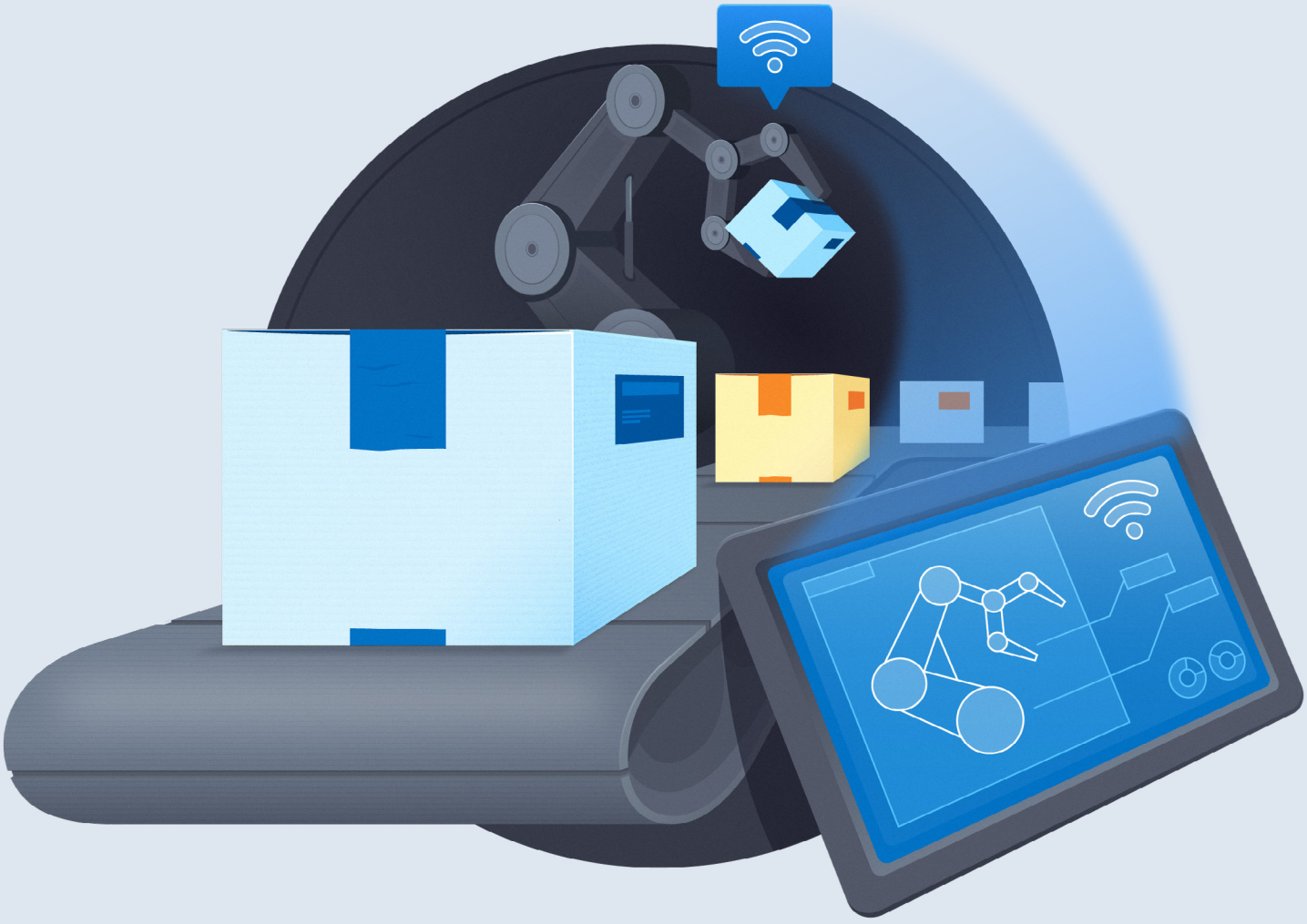
Cloud Industrial Internet of Things (IIoT) - Industrial Control Systems Security Glossary



cloud security alliance®

The permanent and official location for the Industrial Control Systems (ICS) Security Working Group is https://cloudsecurityalliance.org/research/working-groups/industrial-control-systems-ics-security/

Acknowledgments

Lead Author:

Michael Roza

Key Contributors:

William Ho
Sabri Khemissa
Darnell Washington

Peer Reviewers:

Stefan Graf
Nader Zaveri
Olivier Caleff

CSA Analysts:

