ATENA

H2020-DS-2015-1-Project 700581

Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures

D2.0 – ATENA Glossary

General information

Dissemination level	Public
State	Final
Work package	WP2 Resilience & efficiency models
Tasks	Task 2.1 (in charge of the first version)
Delivery date	31/10/2016
Version	1.0

Editors

Name	Organisation
Tiago Cruz, Jorge Proenca, Paulo Simões	UC

Authors

Name	Organisation
Research teams in all the ATENA consortium partners	All the ATENA consortium partners

Reviewers

Name	Organisation	Date
Ridha Soua, Florian Adamsky	UL	20/10/2016
Chiara Foglietta	UNIROMA3	20/10/2016
Paolo Pucci	FNM	28/10/2016

Executive Summary

This document introduces a glossary encompassing a series of relevant key terms in the scope of the ATENA project. This intends to provide a reference for the reader, but also to constitute a common ground, enabling the ATENA project partners to share a common language. A first version of the glossary is published in the ATENA deliverable D2.1.

This document is intended to be a working copy where definitions can be added in the course of the ATENA project. Some deliverables may reference this document for definition of terms.

Table of Contents

1 Glossary

Terminology	Description	Source
Access	The ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.	US-CERT - Common Cyber Language [1]
Accessibility	Information is available and easily usable (formatted for convenient and immediate use).	US-CERT - Common Cyber Language [1]
Accuracy	Closeness of the agreement between the result of a measurement and a true value of the measure and NOTE Accuracy is generally characterized by the overall uncertainty of a measured value.	ISO 18014-4:2011
Advanced Persistent Threat (APT)	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives using multiple attack vectors (NIST SP800-61).	ISACA – Glossary [2]
Adversary	Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.	US-CERT - Common Cyber Language [1]
Asset	Anything that has value to the organisation NOTE: There are many types of assets, including: information; software, such as a computer program; physical, such as computer; services; people, and their qualifications, skills, and experience; intangibles, such as reputation and image."	ISO 2700:2012
ATENA	Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures.	
Attack	Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.	ISO 27000:2012
Attack Detection (Reorder)	An ongoing attack procedure that was recognized by a security system.	
Attack Mechanism	A method used to deliver the exploit. Unless the attacker is personally performing the attack, an attack mechanism may involve a payload, or container, that delivers the exploit to the target.	ISACA - Cybersecurity Fundamentals Glossary [5]
Attack pattern	Abstracted approach utilized to attack software	ISO 20004:2012
Attack potential	Perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation	ISO 15408:2005
Attack Signature	Sequence of computer activities or alterations that are used to execute an attack and which are also used by an IDPS to discover that an attack has occurred and often is determined by the examination of network traffic or host logs NOTE This may also be referred to as an attack pattern.	IS0 27039:2012
Attack Surface	In software security, the collection of interface points that may be attacked and potentially penetrated by a threat agent (i.e., attacker) to obtain unauthorized access to an asset. An attack surface contains the sum of entry points, but we are most interested in those that are exploitable (i.e., vulnerable) to obtain such access via attack vectors (i.e., paths to exploit the vulnerabilities).	Cigital - Software Security Glossary [6]

Attack Vector	Path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome	ISO 27032:2012
Attacker	Person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources	ISO 27033-1:2009
Audit	Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled NOTE 1: to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines). NOTE 2: to entry: “Audit evidence” and “audit criteria” are defined in ISO 19011.	ISO 27000:2014
Awareness	"Cyber Awareness refers to the security awareness of all persons sharing responsibility for information security. Understanding and motivation are necessary to ensure that security rules are observed and implemented on a continuous basis. To remind employees regularly of the importance of their activities for information security, they must be supported through targeted awareness-raising measures".	CCDCOE - Cyber Definitions [4]
Black-box	Idealized mechanism that accepts inputs and produces outputs, but is designed such that an observer cannot see inside the box or determine exactly what is happening inside that box. NOTE This term can be contrasted with glass box	ISO 18031:2011
Business Continuity	Procedures and/or processes for ensuring continued business operations	ISO 27000:2012
Business Continuity Management	Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities	ISO 22301:2012
Category	The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Access Control,” and “Detection Processes”.	NIST cybersecurity-framework glossary [9]
Coherence	The degree to which data that are derived from different sources or methods, but which refer to the same phenomenon, which are similar.	US-CERT - Common Cyber Language [1]
Commercial-off-the-Shelf (COTS)	Products that are readily available commercially and may be used “as is.”	US-CERT - Common Cyber Language [1]
Comparability	The degree to which data can be compared over time and domain.	US-CERT - Common Cyber Language [1]
Computer Security Incident Response Team CERT	Team of security experts to support the handling of information security incidents	ISO 27019:2013
Configuration Management	Discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status and verify compliance with specified requirements NOTE Adapted from IEEE Std 610.12.	ISO 15408-1:2009

