R1.3: IoT-T-Projektglossar

Einheitliche Definitionen für das Projekt

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Version 4.2, Datum: 30.06.2017

Autoren:

Frank-Walter Jäkel (Ed) – Fraunhofer IPK
Theo Margraf – AUDI AG
Stefan Stölzle – AUDI AG
Paul Hopton – Relayr
Yuliya Brynzak – Relayr
Michael Wagner – Fraunhofer FOKUS
Axel Rennoch – Fraunhofer FOKUS
Rutten, Stefan – DEKRA
Andre Wardaschka – DEKRA

Inhalt

1 Einleitung

Das IoT-T-Projektglossar ist für alle Partner des Projekts im Internet seit Februar 2017 verfügbar. Der folgende Report thematisiert den aktuellen Stand der Begriffsdefinitionen. Die Begriffe haben einen starken IoT Bezug. In einzelnen Fällen beziehen sich die Begriffe auf Aspekte der zu realisierenden Anwendungsbeispiele wie sie im Report R1.1 Reviewer beschrieben sind. Ziel ist es ein möglichst einheitliches Verständnis der Begrifflichkeiten zwischen den Projektpartnern zu erreichen.

1.1 Erfassung und Dokumentation der IoT-Prüfanforderungen

Die Beschreibung der Begriffe erfolgt in einer WebApp „https://iot-t.fokus.fraunhofer.de/term/“. Alle Projektpartner haben zu dieser App entsprechende Zugriffsrechte. Neben des Begriffes, der entsprechenden Definition, dem Verantwortlichen und dem Reviewer können in der App auch Referenzen, mögliche Anwendungsfälle zum Begriff, Feedbacks und eine englische Definition hinterlegt werden (siehe Abbildung 1).