Haojie Zhuang

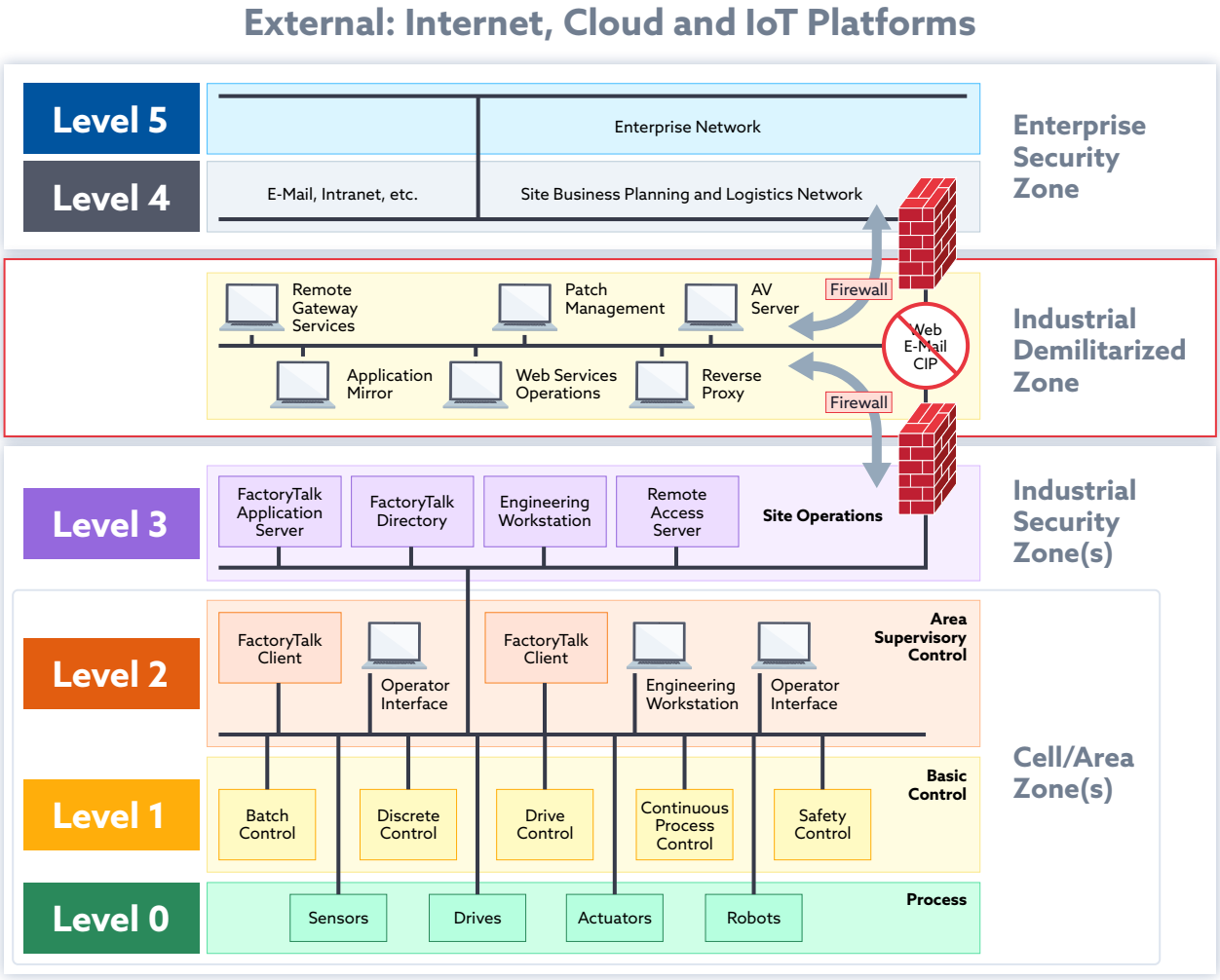
About the Industrial Control Systems (ICS) Security Working Group:
As Industrial Control Systems (ICS) advance from communicating with networks within the enterprise to interacting externally via IoT platforms and the cloud, efficiency, effectiveness and scalability, have improved. However, these advances' additional complexity and larger attack surface have increased the opportunity for cyber-attacks. The ICS Security Working Group (WG) aims to develop security guidance to encourage cloud providers, asset owners and device manufacturers towards adopting best practices to secure ICS.

Table of Contents

Introduction

The Industrial Control Systems (ICS) Security Glossary is a reference document that brings together ICS and IT/OT related terms and definitions.