Consequence	Outcome of an event affecting objectives NOTE 1: An event can lead to a range of consequences. NOTE 2: A consequence can be certain or uncertain and in the context of information security is usually negative. NOTE 3: Consequences can be expressed qualitatively or quantitatively. NOTE 4: Initial consequences can escalate through knock-on effects.	ISO 27005:2011
	The effect of an event, incident, or occurrence, including the number of deaths, injuries, and other human health impacts along with economic impacts both direct and indirect and other negative outcomes to society.	US-CERT - Common Cyber Language [1]
Control Systems	Hardware and software components of an IACS	IEC 62443-3-3:2013-v1
	Computer-based systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (opera- tors). Examples of types of control systems include SCADA systems, Process Control Systems, and Distributed Control Systems.	2009 NIPP [11]
Countermeasure	Action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken NOTE 1 to entry: The term “control” is also used to describe this concept in some contexts. The term countermeasure has been chosen for this standard to avoid confusion with the term “control” in the context of “process control”."	IEC 62443-3-3:2013-v1
Critical Infrastructure	"Organizations and facilities that are essential for the functioning of society and the economy as a whole NOTE A: failure or malfunction of such organizations and facilities would result in sustained supply shortfalls, make a significant impact on public security and have other wide ranging impacts."	ISO 27019:2013
Critical Infrastructure Owners and Operators	Those entities responsible for day-to-day operation and investment of a particular-lar critical infrastructure entity. (Source: Adapted from the 2009 NIPP).	US-CERT - Common Cyber Language [1]
Critical Infrastructure Partner	Governmental entities, public and private sector owners and opera-tors and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-profit and private volunteer organizations that share responsibility for securing and strengthening the resilience of the Nation’s critical infrastructure.	US-CERT - Common Cyber Language [1]
Critical Infrastructure Protection	The ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction	EU_Green book
	Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Also called CIP. See also defence critical infrastructure.	CCDCOE - Cyber Definitions [4]
Criticality	The importance of a particular asset or function to the enterprise, and the impact if that asset or function is not available.	ISACA - Cybersecurity Fundamentals Glossary [5]
Cryptography	A way to encode (hide) information such that the sender intends that only the recipient should understand the message.	US-CERT - Common Cyber Language [1]

Cyber Incident	An occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.	US-CERT - Common Cyber Language [1]
Cyber System	Any combination of facilities, equipment, personnel, procedures, and communications integrated to provide cyber services; examples include business systems, control systems, and access control systems.	US-CERT - Common Cyber Language [1]
Cybersecurity Cyberspace Security	Preservation of confidentiality, integrity and availability of information in the Cyberspace NOTE 1 In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. NOTE 2 Adapted from the definition for information security in ISO/IEC 27000:2009.	ISO 27032:2012
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).	US-CERT - Common Cyber Language [1]
Cyberspace	The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.	US-CERT - Common Cyber Language [1]
Cyclic Redundancy Check (CRC)	An error detection code used in digital networks to detect accidental changes in data during transmission or storage.	US-CERT - Common Cyber Language [1]
Decision Support System	An interactive system that provides the user with easy access to decision models and data, to support semi structured decision-making tasks.	ISACA - Glossary [2]
Dependency	The one-directional reliance of an asset, system, network, or collection thereof—within or across sectors—on an input, interaction, or other requirement from other sources in order to function properly.	2009 NIPP [11]
Detect (Function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	NIST cybersecurity-framework glossary [9]
Deterrent	Measure that discourages, complicates, or delays an adversary's action or occurrence by instilling fear, doubt, or anxiety.	US-CERT - Common Cyber Language [1]
Electronic Security Perimeter (ESP)	Adapted from NERC-CIP electric power regulations, a logical perimeter drawn around electronic assets in a security zone to separate it from other zones.	US-CERT - Common Cyber Language [1]
Emergency Cut-off (Blue Light) System	A safety system installed at passenger stations that cuts off traction power and notifies the control centre that power has been cut at this location.	US-CERT - Common Cyber Language [1]
Enterprise Risk Management	Comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.	US-CERT - Common Cyber Language [1]
Enterprise Zone	The zone of a transit agency that handles its routine internal business processes and other non-operational; non-fire, life- safety; and non-safety-critical information.	US-CERT - Common Cyber Language [1]
European Union Agency for Network and Information Security	The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. ENISA actively contributes to a high level of network and information security (NIS) within the Union, since it was set up in 2004, to the development of a culture of NIS in society and in order to raise awareness of NIS, thus contributing to proper functioning of the internal market.	Cf. [12]