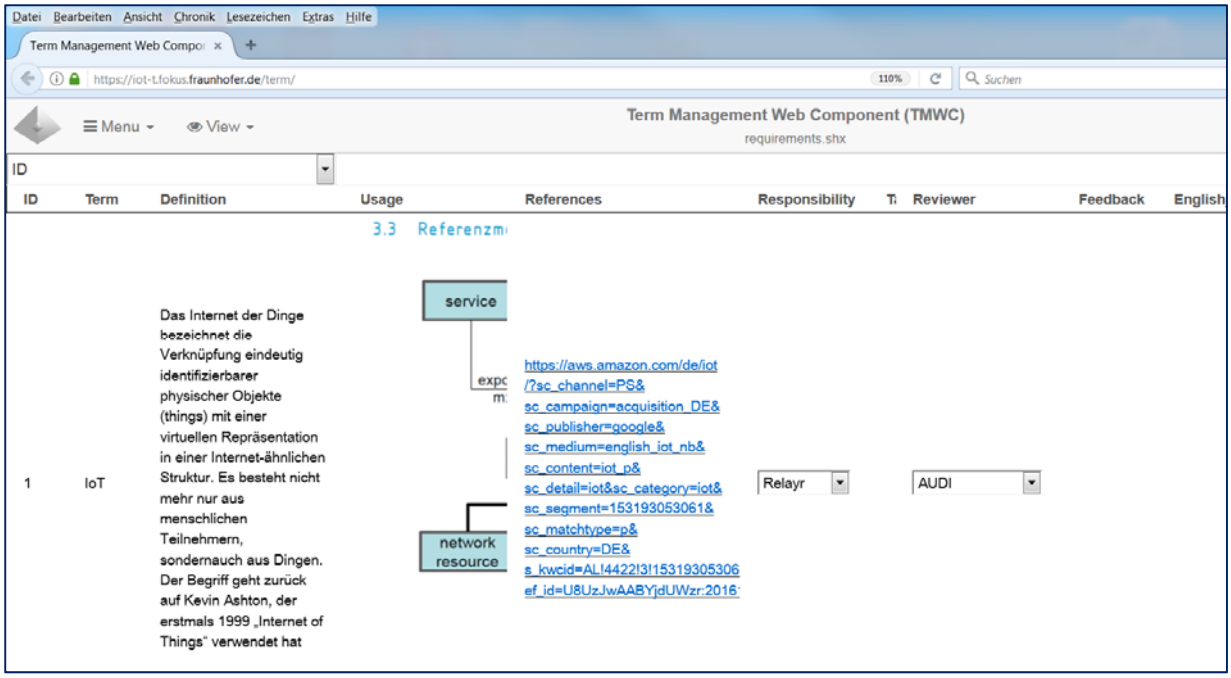

Abbildung 1: Beispiel für die Begriffsdefinition in der WebApp

Die Daten werden in einer zentralen Engine gesammelt und können von dort weiterverarbeitet werden.

1.2 Vorgehen

Die Begriffe des Glossars wurden in Projekttreffen und Telefonkonferenzen sowie in den Dokumenten der Partner identifiziert und nach kurzer Diskussion gesammelt. Anschließend wurden Verantwortlichkeiten für die Erstellung der jeweiligen Definition zugeordnet. Zur besseren Absicherung der Definition wurde zudem ein Reviewer bestimmt. Da einige Begriffe in englischer Sprache vorlagen wurde auch die Möglichkeit zum Hinterlegen der englischen Definition zur Verfügung gestellt. Fragen zu den Definitionen wurden in Telefonkonferenzen geklärt. Es wurden auch gängige Akronyme in das Glossar aufgenommen, welche im IoT Kontext häufig verwendet werden.

2 IoT-T- Projektglossar

2.1 Aufbau

Der Report beinhaltet die aktuelle Sammlung an Begriffen, welche im Projekt weiter ergänzt werden kann. Dabei wurden nur der **Begriff**, die **Definition** und die **Referenz** in den Report übernommen.

2.2 Liste der Begriffe

2.2.1 Cloud

Definition:

Eine Cloud im Kontext der IT ist eine Ansammlung von Hard- und Software, welche dem Anwender die wesentlichen Merkmale von Cloud-Computing bereitstellt. Dazu gehören unter anderem die bedarfsorientierte Selbstzuweisung und Skalierbarkeit von Ressourcen, ein breiter Netzwerkzugriff und die Erreichbarkeit über das Internet sowie Mandantenfähigkeit und messbare Dienste.

Referenz:

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdfhttp://www.gartner.com/it-glossary/cloud-computing/

2.2.2 CoAP

Definition:

Das Constrained Application Protocol (CoAP) ist ein Übertragungsprotokoll, das von der IETF eigens für das Internet der Dinge entwickelt wurde. Ähnlich wie HTTP folgt CoAP dem REST Paradigma, ist dabei jedoch deutlich ressourcenschonender.

Referenz:

coap.technology

IETF RFC 7252

2.2.3 Cyber System / Physical System

Definition:

Ein CPS ist eine Verbindung von einem physischen System und deren digitale Abbildung in einer vernetzten Infrastruktur. Das physische System besteht dabei aus Hardware Komponenten wie zum Beispiel Maschinen oder anderen mechanischen und elektronischen Teilen. Über die digitale Abbildung lassen sich die Hardware Komponenten steuern und deren Daten erfassen. Das CPS stellt dazu in der Infrastruktur eine Kommunikationsmöglichkeit bereit.

Referenz:

Drath, R.: Industrie 4.0 – eine Einführung. In: open automation (2014), Nr. 3, S. 16-21. http://www.openautomation.de/detailseite/industrie-40-eine-einfuehrung.html. – Eingesehen am 26.06.2017.

Jasperneite, J.: Was hinter Begriffen wie Industrie 4.0 steckt. In: Computer & Automation (2012). http://www.computer-automation.de/steuerungsebene/steuern-regeln/artikel/93559/0/. – Eingesehen am 29.06.2017.

2.2.4 DDS

Definition:

Das Data Distribution Service (DDS) ist ein von der Object Management Group spezifizierter Standard, der ein datenzentriertes publish/subscribe Modell für die Kommunikation und Integration von verteilten Anwendungen verwendet. Das Ziel von DDS ist es, "eine effiziente und robuste Auslieferung der richtigen Informationen an die richtige Stelle zur richtigen Zeit" zu ermöglichen.