ICS with access to the cloud via web-enabled services are where IT (Information Technology) and OT (Operational Technology) converge resulting in an integrated process and information flow that brings with it a more complex architecture and security complexities as reflected in the adjusted Purdue Enterprise Reference Architecture (PERA) below.



https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems

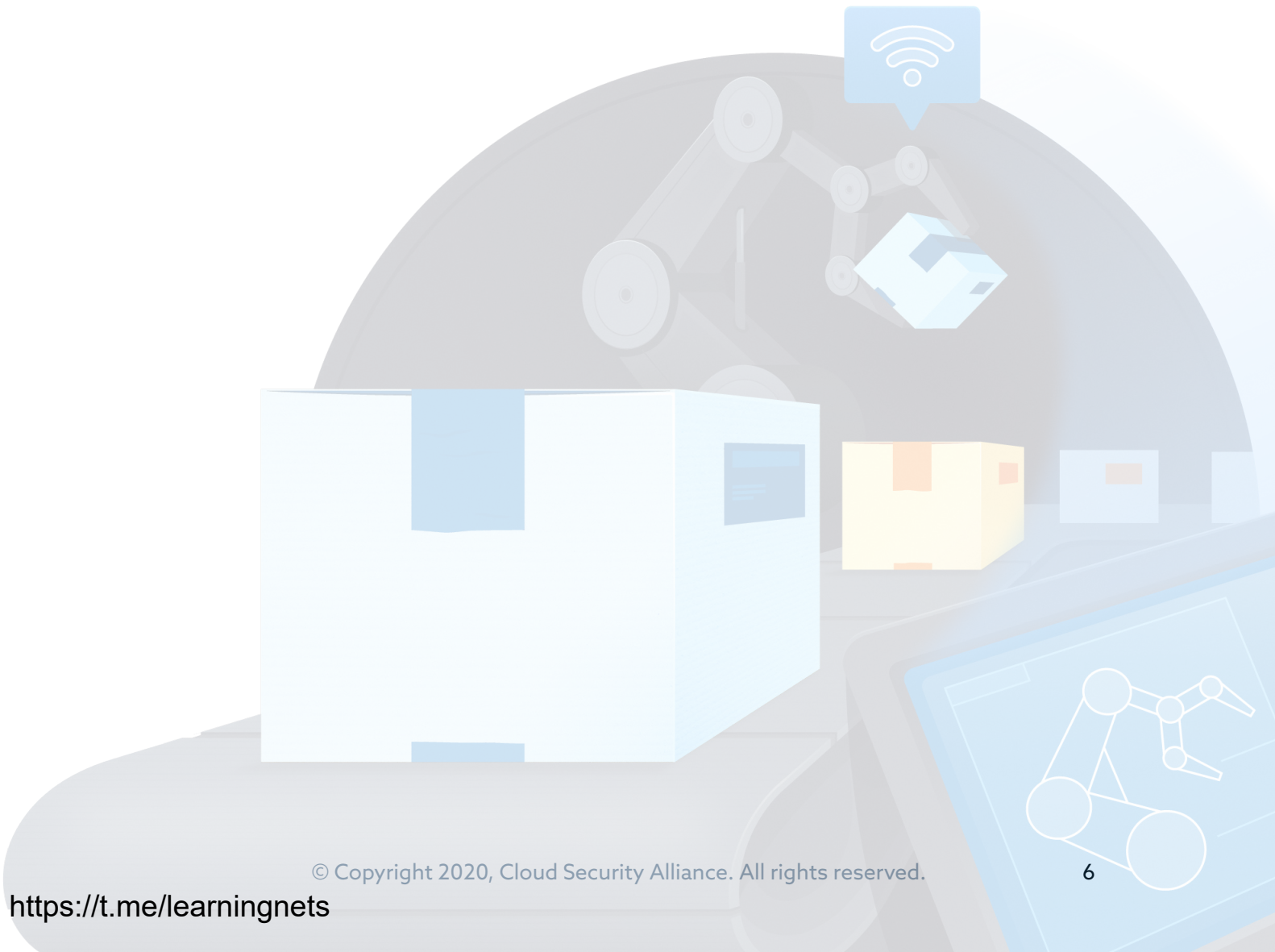
Bringing together the terms and definitions in this document is meant to minimize misinterpretation and provide a common ICS and IT/OT language. A balance has been struck between the length of definitions and understandability with reliance on the reference source as the final arbiter.

Goal

The goal of this document is to provide a common language to stimulate discussion within the group as well as to communicate, understand, debate, conclude, and present the results of the ICS WG's work.

Audience

The intended audience includes everyone from the Board to security staff inside an organization to customers and third-party suppliers including cloud service providers.