Evaluation	Process of examining, measuring and/or judging how well an entity, procedure, or action has met or is meeting stated objectives.	US-CERT - Common Cyber Language [1]
Fail-safe	A device that fails in a manner that protects the safety of personnel and equipment.	US-CERT - Common Cyber Language [1]
Failure	Termination of the ability of a functional unit to perform a required function [ISO/IEC 61508-4] NOTE The inability of a system or component (1) to perform, or the non-performance by the system or component, of an intended function or service; or (2) a deviation of a function or service from its specified, expected performance, resulting in its incorrect performance. Failures fall into two general categories: • Value failures: the functionality or service no fulfills its specified/expected purpose, i.e., it no longer delivers its specified/expected value; • Timing failures: the timing of the functionality or service no longer falls within its specified/expected temporal constraints.	ISO 29193:2011
Fault	Abnormal condition that may cause in reduction, or loss, of the capability of the functional unit to perform a required function [ISO/IEC 61508-4] NOTE The adjudged or hypothesized cause of an error. A fault is considered active when it causes an error or failure; otherwise it is considered dormant. Some dormant faults never become active. In common usage, "bug" or "error" is used to express the same meaning. Software faults include incorrect steps, processes, and data definitions in computer programs. Faults fall into three basic categories: • Development faults: introduced into the software during some stage of its development; developmental faults include incorrect steps, processes, and data definitions that cause the software to perform in an unintended or unanticipated manner; • Physical faults: originate from defects in the hardware on which the software runs (hardware faults include such defects as short circuits or broken wires); • External faults: originate in the interactions between the software and external entities (users, other software).	ISO 29193:2011
Fault Detection	Determination of faults present in a system and time of detection.	Fredrik Gustafsson, Adaptive Filtering and Change Detection, John Wiley & Sons, Ltd, 2000 [14]
Fault Identification	Determination of the size and time-variant behaviour of a fault. Follows fault isolation.	Fredrik Gustafsson, Adaptive Filtering and Change Detection, John Wiley & Sons, Ltd, 2000 [14]
Fault Isolation	Determination of kind, location and time of detection of a fault. Follows fault detection.	Fredrik Gustafsson, Adaptive Filtering and Change Detection, John Wiley & Sons, Ltd, 2000 [14]
Fault Tolerance	A system's level of resilience to seamlessly react to hardware and/or software failure.	ISACA - Glossary [2]
Fibre-optic Strand	A portion of a cable in a fibre-optic network. Each strand carries information unique to it and is isolated from all the other strands.	US-CERT - Common Cyber Language [1]
Fire Life-Safety Security Zone (FLSZ)	A zone containing systems whose primary function is to warn, protect or inform in an emergency. It contains systems such as fire alarms and emergency ventilation.	US-CERT - Common Cyber Language [1]