Referenz:

https://de.wikipedia.org/wiki/Data_Distribution_Service

http://www.omg.org/omg-dds-portal/

2.2.5 Das Ding / The Thing

Definition:

Ein Ding ist eine Entität, das in der Informationswelt verwaltet wird. Wenn es Services/Dienst anbietet, die über Schnittstellen benutzt werden können ist es Teil des IoT.

2.2.6 Echtzeit / real time

Definition:

„Unter Echtzeit versteht man den Betrieb eines Rechensystems, bei dem Programme zur Verarbeitung anfallender Daten ständig betriebsbereit sind, derart, dass die Verarbeitungsergebnisse innerhalb einer vorgegebenen Zeitspanne verfügbar sind. Die Daten können je nach Anwendungsfall nach einer zeitlich zufälligen Verteilung oder zu vorherbestimmten Zeitpunkten anfallen.“[1]

Durch die Hardware und Software muss sichergestellt werden, dass keine Verzögerungen auftreten, welche die Einhaltung dieser Bedingung verhindern könnten. Die Verarbeitung der Daten muss dabei nicht besonders schnell erfolgen, sie muss nur garantiert schnell genug für die jeweilige Anwendung erfolgen.

Der Duden bietet für Echtzeit zwei Beschreibungen an, einerseits als eine „vorgegebene Zeit, die bestimmte Prozesse einer elektronischen Rechenanlage in der Realität verbrauchen dürfen“, sowie als „simultan zur Realität ablaufende Zeit“. Für Echtzeitbetrieb in der EDV gibt der Duden folgende Bedeutung an: „Arbeitsweise einer elektronischen Rechenanlage, bei der das Programm oder die Datenverarbeitung (nahezu) simultan mit den entsprechenden Prozessen in der Realität abläuft“.[2]

Referenz:

Die Definition der inzwischen durch DIN ISO/IEC 2382 abgelösten Norm DIN 44300 (Informationsverarbeitung), Teil 9 (Verarbeitungsabläufe)

2.2.7 Event

Definition:

Auslöser (engl. trigger) bezeichnet im allgemeinen Sprachgebrauch ein Ereignis, das ein anderes Ereignis oder eine Ereigniskette oder mehrere Ereignisse gleichzeitig in Gang setzt.

Referenz:

https://de.wikipedia.org/wiki/Ausl%C3%B6ser

2.2.8 Fertigungsplan

Definition:

Ein Fertigungsplan beschreibt vollständig alle Funktionen in den Dimensionen Produkt, Prozess und Ressourcen, die zur Fertigung eines Produktionsauftrages notwendig sind.

Funktionen sind Klassen.

Referenz:

Ein Beispiel ist der Fertigungsplan, der den Einbau der Heckleuchten im Bandabschnitt 3 am Takt 70 beschreibt.

2.2.9 Fuzz Testing

Definition:

Testtechnik, die mit Hilfe automatisch generierter und an ein Zielsystem versendeter anomaler ungültiger Nachrichtenfolgen, gebrochener Datenstrukturen oder ungültiger Daten Eingaben findet, die Störungen oder eine Verschlechterung von Dienstleistungen verursacht.

Referenz:

http://www.etsi.org/deliver/etsi_tr/101500_101599/101583/01.01.01_60/tr_101583v010101p.pdf

2.2.10 Hardware-Komponente

Definition:

Eine Komponente ist eine Hard-oder Software-Einheit über deren Einsatz/Nutzung dediziert entschieden werden kann; d.h. aus Betriebssicht an- und abgeschaltet werden kann.

