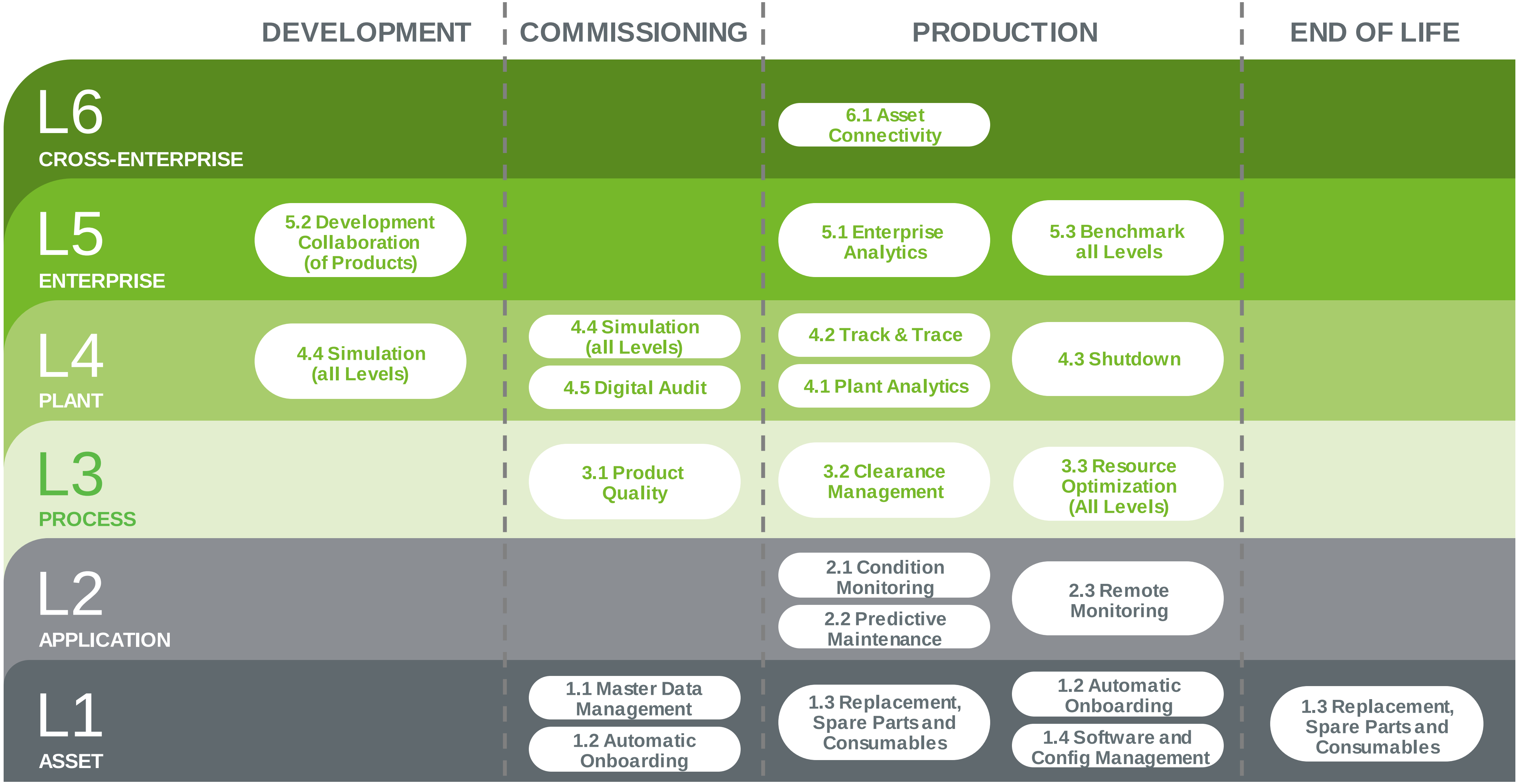
Easy asset onboarding without affecting availability of operation