Terms and Definitions

#	Term	Definition
1	**Actuators**	An actuator is a component of a machine that is responsible for moving and controlling a mechanism or system, for example by opening a valve. In simple terms, it is a "mover". An actuator requires a control signal and a source of energy. The control signal for an actuator is relatively low energy and may be electric voltage or current, pneumatic or hydraulic pressure, or even human power. Its main energy source may be an electric current, hydraulic fluid pressure, or pneumatic pressure. When it receives a control signal, an actuator responds by converting the signal's energy into mechanical motion. An actuator is a mechanism by which a control system acts upon an environment. The control system can be simple (a fixed mechanical or electronic system), software-based (e.g. a printer driver, robot control system), a human, or any other input.
	Source:	https://en.wikipedia.org/wiki/Actuator
2	**Air-Gapped**	An interface between two systems in which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control).
	Source:	https://csrc.nist.gov/glossary/term/air-gap
3	**Automation Gateway**	Automation gateways are single or multiple devices that can operate as masters "host" or subordinates "slaves" to transmit data using serial lines or TCP/IP between disparate electronic devices. Manufacturers build automation gateways to transmit signals from instrumentation and control devices back to a main controller or data gathering system.
	Source:	http://www.bb-elec.com/Learning-Center/All-White-Papers/Modbus/The-Answer-to-the-14-Most-Frequently-Asked-Modbus.aspx
4	**Control Loop**	A control loop is the fundamental building block of industrial control systems. It consists of all the physical components and control functions necessary to automatically adjust the value of a measured process variable (PV) to equal the value of a desired set-point (SP). It includes the process sensor, controller function, and final control element (FCE) which are all required for automatic control.
	Source:	https://en.wikipedia.org/wiki/Control_loop

5	**Controllers (or Control Server)**	Controllers (or control servers) are most often comprised of Programmable Logic Controllers (PLC), designed to perform logic functions executed by electrical hardware such as relays, switches or sensors. Other types of controllers include Remote Terminal Units (RTUs) that differ from PLCs in that RTUs are more suitable for wide geographical telemetry, often using wireless communications while PLCs are more suitable for local area control. Master Terminal Units (MTU's) are controllers that serve as the Master in an ICS system, controlling the operation of the Slave subsystems (PLCs and RTUs).
	Source:	https://www.sciencedirect.com/topics/computer-science/industrial-control-system
6	**CPS (Cyber Physical Systems)**	Cyber-Physical Systems (CPS) are systems of collaborating computational entities that are in intensive connection with the surrounding physical world and its on-going processes, providing and using, at the same time, data-accessing and data-processing services available on the internet. In other words, CPS can generally be characterized as "physical and engineered systems whose operations are monitored, controlled, coordinated, and integrated by a computing and communicating core" (Rajkumar et al 2010). The interaction between the physical and cyber elements is of key importance: "CPS is about the intersection, not the union, of the physical and cyber. It is not sufficient to separately understand the physical components and the computational components. We must understand their interaction" (Lee and Seshia 2014).
	Source:	https://link.springer.com/referenceworkentry/10.1007/978-3-642-35950-7_16790-1
7	**Data Historian**	A centralized database located in the control system LAN supporting data archival and data analysis using statistical process control techniques.
	Source:	https://www.us-cert.gov/ics/Control_System_Historian-Definition.html
8	**DCS (Distributed Control Systems)**	Refers to control achieved by intelligence that is distributed throughout the system, rather than by a centrally located single unit.
	Source:	NIST SP 800-82r2 https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

9	**DMZ (Demilitarized Zone)**	In computer security, a demilitarized zone (DMZ) or perimeter network is a network area (a subnetwork) that sits between an internal network and an external network. The purpose of a DMZ is that connections from the internal and the external network to the DMZ are permitted, whereas connections from the DMZ are only permitted to the external network -- hosts in the DMZ may not connect to the internal network. This allows the DMZ's hosts to provide services to the external network while protecting the internal network in case intruders compromise a host in the DMZ. For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end. The Security DMZ is used for providing controlled and secure access to services used by external personnel or systems. Access may be granted to control system networks, control system equipment, or other applications services provided.
	Source:	https://www.us-cert.gov/ics/Control_System_Security_DMZ-Definition.html
10	**EMS (Energy Management System)**	An energy management system (EMS) is a computer-aided tool used by power system operators to monitor, control, and carry out optimal energy management. The purpose of an EMS is to determine power generation or power demands that minimize a certain objective such as generation cost, power loss, or environmental effect.
	Source:	https://www.sciencedirect.com/topics/engineering/energy-management-system