2.2.11 Harsche Umgebung

Definition:

„Neben den Software- und Vernetzungsaspekten einer IoT-Lösung ist zudem oftmals ihre Robustheit und Verlässlichkeit in harschen und unsicheren Umgebungen zu prüfen, beispielsweise dann, wenn eine IoT-Lösung im Außenraum, wie z. B. an Straßenlaternen oder Verkehrssignalanlagen, genutzt wird. Auch die Absicherung von IoT-Lösungen in dynamischen Konfigurationen, die sich beispielsweise aus dem Ausfall oder der Hinzunahme von IoT-Geräten ergeben, stellt eine Herausforderung dar. Letztendlich führt das dazu, dass IoT-Lösungen nicht mehr allein während der Entwicklung und im Labor getestet und abgesichert werden können. Es erfordert eine Verlängerung der Qualitätssicherung in die Laufzeitumgebung hinein – mit Laufzeittests (sogenannten Online-Tests), die über ein traditionelles Monitoring hinausgehen und auch als Safe Guards funktionieren können. Dabei nutzen die Komponenten einer IoT-Lösung Wissen (in Komponenten-internen Modellen repräsentiert) über ihre Konfiguration und Umgebung zur Herleitung oder Anpassung der Laufzeittests. “http://www.informatik-aktuell.de/betrieb/netzwerke/iot-testing-wirkungsvoll-und-konsequent.html"

robuste, leistungsfähige IT in harschen Umgebungen. Kennzeichen für diese Baureihen sind unter anderem ein Full Rugged Design mit hoher Toleranz gegen mechanische und thermische Belastungen. Diese werden durch unabhängige Prüfverfahren wie dem vom US-Militär angewendeten MIL-STD810 oder InternationalProtection Level IP zertifiziert. IndustrieEmbedded Computer sind für einen langfristigen Einsatz ausgelegt.

2.2.12 IT-Plattform

Definition:

Plattformen sind die Basis zur Entwicklung und zum Betrieb von Services und Applikationen.

Sie bestehen typischerweise aus den Layern Hardware, Betriebssystem, Netzwerk/Kommunikation, Datenhaltung, Applikationsservern und Präsentationskomponenten.

Referenz:

IPK: https://de.wikipedia.org/wiki/Plattform_(Computer)

2.2.13 Industrie 4.0

Definition:

Laut Arbeitskreis Industrie 4.0 versteht man darunter »eine Vernetzung von autonomen, sich situativ selbst steuernden, sich selbst konfigurierenden, wissensbasierten, sensorgestützten und räumlich verteilten Produktionsressourcen (Produktionsmaschinen, Roboter, Förder- und Lagersysteme, Betriebsmittel) inklusive deren Planungs- und Steuerungssysteme«.

Referenz:

http://www.ipk.fraunhofer.de/top-themen/

http://www.ipk.fraunhofer.de/fileadmin/user_upload/IPK/publikationen/futur/Futur_1_2015/Futur_1_2015.pdf

http://www.ipk.fraunhofer.de/industrie-40/

2.2.14 Informationsprozess

Definition:

Ein Informationsprozess beschreibt die Bereitstellung, Erfassung und Transformation von Informationen.

Informationsprozesse können Geschäftsprozesse sein, wie. z.B. die Erstellung und Pflege der Produktstückliste oder sie unterstützen Fertigungsprozesse wie z.B. die Endmontage von Fahrzeugen. Informationsprozesse vernetzen unterschiedliche Unternehmensfunktionen und haben das Ziel, die relevanten Informationen, nutzregerecht, zur richtigen Zeit, am richtigen Ort, sicher zur Verfügung zu stellen.

2.2.15 Interoperability

Definition:

Interoperabilität definiert die Fähigkeit von zwei oder mehr Systemen oder deren Komponenten, Informationen auszutauschen und die ausgetauschten Informationen semantisch korrekt zu verarbeiten.

Referenz:

https://www.ieee.org/education_careers/education/standards/standards_glossary.html

http://www.dfi-ev.de/home/

http://interop-vlab.eu/

2.2.16 IoT

Definition:

Das Internet der Dinge bezeichnet die Verknüpfung eindeutig identifizierbarer physischer Objekte (things) mit einer virtuellen Repräsentation in einer Internet-ähnlichen Struktur. Es besteht nicht mehr nur aus menschlichen Teilnehmern, sondern auch aus Dingen. Der Begriff geht zurück auf Kevin Ashton, der erstmals 1999 „Internet of Things“ verwendet hat.