Security and data sovereignty

Secure cloud architecture without surrendering data uncontrolledly

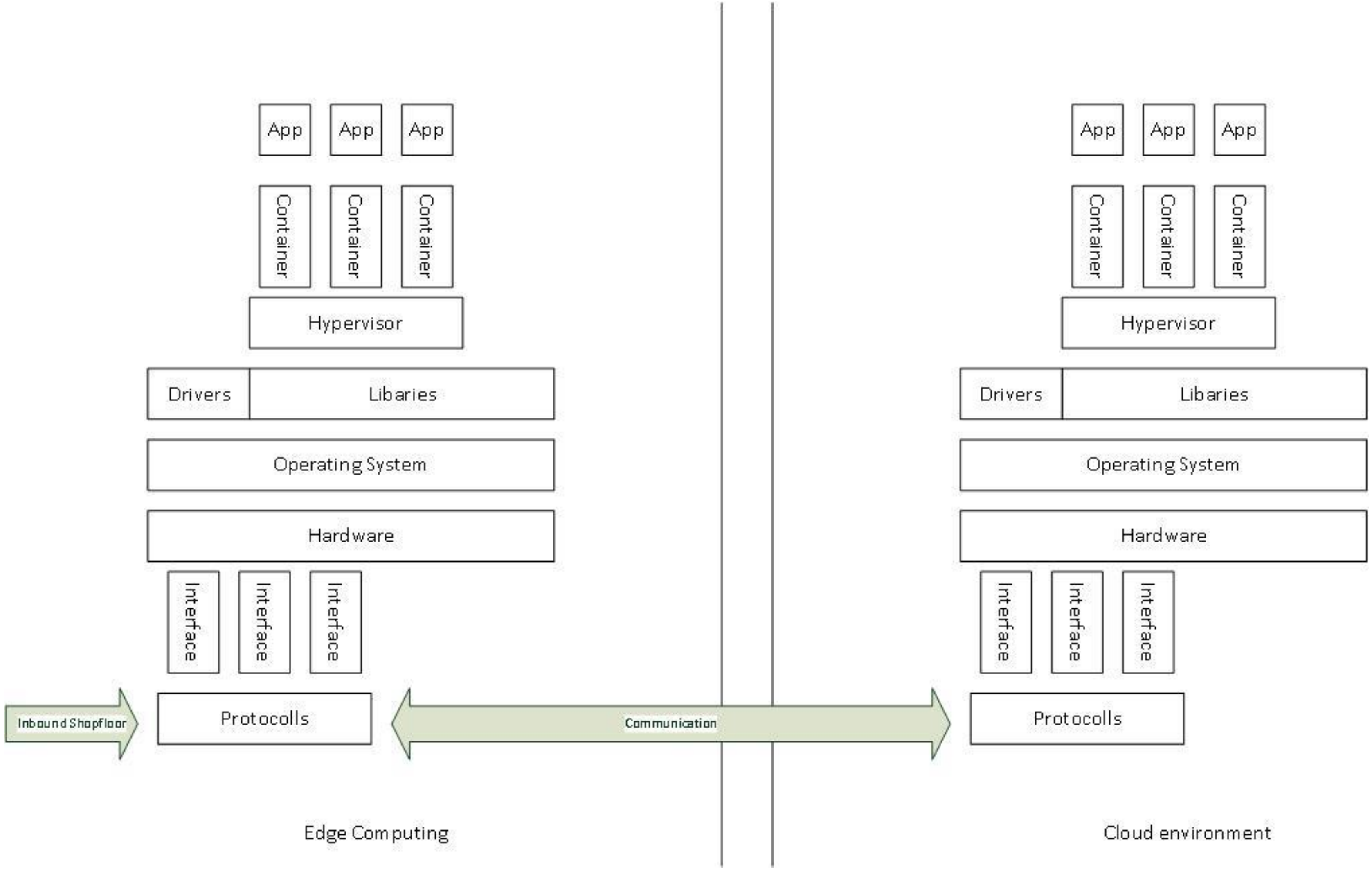
The Open Industry 4.0 Alliance is working to make e2e processes work

Example – Asset Lifecycle



	DEVELOPMENT	COMMISSIONING	PRODUCTION	END OF LIFE
L6 CROSS-ENTERPRISE			6.1 Asset Connectivity	
L5 ENTERPRISE	5.2 Development Collaboration (of Products)		5.1 Enterprise Analytics 5.3 Benchmark all Levels	
L4 PLANT	4.4 Simulation (all Levels)	4.4 Simulation (all Levels) 4.5 Digital Audit	4.2 Track & Trace 4.1 Plant Analytics 4.3 Shutdown	
L3 PROCESS		3.1 Product Quality	3.2 Clearance Management 3.3 Resource Optimization (All Levels)	
L2 APPLICATION			2.1 Condition Monitoring 2.2 Predictive Maintenance 2.3 Remote Monitoring	
L1 ASSET		1.1 Master Data Management 1.2 Automatic Onboarding	1.3 Replacement, Spare Parts and Consumables 1.2 Automatic Onboarding 1.4 Software and Config Management	1.3 Replacement, Spare Parts and Consumables