Forensic Examination	The process of collecting, assessing, classifying and documenting digital evidence to assist in the identification of an offender and the method of compromise.	ISACA - Cybersecurity Fundamentals Glossary [5]
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: The Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the “Cybersecurity Framework.”.	NIST cybersecurity-framework glossary [9]
Framework Core	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.	NIST cybersecurity-framework glossary [9]
Framework Implementation Tier	A lens through which to view the characteristics of an organization’s approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.	NIST cybersecurity-framework glossary [9]
Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.	NIST cybersecurity-framework glossary [9]
Function	One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.	NIST cybersecurity-framework glossary [9]
Hazard	Natural or manmade source or cause of harm or difficulty.	DHS Lexicon, 2010 [3]
Human-machine Interface (HMI)	The control interface between humans and machines.	US-CERT - Common Cyber Language [1]
Identify (Function)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	NIST cybersecurity-framework glossary [9]
Incident	Event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system	IEC 62443-3-3:2013-v1
Incident Mitigation (or simply Mitigation)	The activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during, or after an incident. Mitigation measures are often formed by lessons learned from prior incidents. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards. Measures may include zoning and building codes, floodplain buyouts, and analysis of hazard-related data to determine where it is safe to build or locate temporary facilities. Mitigation can include efforts to educate governments, businesses, and the public on measures they can take to reduce loss and injury.	ICS - Glossary [15]

Incident Response (or Reaction)	Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavourable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at pre-empting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.	ICS - Glossary [15]
	(B767or intrusion response) actions taken to protect and restore the normal operational conditions of an Information System and the information stored in them when an attack or intrusion occurs	ISO SD
April 2007Incident Service Restoration (or Recovery)	The development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental, and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents.	ICS - Glossary [15]
Information Sharing	The process through which information is provided by one entity to one or more other entities to facilitate decision-making under conditions of uncertainty.	US-CERT - Common Cyber Language [1]
Informative Reference	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each subcategory.	NIST cybersecurity-framework glossary [9]
Inputs	Resources invested into the program or activity being measured, such as funds, employee-hours, or raw materials.	US-CERT - Common Cyber Language [1]
Interdependency	Mutually reliant relationship between entities (objects, individuals, or groups); the degree of interdependency does not need to be equal in both directions.	US-CERT - Common Cyber Language [1]
Intrusion	An unauthorized act of bypassing the security mechanisms of a network or information system.	US-CERT - Common Cyber Language [1]
Isolate Attack(s)	The act of containing an attack within a perimeter, in order to mitigate and minimize its impact.	
Likelihood	"Chance of something happening NOTE 1: In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period). NOTE 2: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English."	ISO 27005:2011

Loss of Control	Sharing with inappropriate entities (i.e., unauthorized users) and sharing for inappropriate purposes (i.e., unauthorized uses).	US-CERT - Common Cyber Language [1]
Malware	Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability NOTE Viruses and Trojan horses are examples of malware.	ISO 27033-1:2009
Man-in-the-middle (MitM)	A type of cyber-attack where an interloper inserts him- or herself in-between two communicating devices, without either side being aware of the interloper.	US-CERT - Common Cyber Language [1]
Metric	A quantifiable entity that allows the measurement of the achievement of a process goal.	ISACA - Glossary [2]
Mitigation	Capabilities necessary to reduce loss of life and property by lessening the impact of disasters.	US-CERT - Common Cyber Language [1]
Mobile Code	Program transferred between a remote, possibly "untrusted" system, across a network or via removable media that can be executed unchanged on a local system without explicit installation or execution by the recipient NOTE 1 to entry: Examples of mobile code include JavaScript, VBScript, Java applets, ActiveX controls, Flash animations, Shockwave movies, and Microsoft Office macros.	IEC 62443-3-3:2013-v1
Network	A group of components that share information or interact with each other to perform a function.	2009 NIPP [11]
Network and Information Security	It refers to the safeguards and actions that can be used to protect the cyber domain, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.	Adapted from [16]
Network Resilience	The ability of a network to: (1) provide continuous operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged); (2) recover effectively if failure does occur; and (3) scale to meet rapid or unpredictable demands.	US-CERT - Common Cyber Language [1]
Operations Control Centre	A central location that monitors, and in some cases controls, some portion of a transportation system. It may handle just one system or many systems simultaneously.	US-CERT - Common Cyber Language [1]
Outcomes	Events, occurrences or changes in condition that indicate programmatic progress, brought about at least in part through outputs.	US-CERT - Common Cyber Language [1]
Outputs	Completed or delivered products or services generated through inputs.	US-CERT - Common Cyber Language [1]
Patch Management	Area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system NOTE Patch management tasks include: maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation and documenting all associated procedures, such as specific configurations required remotely across heterogeneous environments according to recognized best practices. "	IEC 62443-2-1:2010-v1
Performance evaluation	Process of determining measurable results	ISO 22301:2012
Performance Management	The use of performance information to affect programs, policies, or any other organization actions aimed at maximizing the benefits of public services.	US-CERT - Common Cyber Language [1]
Performance Measurement	Regular measurement of the results (outcomes) and efficiency of services or programs.	US-CERT - Common Cyber Language [1]