Referenz:

https://aws.amazon.com/de/iot/?sc_channel=PS&sc_campaign=acquisition_DE&sc_publisher=google&sc_medium=english_iot_nb&sc_content=iot_p&sc_detail=iot&sc_category=iot&sc_segment=153193053061&sc_matchtype=p&sc_country=DE&s_kwcid=AL!4422!3!153193053061!p!!g!!iot&ef_id=U8UzJwAABYjdUWzr:20161230073825:s

2.2.17 IoT-Architektur

Definition:

Eine IoT-Architektur ist eine konkrete Umsetzung und Anpassung einer (gewählten) IoT-Referenzarchitektur für einen konkreten Anwendungsfall.

2.2.18 IoT-Gateway

Definition:

Ein IoT-Gateway ist eine Komponente die zwischen IoT-Geräten und der Cloud platziert wird. Das Gateway ist neben der Übersetzung von Protokollen und Verbindung zur Cloud auch für die Aufbereitung, Speicherung, Absicherung und Filterung der Daten zuständig.

2.2.19 IoT-Geräte

Definition:

Ein IoT-Gerät ist "the Thing" in IoT. Dieses besteht aus einer IoT-Komponente (Software) und der Hardware-Plattform auf der diese Komponente ausgeführt wird. Das Gerät ist in der Lage sich mit einem Netzwerk zu verbinden und über dieses Daten auszutauschen. Für die Verbindung zur physischen Welt sind IoT-Geräte mit Aktuatoren und/oder Sensoren bestückt.

Referenz:

Techtarget Definition IoT-Device

2.2.20 IoT-Komponente

Definition:

IoT-Komponenten stellen Funktionen als Services/Dienste zur Nutzung im Netzwerk und oder in der Cloud zur Verfügung. IoT-Komponenten werden auf Plattformen, die aus Hardware-Komponente bestehen implementiert.

2.2.21 IoT-Lösungen

Definition:

Eine IoT-Lösung ist ein spezialisiertes System für einen bestimmten Anwendungsfall und setzt sich in der Regel aus Einzelkomponenten wie z.B. IoT-Geräten, IoT-Gateways und Cloud Komponenten zusammen. Eine IoT-Lösung wird nach einer IoT-Architektur erstellt.

2.2.22 IoT-Referenzarchitektur

Definition:

Eine IoT-Referenzarchitektur stellt eine Vorlage/Schablone/Modellmuster für die Klasse der IoT spezifischen Architekturen zur Verfügung. Dieses Modellmuster soll dabei helfen eine IoT-Architektur für ein spezifisches/konkretes System zu entwerfen.

Referenz:

The Internet of Things - Architecture

WSO2 Reference Architecture for IoT

IEEE IoT Architecture

InfoQ: A Reference Architecture for IoT

Wiki: Reference Architecture

Wiki Referenzarchitektur

2.2.23 Konformität / Conformity

Definition:

Die Konformitätsbewertung zeigt, dass spezifizierte Anforderungen an ein Produkt, Prozess, System oder Person erfüllt sind. Dies kann jede Tätigkeit einschließen, die unmittelbar oder mittelbar feststellt, dass relevante Anforderungen erfüllt sind.

Referenz:

Übersetzte Definition aus ISO/IEC 17000:2004(en)

2.2.24 MQTT

Definition:

MQ Telemetry Transport (MQTT) ist ein Übertragungsprotokoll, das seit 2013 von OASIS für den Einsatz in M2M und IoT standardisiert wird. Das Protokoll setzt konsequent auf das publish/subscribe Übertragungsmodell und ist dadurch außerordentlich flexibel einsetzbar.

Referenz:

mqtt.org

OASIS MQTT v3.1.1: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html

2.2.25 Neutrale Verrichtungsklassen

Definition:

Beschreibt Standard Fachmodule (Transportieren, Handhaben, Identifizieren, Fertigen, …) in der Industrie.