11	**Fourth Industrial Revolution**	The phrase Fourth Industrial Revolution was first introduced by Klaus Schwab, executive chairman of the World Economic Forum. In the 2015 article in Foreign Affairs, "Mastering the Fourth Industrial Revolution" was the theme of the World Economic Forum Annual Meeting 2016 in Davos-Klosters, Switzerland. On October 10, 2016, the Forum announced the opening of its Centre for the Fourth Industrial Revolution in San Francisco. This was also the subject and title of Schwab's 2016 book. Schwab includes in this fourth era technologies that combine hardware, software, and biology (cyber-physical systems), and emphasizes advances in communication and connectivity. This Fourth Industrial Revolution is, however, fundamentally different. It is characterized by a range of new technologies that are fusing the physical, digital and biological worlds, impacting all disciplines, economies and industries, and even challenging ideas about what it means to be human. The resulting shifts and disruptions mean that we live in a time of great promise and great peril. The world has the potential to connect billions of more people to digital networks, dramatically improve the efficiency of organizations and even manage assets in ways that can help regenerate the natural environment, potentially undoing the damage of previous industrial revolutions.[WEFORUM]
	Source:	https://en.wikipedia.org/wiki/Technological_revolution#Potential_future_technological_revolutions and https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab
12	**HMI (Human Machine Interface)**	A Human-Machine Interface (HMI) is a user interface or dashboard that connects a person to a machine, system, or device. While the term can technically be applied to any screen that allows a user to interact with a device, HMI is most commonly used in the context of an industrial process. In industrial settings, HMIs can be used to visually display data, track production time, trends, and tags, oversee key performance indicators, and monitor machine inputs and outputs.
	Source:	https://www.inductiveautomation.com/resources/article/what-is-hmi

13	**ICS (Industrial Control Systems)**	A general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).
	Source:	NIST SP 800-82r2 https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
14	**IEC (International Electrotechnical Commission)**	Founded in 1906 IEC prepares and publishes International Standards for all electrical, electronic and related technologies. These are known collectively as "electrotechnology". The IEC is one of three global sister organizations (IEC, ISO, ITU) that develop International Standards for the world. Of particular interest to the CSA WG is IEC's work on the IEC-62443 series of standards addressing Security for industrial automation and control systems. The IEC-62443 series of standards was adopted from the ISA-99 series developed by the ISA (International Society of Automation) providing a framework for mitigating vulnerabilities in Industrial Automation and Control Systems (IACS) associated with Industry 4.0 and Critical Infrastructure.
	Source:	https://www.iec.ch/about/ and https://isaeurope.com/how-can-the-62443-series-of-standards-help-your-company/
15	**IED (Intelligent Electronic Device)**	An Intelligent Electronic Device (IED) is a term used in the electric power industry to describe microprocessor-based controllers of power system equipment, such as circuit breakers, transformers and capacitor banks.
	Source:	https://en.wikipedia.org/wiki/Intelligent_electronic_device

16	**IIoT (Industrial Internet of Things)**	A system that connects and manages sensors as well as actuators while integrating them with mainly cloud-based control components that act together to exercise control in the physical world. IIoT connects and integrates industrial control systems with enterprise systems, business processes and analytics. This combination of machines, computers, and people, enable intelligent industrial operations using advanced data analytics for transformational business outcomes. IIoT may also refer to the integration of a cloud-based IIoT device management solution with on-premise SCADA systems to enable new business processes and analytics.
	Source:	Industrial internet Consortium (IIC). The Industrial Internet of Things Vocabulary Technical Report V2.2. https://www.iiconsortium.org/vocab/
17	**IIoT Edge Gateway & Device**	An Edge Gateway is an intelligent device in edge computing. It is deployed between networks and fulfills mainly two functions: 1. Act as a gateway between the connected industry control system (external) and the local (internal) industry control network. 2. Act as local Control Server (IoT Edge runtime) controlling the locally deployed devices (PLCs, sensors, actors, ...) The IoT Edge runtime runs on each IoT Edge device and manages all local devices using a large variety of protocols, like WiFi, Ethernet, CAN-Bus, Modbus, BACnet or ZigBee. At the same time, it analyses and uses collected process and sensor data to control the actors and provide feedback into a central, mostly cloud-based, control system.
	Source:	https://www.itwissen.info/edge-gateway-EGW-Edge-Gateway.html and https://brainly.in/question/2436258

18	**Industrial Control Plane**	Carries the control information in the network. In industrial networks, control-plane activity consists of any engineering activity related to the maintenance life cycle of the industrial controllers, including any read/change of controller state, control-logic, configuration settings, or firmware. In industrial networks, industrial controllers (e.g. PLCs, RTUs, DCS) are the "brains" responsible for the continuous execution of the entire industrial process lifecycle. These controllers are specialized computers, provided by vendors like Rockwell Automation, Siemens, GE, Schneider Electric and others. These industrial solid-state computers monitor inputs and outputs, and make logic-based decisions. The control plane uses protocols for communicating activities (e.g. firmware download/ upload, configuration updates, code and logic changes) and are mostly proprietary and undocumented. Each vendor uses their own unique implementation of the IEC-61131 standard for programmable controllers. Therefore, they vary based on the vendor and device models. Usually, these control-plane protocols are unnamed because of the fact they were meant to be used internally only via the vendor's engineering software
	Source:	https://info.indegy.com/wp-5-things-industrial-control-plane-ty?submissionGuid=84f66e5e-db70-419c-817f-b678e5ed08f4 Pages 2, 3 and 7
19	**Industrial Data Plane**	Sometimes referred to as the user plane, Industrial Data Plane carries the user-data traffic. In industrial networks, the data-plane is used by the HMI and SCADA applications to communicate process parameters and physical measurements between the human operator and the industrial equipment (I/Os). The Data Plane uses protocols like Modbus, PROFINET and DNP3 which are used by HMI/ SCADA applications to communicate physical measurements and process parameters (e.g. current temperature, current pressure, valve status, etc.). These protocols are typically well documented and standardized.
	Source:	https://info.indegy.com/wp-5-things-industrial-control-plane-ty?submissionGuid=84f66e5e-db70-419c-817f-b678e5ed08f4 Pages 2 and 6