PICERL	SANS model for Incident response, encompassing the following stages: Preparation, Identification, Containment, Eradication, Recovery and Lessons learned.	SANS Institute - Infosec Reading Room [17]
Prevention	Those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism.	US-CERT - Common Cyber Language [1]
Privileged User	A user that is authorized (and, therefore, trusted) to perform security- relevant functions that ordinary users are not authorized to perform.	NIST cybersecurity-framework glossary [9]
Processes	The steps that turn inputs into outputs.	US-CERT - Common Cyber Language [1]
Programmable Logic Controller (PLC)	Programmable logic controller.	ISO 27019:2013
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	NIST cybersecurity-framework glossary [9]
Quality of Service	A utility company's quality of service applies to the delivery of services to the end user. "Delivery" in this context includes activities preceding and following service delivery and the network components (hardware and software) through which those services (telephone signals, water, and voltage) are provided. Certain services are common to all three utility industries (telecommunications, electricity, and water), and the quality concerns are likewise similar, notably in regard to customer and technical services (e.g., timely installations or connections, prompt responses to customer complaints, efficient billing practices, safeguarding of customer accounts, accuracy of customer information, and network reliability). Other concerns about non-price performance are industry-specific.	Lynne Holt, paper "Utility Service Quality - Telecommunications, Electricity, Water", March 2004 [18]
Recover (Function)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	NIST cybersecurity-framework glossary [9]
Recovery (1)	Those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources.	US-CERT - Common Cyber Language [1]
Recovery (2)	The activities after an incident to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.	US-CERT - Common Cyber Language [1]
Redundancy	Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.	US-CERT - Common Cyber Language [1]
Relevance	The degree to which the product meets user needs for both coverage and content.	US-CERT - Common Cyber Language [1]
Residual Risk	Risk that remains after risk management measures have been implemented.	US-CERT - Common Cyber Language [1]
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.	US-CERT - Common Cyber Language [1]
Respond (Function)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	NIST cybersecurity-framework glossary [9]

Risk (1)	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.	NIST cybersecurity-framework glossary [9]
Risk (2)	Combination of the probability of an event and its consequence	ISO 2700:2009
Risk Analysis	Process to comprehend the nature of risk and to determine the level of risk NOTE 1: Risk analysis provides the basis for risk evaluation and decisions about risk treatment. NOTE 2: Risk analysis includes risk estimation."	ISO 27000:2012
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation	ISO 27000:2012
Risk Avoidance	Decision not to become involved in, or action to withdraw from, a risk situation	ISO 27005:2009
Risk Communication	Exchange or sharing of information about risk between the decision-maker and other stakeholders	ISO 27005:2009
Risk Estimation	Activity to assign values to the probability and consequences of a risk	ISO 27005:2009
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable NOTE: Risk evaluation assists in the decision about risk treatment.	ISO 27000:2012
Risk identification	Process of finding, recognizing and describing risks NOTE 1: Risk identification involves the identification of risk sources, events, their causes and their potential consequences. NOTE 2: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.	ISO 27000:2012
Risk Management (1)	The process of identifying, assessing, and responding to risk.	NIST cybersecurity-framework glossary [9]
Risk Management (2)	The process of identifying, analysing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.	US-CERT - Common Cyber Language [1]
Risk Management (3)	Coordinated activities to direct and control an organization with regard to risk NOTE: Risk management generally includes risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review."	ISO 27000:2009
Risk Prediction	The process of analysing and anticipating the possible occurrence of a risk-related event.	