2.2.26 OPC-UA

Definition:

OPC UA ist eine plattformunabhängige und serviceorientierte Architektur, speziell entworfen für den Einsatz in der industriellen Automatisierung. OPC UA integriert sämtliche Funktionalitäten aus den klassischen OPC Spezifikationen in einem einzigen und flexiblen Framework.

Referenz:

About OPC-UA: https://opcfoundation.org/about/opc-technologies/opc-ua/

OPC-UA Specification: https://opcfoundation.org/developer-tools/specifications-unified-architecture

2.2.27 RAMI4.0

Definition:

Das Akronym steht für "Referenzarchitektur für Industrie 4.0".

Das Referenzarchitekturmodell Industrie 4.0, kurz RAMI 4.0, besteht aus einem dreidimensionalen Koordinatensystem, das die wesentlichen Aspekte von Industrie 4.0 beinhaltet. Komplexe Zusammenhänge können so in kleinere, überschaubare Pakete aufgegliedert werden.

Referenz:

https://www.zvei.org/themen/industrie-40/das-referenzarchitekturmodell-rami-40-und-die-industrie-40-komponente/

http://industrie40.vdma.org/documents/4214230/15346103/1486621809874_04%20HANKEL%20Industrie%204.0%20Semantik%20und%20Produktkriterien%20in%20der%20Antriebs-%20und%20Fluidtechnik.pdf/b557d400-505d-4776-9fc5-e4430479b49a

2.2.28 Robustness

Definition:

Robustheit, auch als "Fehlertoleranz" bezeichnet, beschreibt die Fähigkeit eines Elements, eine erforderliche Funktion auch unter Vorlage bestimmter vorgegebener Teilfehler auszuführen.

Dies gilt sowohl für Hardware als auch Software Fehler.

Referenz:

Übersetzte Definition aus 394-33-13 in IEC 60050-394:2007

2.2.29 Safety

Definition:

Sicherheit im Sinne von "Safety" ist der Zustand "sicher" (von Französisch sauf), die Bedingung, um vor Schaden oder anderen nicht wünschenswerten Ergebnissen (**welche die Gesundheit oder das Leben von Personen bedrohen**) geschützt zu werden. Sicherheit kann sich auch auf die Bekämpfung von anerkannten Gefahren (für Leib und Leben) beziehen, um ein annehmbares Risiko zu erreichen.

Referenz:

Erweiterte Übersetzung der Safety-Definition aus Wikipedia, s. https://en.wikipedia.org/wiki/Safety

2.2.30 Security

Definition:

Sicherheit im Sinne von "security" ist der Grad der Widerstandsfähigkeit oder des **Schutzes vor Schaden**. Es **gilt für alle anfälligen und / oder wertvollen Vermögenswerte**, wie einer Person, Wohnung, Gemeinschaft, einem Gegenstand, einer Nation oder Organisation.

Referenz:

Übersetzung der Security-Definition aus Wikipedia, s. https://en.wikipedia.org/wiki/Security

2.2.31 Service

Definition:

Ein Service/Dienst ist ein abgegrenzter Funktionsumfang, der von einer Entität oder Organisation über Schnittstellen angeboten wird.

Referenz:

http://i40.iosb.fraunhofer.de/FA7.21%20Begriffe%20-%20IKT#dienst-service

2.2.32 Services zur Steuerung der Produktionsressourcen

Definition:

Üblicherweise kann die Funktionen durch einen „Adapter“ umgesetzt.

2.2.33 Shopfloor IT

Definition:

Shopfloor IT umfasst alle Informationsprozesse und IT Lösungen, die mittelbare Tätigkeiten am Produkt steuern, absichern und erfassen.

Die Shopfloor IT unterstützt somit die unmittelbare Ausführung auf Werker und Anlagenebene.

2.2.34 Software Produktlinie

Definition:

Eine Software-Produktlinie beschreibt eine Menge von Softwareprodukten, die auf einer gemeinsamen Grundlage - einer Plattform - aufgebaut werden. Durch Konfigurationen der Plattform und Erweiterungen durch zusätzliche Softwarekomponenten entstehen individuelle Softwareprodukte aus einer gemeinsamen Produktlinie.