20	**Industry 4.0**	Industry 4.0 is the subset of the fourth industrial revolution that concerns industry. The fourth industrial revolution encompasses areas that are not normally classified as industry, such as smart cities for instance. Although the terms "industry 4.0" and "fourth industrial revolution" are often used interchangeably, "industry 4.0" factories have machines which are augmented with wireless connectivity and sensors, connected to a system that can visualize the entire production line and make decisions on its own. In essence, industry 4.0 is the trend towards automation and data exchange in manufacturing technologies and processes which include cyber-physical systems (CPS), the internet of things (IoT), industrial internet of things (IIOT), cloud computing, cognitive computing, and artificial intelligence. The concept includes: • Smart manufacturing • Smart factory • Lights out (manufacturing) also known as dark factories • Industrial internet of things also called internet of things for manufacturing
	Source:	https://en.wikipedia.org/wiki/Industry_4.0
21	**Industry 4.0 Technologies**	Below are some of the technologies that will transform manufacturing and the supply chain allowing Industry 4.0 to realize its full potential: "Big Data and Analytics, Autonomous Robots , Simulation, Horizontal and Vertical System Integration, The Industrial, Internet of Things, Cybersecurity, The Cloud, Additive Manufacturing, Augmented Reality"[BCG], "Artificial Intelligence, Robotics, Internet of Things, Autonomous Vehicles, 3-D Printing, Nanotechnology, Biotechnology, Materials Science, Energy Storage, Quantum Computing" [WEFORUM]
	Source:	https://www.bcg.com/capabilities/operations/embracing-industry-4.0-rediscovering-growth.aspx and https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

22	**IOC (Indicators of Compromise)**	IOCs are technical artifacts or observables that suggest an attack is imminent or is currently underway, or that a compromise may have already occurred. Indicators can be used to detect and defend against potential threats. Examples of indicators include the Internet Protocol (IP) address of a suspected command and control server, a suspicious Domain Name System (DNS) domain name, a Uniform Resource Locator (URL) that references malicious content, a file hash for a malicious executable, or the subject line text of a malicious email message.
	Source:	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf Page 2
23	**ISA (International Society of Automation)**	Founded in 1945 ISA set the standards for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. Of particular interest to the CSA WG is IEC's work on the ISA-99 series of standards addressing Security Technologies for Industrial Automation and Control Systems. The ISA-99 series of standards developed by ISA (International Society of Automation) was adopted by the International Electrotechnical Commission (IEC) as IEC-62443 providing a framework for mitigating vulnerabilities in Industrial Automation and Control Systems (IACS) associated with Industry 4.0 and Critical Infrastructure.
	Source:	https://www.isa.org/about-isa/ and https://isaeurope.com/how-can-the-62443-series-of-standards-help-your-company/
24	**IT / OT (Operational Technology) Convergence**	IT and OT are primarily seen as different technology areas with different responsibilities. This is due to the different requirements in regards to CIA and safety. IT/OT convergence is the end state sought by organizations, where instead of a separation of IT and OT as technology areas, a integrated process and information flow is used.
	Source:	https://www.gartner.com/en/information-technology/glossary/it-ot-integration