Full-Stack Secure Solution Architecture



Roles and Responsibilities in the Open Industry 4.0 Ecosystem

Roles involved	Responsibilities
Application Providers	• Follow a secure software development lifecycle • Carefully consider open source software components/tools and integrate only if needed • Ensure vendor risk management when outsourcing development activities
Technology Providers	Software (IaaS, PaaS) providers: • Physically protect infrastructure • Ensure all systems are up-to-date with patch management best practices • Monitor and protect against malicious activity • Manage and protect cloud credentials • Audit frequently Hardware providers: • Design the hardware to meet minimum security requirements • Ensure hardware is tamper proof • Ensure secure software updates
System Integrators	• Deploy hardware securely, for e.g., control access to the hardware with strong authentication and authorization • Separate assets based on criticality using appropriate network security best practices • Ensure a key management mechanism is present to keep authentication keys safe
OEMs/Manufacturers	• Industrial automation and control system security
Operators	• Ensure proper supply chain risk management practices • Ensure suppliers provide security assurance for their solutions and comply with internal security standards
Service Providers	• Ensure proper life cycle risk management practices • Ensure work methods and processes provide security assurance for customer solutions and comply with customer security standards

Relevance of Norms and Standards Regarding Open Industry 4.0 Layer Structure

Norm, Standard / Layer	Layer 1 – Devices	Layer 2 – Open Edge Computing (OEC)	Layer 3 – Open Operator Cloud (OOC)	Layer 4 – Common Cloud Central (CCC)
IEC 62443-4-1 (organizational focus)	x	x		
IEC 62443-4-2 (device focus)	x	x		
OWASP		x		
SSDL - Secure Software Development		x		
DIN SPEC 27070		x		
PSIRT		x		x
IEC 27017			x	x
Cloud Ecosystem			x	x
CSA requirements			x	x

Call to Action – Putting secure Industry 4.0 into reality

Embrace a common and embedded multivendor security framework within the industry

- Combined with better plug ‘n use it can be a competitive advantage PLUS a value driver
- Utilize set-ups like the Open Industry 4.0 Alliance to drive frameworks across all layers of the solution which will enable the e2e scenario

Achieve common interpretation of security across all layers of an hybrid reference architecture

- Based on end-to-end scenarios, establish implementation recommendations for appropriate levels of security
- Ensure that forward looking concepts, like IDTA (Industrial Digital Twin Association) and IDSA (International Data Space Association), embrace and embed security considerations into their work

Ensure massive distribution of relevant knowledge

- Conduct pragmatic plug-fests to establish deficits, but more importantly, so-called ‚How to …‘ guides for the various constituents
- Create lighthouse implementations – not Proof of Concepts – to credibly de-mystify security myths

Establish strong expertise to secure the center stage for the overall topic of security

- Locate the available talent pools for the design, the implementation and audit of Industry 4.0 security

OPEN INDUSTRY 4.0
ALLIANCE

THANK YOU.

www.OpenIndustry4.com

https://www.linkedin.com/company/open-industry-4-0-alliance/

OPEN INDUSTRY 4.0
ALLIANCE

OPEN INDUSTRY 4.0 ALLIANCE
WHITE PAPER

OPEN INDUSTRY 4.0
ALLIANCE

OPEN INDUSTRY 4.0 ALLIANCE
TECHNICAL SOLUTION DESIGN
PRINCIPLES

Enhanced Industry 4.0 Interoperability
for Quicker ROI

OPEN INDUSTRY 4.0
ALLIANCE

OPEN INDUSTRY 4.0 ALLIANCE
INDUSTRIAL CYBERSECURITY
DESIGN PRINCIPLES

End-to-End Protection of Industrial Assets
in a Multi-vendor Scenario

To download Whitepapers:

https://www.openindustry4.com/Download-Center.html