Risk Treatment	"Process to modify risk NOTE 1: Risk treatment can involve: – avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; – taking or increasing risk in order to pursue an opportunity; – removing the risk source; – changing the likelihood; – changing the consequences; – sharing the risk with another party or parties (including contracts and risk financing); and – retaining the risk by informed choice. NOTE 2: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction". NOTE 3: Risk treatment can create new risks or modify existing risks."	ISO 27000:2014
SCADA	A control system involving a master terminal unit and remote terminal units, used for supervisory control and data acquisition.	US-CERT - Common Cyber Language [1]
Scenario	A scenario consists of a CI model, the initial states of all components and the scenario behaviour that describes the events that happen within the scenario.	CIPRNet CIP glossary [19]
Sector	A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society.	Adapted from 2013 NIPP [8]
Security Metric	quantitative measure of the confidence in the assurance that availability, integrity and confidentiality of data as well as access to and use of data and automation devices is protected, data flows are securely managed, and anomalous events are reported in a timely manner.	ISA99 Committee - ISA 99 wiki [20]
Service Operative Level	The service operative level corresponds, in measurable terms, to the characterization of the operating service conditions provided by a utility or provider, within a time frame.	
Service Restoration	The act of reinstating a service after the occurrence of an incident interrupting its delivery.	
Smart Extension	A device developed within the scope of the CockpitCI FP7 project, designed to improve the availability and resiliency of legacy RTU and PLC devices.	CockpitCI Project [21]
Software Defined Security	Software-defined security (SDS) is a type of security model in which the information security in a computing environment is implemented, controlled, and managed by security software. It is a software-managed, policy-driven and governed security where most of the security controls such as intrusion detection, network segmentation and access controls are automated and monitored through software.	Symantec™ Data Centre Security - Glossary [22]
Subcategory	The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."	NIST cybersecurity-framework glossary [9]
System	Combination of interacting elements organized to achieve one or more stated purposes NOTE 1 A system may be considered as a product and/or as the services it provides. NOTE 2 In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g. aircraft system. Alternatively the word system may be substituted simply by a context dependent synonym, e.g. aircraft, though this may then obscure a system principles	ISO 15443-1:2011

	perspective. NOTE 3 NOTEs 1 and 2 are also taken from ISO/IEC 15288:2008.	
Terrorism	Premeditated threat or act of violence against non-combatant persons, property, and environmental or economic tar- gets to induce fear, intimidate, coerce, or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives.	DHS Lexicon, 2010 [3]
Threat(1)	Potential cause of an unwanted incident, which may result in harm to a system or organization	ISO 27000:2012
Threat(2)	Capabilities, intentions and attack methods of adversaries, or any circumstance or event, whether originating externally or internally, that has the potential to cause harm to information or a program or system or cause those to harm others	ISO 21827:2002
Threat(3)	A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.	US-CERT - Common Cyber Language [1]
Threat Identification	The process of identifying situations or conditions that have the potential to cause injury to people, damage to property, or damage to the environment.	ENISA - Glossary [23]
Trusted (Network)	Network of an organization that is within the organization's ability to control or manage. Further, it is known that the network's integrity is intact and that no intruder is present.	US-CERT - Common Cyber Language [1]
Unauthorized Access	Any access to an information system or network that violates the owner or operator's stated security policy.	US-CERT - Common Cyber Language [1]
Uncertainty	The state of being not known, indeterminate, questionable, variable.	US-CERT - Common Cyber Language [1]
Use case	Use cases are often employed in information technology systems design and engineering. They describe the desired response of a system when it receives external requests. The technique is used to develop the behavioural requirements for a system by describing numerous functional scenarios. Each use case characterizes the interaction between an actor (which may be a human user, another system, or a hardware device that initiates an action) and the system. Use cases typically represent the function as a sequence of simple steps. Each use case is a complete series of events, as seen from the actor's point of view. Use cases in their full, formal sense are often associated with the Unified Modelling Language (UML), the Rational Unified Process (RUP), and Systems Modelling Language (SysML). Their application increased during the 1990s, especially among those who employ object-oriented design and programming. Simple, informal use cases may also be applied in various settings. Some of the planning documents being drafted by the Federal Agencies Digitization Guidelines Initiative provide use cases as a form of explanation. For example, the objectives for still imaging (still in draft form at this writing) are stated as simple use cases, e.g., "patron makes a hard copy of one or more images for personal use.".	Federal Agencies Digitization Guidelines - Glossary [24]
Vector (for cyber-attack)	The path an attacker takes to attack a network.	US-CERT - Common Cyber Language [1]
Virtual Private Network	A computer network in which some of the connections are virtual circuits instead of direct connections via physical wires within some larger network, such as the internet.	US-CERT - Common Cyber Language [1]
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats	ISO 27000:2012
White-listing	Describes a list or register of entities that are granted certain privileges, services, mobility, access or	US-CERT - Common Cyber Language [1]