25	**Kill Chain for Industrial Control Systems**	In 2011, Lockheed Martin analysts Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin created the Cyber Kill Chain™ to help the decision-making process for better detecting and responding to adversary intrusions. This model was adapted from the concept of military kill chains and has been a highly successful and widely popular model for defenders in IT and enterprise networks. This model is not directly applicable to the nature of ICS-custom cyber attacks, but it serves as a great foundation and concept on which to build. The ICS Kill Chain has 2 stages: • Stage 1 - Cyber Intrusion Preparation and Execution 1. Preparation 2. Cyber Intrusion 3. Management and Enablement • Stage 2 - Attack Development and Execution 1. Attack Development and Tuning 2. Validation and 3. The Actual Attack
	Source:	https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
26	**MES (Manufacturing Execution System)**	A system that uses network computing to automate production control and process automation. By downloading recipes and work schedules, and uploading production results, a MES bridges the gap between business and plant-floor or process-control systems. NIST Manufacturing Execution Systems (MES) solutions that ensure quality and efficiency are built into the manufacturing process and are proactively and systematically enforced. Manufacturing Execution Systems connect multiple plants, sites, vendors' live production information, and integrate easily with equipment, controllers and enterprise business applications. The result is complete visibility, control and manufacturing optimization of production and processes across the enterprise. SIEMENS
	Source:	NIST:https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf Page B 10 SIEMENS: https://www.plm.automation.siemens.com/global/ja/our-story/glossary/manufacturing-execution-systems-mes/38072

27	**MITRE ATT&CK for ICS Matrix™**	A knowledge base useful for describing the actions an adversary may take while operating within an ICS network. The knowledge base can be used to better characterize and describe post-compromise adversary behavior. An overview of the tactics and techniques described in the ATT&CK for ICS knowledge base. It visually aligns individual techniques under the tactics in which they can be applied.
	Source:	https://collaborate.mitre.org/attackics/index.php/Main_Page
28	**MQTT (Message Queuing Telemetry Transport)**	A Client-Server publish/subscribe messaging transport protocol. It is lightweight, open, simple, and designed to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium. The protocol runs over TCP/IP, or over other network protocols that provide ordered, lossless, bidirectional connections.
	Source:	https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.pdf Abstract at bottom, Page 1
29	**MTUs (Master Terminal Unit or SCADA Server)**	A controller that also acts as a server that hosts the control software which communicates with lower-level control devices, such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), over an ICS network. In a SCADA system, this is often called a SCADA server, MTU, or supervisory controller.
	Source:	NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf page B-3
30	**OT (Operational Technology)**	Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.
	Source:	https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

31	**PAC (Programmable Automation Controllers)**	A programmable automation controller (PAC) is a term used to describe any type of automation controller that incorporates higher-level instructions. A PAC makes it possible to provide more complex instructions to automated equipment, enabling similar capabilities as that of PC-based controls, in an all-in-one package, like a programmable logic controller (PLC). Higher-end PLCs with increased capabilities are often marketed as PAC.
	Source:	https://whatis.techtarget.com/definition/programmable-automation-controller-PAC
32	**PCS (Process Control System),**	Process control systems (PCS) — sometimes called industrial control systems (ICS) — function as pieces of equipment along the production line during manufacturing that tests the process in a variety of ways, and returns data for monitoring and troubleshooting. Many types of process control systems exist, including supervisory control and data acquisition (SCADA), programmable logic controllers (PLC), or distributed control systems (DCS), and they work to gather and transmit data obtained during the manufacturing process.
	Source:	https://www.thebalancesmb.com/process-control-systems-pcs-2221184
33	**PERA (Purdue Enterprise Reference Architecture)**	PERA is a structure with which to design enterprise architectures. It includes a generalized model of the life cycle of an enterprise, and a methodology for planning the evolution of the enterprise. The PERA methodology is unique, in that it: 1. Specifically addresses the human and organizational aspects of the enterprise. 2. It is designed to address all phases of an enterprise from planning, to operations and renewal. 3. Integrates facility engineering and IT systems development methodologies 4. Addresses both process industries and discrete manufacturing.[PERA] This model can be used for a variety of purposes including ICS Kill Chain Analysis[SANS] as well as ICS Network Segmentation Analysis.[SEQ]
	Source:	http://www.pera.net/ and https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297 Page 13 and https://seqred.pl/en/ot_network_segmentation/

34	**PLC (Programmable Logic Controllers)**	A solid-state control system with a user-programmable memory to store instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing.
	Source:	NIST SP 800-82r2 https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
35	**REST (Representational State Transfer)**	REST (REpresentational State Transfer) is an architectural style that defines a set of constraints to be used for developing web services that use the Hypertext Transfer Protocol (HTTP/S). A RESTful interface provides interoperability between computer systems on the Internet and allows the requesting system to access and manipulate data by a uniform set of stateless operations. Data in devices not yet IoT enabled can be utilized by any application that can make RESTful HTTPS requests to read and write data from devices such as controllers.
	Source:	https://www.controldesign.com/articles/2016/it-invades-controller-programming/ and https://en.wikipedia.org/wiki/Representational_state_transfer
36	**RTUs (Remote Terminal Units)**	Remote Terminal Units (RTU) are also referred to as Remote Telemetry Units. An RTU is an electronic device which is controlled by a microprocessor. The main function of an RTU is to interface the SCADA or Distributed Control System (DCS) to physically present objects. The functionality of RTUs and PLCs has started to overlap due to cheaper hardware, thus encouraging the industry to standardize the language for programs on which RTUs run.
	Source:	http://www.differencebetween.net/technology/industrial/difference-between-plc-and-rtu/
37	**SCADA (Supervisory Control And Data Acquisition)**	SCADA systems are used to control dispersed assets where centralized data acquisition is as important as control. These systems are used in various industrial systems. SCADA systems integrate data acquisition systems with data transmission systems and HMI software to provide a centralized monitoring and control system for numerous process inputs and outputs. SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in near real-time. Based on the sophistication and setup of the individual system, control of any individual system, operation, or task can be automatic, or it can be performed by operator commands.
	Source:	NIST SP 800-82r2 https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