Referenz:

Carnegie Mellon Software Engineering Institute

2.2.35 Standard Informationsgrundfunktionen

Definition:

IT-Module (Datenverarbeitung), werden benutzt um Daten zu verarbeiten.

2.2.36 Standard Interaktionsfunktionen

Definition:

IT-Module (Kommunikation), werden benutzt um Ein-/Ausgangssignale zu erzeugen und auszuwerten.

2.2.37 System (generisch)

Definition:

Ein System ist eine "relativ stabile, geordnete Gesamtheit von Elementen und Beziehungen, die durch die Existenz bestimmter Gesetze, d.h. allgemein-notwendiger und wesentlicher Zusammenhänge, charakterisiert ist." (Hörz/Wessel 1983, S. 45).

Gesamtheit von Elementen, die aufeinander bezogen und als nach außen hin abgegrenzte Struktur organisiert sind.

Referenz:

http://www.thur.de/philo/system.htm

http://www.complexity-research.com/KomplexiSystem.htm

2.2.38 System under Test

Definition:

Die Komponente oder das System, welches getestet wird. (Testobjekt)

Referenz:

http://glossar.german-testing-board.info/#system_under_test

2.2.39 Test Case

Definition:

Ein Satz von Eingabewerten, Ausführungsvoraussetzungen, erwarteten Ergebnissen und Ausführungsaufgaben, die für ein bestimmtes Ziel oder eine Testbedingung entwickelt wurden, um einen bestimmten Programmpfad auszuüben oder die Einhaltung einer bestimmten Anforderung zu überprüfen..

2.2.40 Test purpose

Definition:

Eine Prosa-Beschreibung eines klar definierten Ziels des Testens, das sich auf eine einzige Konformitätsanforderung oder eine Reihe von verwandten Konformitätsanforderungen konzentriert, wie in der entsprechenden Spezifikation spezifiziert (z. B. die Überprüfung eines spezifischen Wertes eines spezifischen Parameters).

Referenz:

https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.290-198811-S!!PDF-E&type=items

2.2.41 TestLab

Definition:

Ein TestLab / Testlabor ist eine Umgebung, in der Experimente kontrolliert, messbar, sicher und reproduzierbar ausgeführt werden können.

2.2.42 Testware

Definition:

Unter Testmittel oder Testware (als Kunstwort aus Testing und Software) versteht man Dokumente und (Software-) Werkzeuge, die bei einem Software-Testprozess verwendet bzw. generiert werden.
Testware is a sub-set of software with a special purpose, that is, for software testing, especially for software testing automation.

Referenz:

https://en.wikipedia.org/wiki/Testware

2.2.43 Use case / Anwendungsfall

Definition:

Ein Anwendungsfall (engl. use case) bündelt alle möglichen Szenarien, die eintreten können, wenn ein Akteur versucht, mit Hilfe des betrachteten Systems ein bestimmtes fachliches Ziel (engl. business goal) zu erreichen. Er beschreibt, was inhaltlich beim Versuch der Zielerreichung passieren kann und abstrahiert von konkreten technischen Lösungen. Das Ergebnis des Anwendungsfalls kann ein Erfolg oder Fehlschlag/Abbruch sein.

Referenz:

https://de.wikipedia.org/wiki/Anwendungsfall

2.2.44 Kritische Infrastruktur

Definition:

Kritische Infrastrukturen sind Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Neben den Sektoren Energie und Gesundheit, zählen z.B. auch Informationstechnik und Telekommunikation sowie die Wasserversorgung zu den Bereichen, die überlebensnotwendige Infrastrukturen bereitstellen.

Referenz:

Gesetzgebung in Deutschland

http://www.bmi.bund.de/DE/Themen/Bevoelkerungsschutz/Schutz-Kritischer-Infrastrukturen/schutz-kritischer-infrastrukturen_node.html

https://www.bundesregierung.de/Content/DE/Artikel/2014/12/2014-12-17-kabinett-it-sicherheitsgesetz.html