	recognition.	

2 References

[1] US-CERT, “Common Cyber Security Language,” 2013.

[2] Information Systems Audit and Control Association - ISACA, “ISACA Glossary,” [Online]. Available: http://www.isaca.org/Pages/Glossary.aspx?tid=2043&char=A. [Accessed September 2016].

[3] DHS Risk Steering Commitee, Department of Homeland Security Risk Lexicon, Washington, DC: Department of Homeland Security (DHS), 2010.

[4] NATO, “Ciber Definitions,” [Online]. Available: https://ccdcoe.org/cyber-definitions.html. [Accessed October 2016].

[5] Information Systems Audit and Control Association - ISACA, “ISACA Cybersecurity Fundamentals Glossary,” [Online]. Available: http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf. [Accessed September 2016].

[6] Cigital, “Software Security Glossary & Terms,” [Online]. Available: https://www.cigital.com/resources/software-security-glossary/. [Accessed September 2016].

[7] SANS, “Glossary of Security Terms,” [Online]. Available: https://www.sans.org/security-resources/glossary-of-terms/. [Accessed September 2016].

[8] M. Chertoff, National Infrastructure Protection Plan (NIPP), Washington, DC: Department of Homeland Security (DHS), 2013.

[9] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” NIST, 2014.

[10] NEC, “Glossary: Cyber Attacks,” [Online]. Available: http://www.nec.com/en/global/solutions/cybersecurity/about/words.html. [Accessed September 2016].

[11] M. Chertoff, National Infrastructure Protection Plan (NIPP), Washington, DC: Department of Homeland Security (DHS), 2009.

[12] ENISA, “ENISA - About,” [Online]. Available: https://www.enisa.europa.eu/about-enisa. [Accessed October 2016].

[13] H. D. Unbehauen, Control Systems, Robotics and AutomatioN – Volume XVI: Fault Analysis and Control, EOLSS Publications, 2009.

[14] F. Gustafsson, Adaptive Filtering and Change Detection, Wiley, 2000.

[15] FEMA, “Federal Emergency Management Institute (FEMA) - ICS Glossary,” [Online]. Available: https://training.fema.gov/emiweb/is/icsresource/assets/icsglossary.pdf. [Accessed September 2016].

[16] EUR-Lex, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” European Union, 2013.

[17] M. Pokladnik, “An incident handling process for small and medium businesses,” SANS, 2007.

[18] L. Holt, “Utility Service Quality - Telecommunications, electricity, water,” *Utilities Policy,* pp. 189-200, September 2005.

[19] CIPRNet, “CIPRNet CIP glossary,” [Online]. Available: https://www.ciprnet.eu/glossary.html. [Accessed July 2016].

[20] ISA99 Commitee, “ISA99 Wiki - Glossary of Terms,” 2013. [Online]. Available: http://isa99.isa.org/ISA99%20Wiki/Master-Glossary.aspx. [Accessed October 2016].

[21] CockpitCI, “A European FP7 Project – CockpitCI,” [Online]. Available: https://www.cockpitci.eu/. [Accessed October 2016].

[22] Symantec, “Glossary,” [Online]. Available: http://help.symantec.com/cs/DCS2.0/DCS2_0/v107984745_v110163010/Glossary/?locale=EN_US. [Accessed August 2016].

[23] ENISA, “Threat and Risk Management Glossary,” [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/glossary. [Accessed October 2016].

[24] Federal Agencies Digitalization Guidelines Initiative, “FADGI - Glossary,” [Online]. Available: http://www.digitizationguidelines.gov/term.php?term=usecase. [Accessed August 2016].