38	**Sensors**	A Sensor is a device that identifies the progressions in electrical or physical or other quantities and in a way to deliver a yield as an affirmation of progress in the quantity. In simple terms, Industrial Automation and Control Sensors are input devices that provide an output (signal) with respect to a specific physical quantity (input). Examples of sensor types include temperature, pressure, vacuum, motion, and torque.
	Source:	https://www.plantautomation-technology.com/articles/types-of-sensors-used-in-industrial-automation
39	**SIS (Safety Instrumented System)**	Safety Instrumented Systems are used to monitor the condition of values and parameters of a plant within the operational limits and, when risk conditions occur, they trigger alarms and place the plant in a safe condition or even at the shutdown condition. The main objective is to avoid accidents inside and outside plants.
	Source:	http://www.smar.com/en/technical-article/sis-safety-instrumented-syst02

References and Further Reading

NIST, Special Publication 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), by Keith Stouffer, Intelligent Systems Division Engineering Laboratory, Victoria Pillitteri, Suzanne Lightman, Computer Security Division Information Technology Laboratory Marshall Abrams The MITRE Corporation Adam Hahn, Washington State University, May 2015, available @ https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

ENISA, Communication network dependencies for ICS/SCADA Systems, December 2016 available @ https://www.enisa.europa.eu/publications/ics-scada-dependencies

ENISA, Critical Infrastructure and Services, ICS Scada, Details and Publication List, October 2019, available @ https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada

SANS, Institute InfoSec Reading Room (Featuring 26 Papers as of June 13, 2019), The Industrial Control System Cyber Kill Chain, by Michael J. Assante and Robert M. Lee, October 2015, available @ https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

SANS, Industrial Control System Library, central resource for all ICS Brochures detailing SANS courses, Posters, Surveys, Whitepapers and our Defense Use Case papers, October 2019, available @ https://ics.sans.org/ics_library

ISA, International Society of Automation, Website, October 2019, available @ https://www.isa.org/technical-topics/cybersecurity/

IEC, International Electrotechnical Commission, Website, October 2019, available @ https://www.iec.ch/cybersecurity/

CISA, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, Website, October 2019, available @ https://www.us-cert.gov/ics

NIST, Special Publication 800-150, Guide to Cyber Threat Information Sharing, by Chris Johnson Lee Badger David Waltermire Computer Security Division Information Technology Laboratory, Julie Snyder Clem Skorupka The MITRE Corporation, October 2016, available @ https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

NISTIR 8183, Cybersecurity Framework Manufacturing Profile by Keith Stouffer, Timothy Zimmerman, CheeYee Tang, Intelligent Systems Division Engineering Laboratory, Joshua Lubell, Systems Integration Division Engineering Laboratory, Jeffrey Cichonski, Applied Cybersecurity Division Information Technology Laboratory, John McCarthy, Dakota Consulting, Inc., Silver Spring, Maryland, September 2017, available @ https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf

NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 National Institute of Standards and Technology, April 16, 2018, available @ https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST, Draft Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, JOINT TASK FORCE, August 2017, available @ https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

MQTT Version 5.0. Edited by Andrew Banks, Ed Briggs, Ken Borgendale, and Rahul Gupta. 07, March 2019. OASIS Standard, available @ https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.html
Latest version: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.pdf

Indegy, 5 Things You Should Know About The Industrial Control-Plane, available @ https://info.indegy.com/wp-5-things-industrial-control-plane-ty?submissionGuid=84f66e5e-db70-419c-817f-b678e5ed08f4

SANS, The SANS Institute Reading Room, The Industrial Control System Cyber Kill Chain, Written by Michael J. Assante and Robert M. Lee, October 2015, available @ https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

ENISA, Good Practices for Security of Internet of Things,in the context of Smart Manufacturing, November 2018, available @ https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

MITRE ATT&CK for ICS Matrix™, ATT&CK for Industrial Control Systems, accessed on January 2020, available @ https://collaborate.mitre.org/attackics/index.php/Main_Page