Reader for VEDLIoT's WP2.1 Architecture Workshop

Hans-Martin Heyn

February 17, 2021

Chapter 1

A list of concerns for IoT systems

Based on the IEEE 2413 Standard for an Architectural Framework for the Internet of Things (IoT), the following presents a list of stakeholder concerns which have been identified in multiple IoT domains:

Concern	Description	Source
Actuation	Concerns related to the ability of the cyber-physical system (CPS) to effect change in the physical world.	
Adaptability	Concerns related to the ability of the CPS to achieve an intended purpose in the face of changing external conditions such as the need to upgrade or otherwise reconfigure a CPS to meet new conditions, needs, or objectives.	
Assurance	The level of confidence that a CPS is free from vulnerabilities, either intentionally designed into it or accidentally inserted during its lifecycle, and that the CPS functions in the intended manner.	
Autonomy	Concerns related to optimal functionality under independent operating conditions in a changing environment.	
Behavioral	Concerns related to interdependence among behavioral domains. Concerns related to the ability to successfully operate a CPS in multiple application areas.	
Collaboration	Concerns related to formation of two or more systems that form an ecosystem that guarantees value delivery.	
Communication	Concerns related to the exchange of information internal to the CPS and between the CPS and other entities.	

Concern	Description	Source
Complexity	Concerns related to our understanding of the behavior of CPS due to the richness and heterogeneity of interactions among its components, such as existence of legacy components and the variety of interfaces.	
Conceptual	Concerns related to requirements engineering and concept engineering (including architecture development).	
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes	
Constructivity	Concerns related to the ability to combine CPS modular components (hardware, software, and data) to satisfy user requirements.	
Controllability	Ability of a CPS to control a property of a physical thing. There are many challenges to implementing control systems with CPS including the non-determinism of cyber systems, the uncertainty of location, time, and observations or actions, their reliability and security, and complexity. Concerns related to the ability to modify a CPS or its function, if necessary.	
Cost	Concerns related to the direct and indirect investment or monetary flow or other resources required by the CPS throughout its lifecycle.	
Data semantics	Concerns related to the agreed and shared meaning(s) of data held within, generated by, and transiting a system.	
Data velocity	Concerns related to the speed with which data operations are executed.	
Data volume	Concerns related to the volume or quantity associated with a CPS's operation.	
Deployability	Concerns related to the ease and reliability with which a CPS can be brought into productive use.	
Discoverability	Concerns related to the ease and reliability with which a CPS component can be observed and understood (for purposes of leveraging the component's functionality) by an entity (human, machines). Concerns related to the ease and reliability with which a CPS component's functions can be ascertained (for purposes of leveraging that functionality) by an entity (human, machines).	
Disposability	Concerns related to the impacts that may occur when the CPS is taken physically out of service.	

Concern	Description	Source
Engineerability	Concerns related to the ease and reliability with which a CPS design concept can successfully be realized via a structured engineering process.	
Enterprise	Concerns related to the economic aspects of CPS throughout their lifecycle.	
Environment	Concerns related to the impacts of the engineering and operation of a CPS on the physical world.	
Evolvability	Concerns related to the system's ability to evolve and to be functional with newer technology (backward compatibility).	
Functionality	Concerns related to the function that a CPS provides.	
Human factors	Concern about the characteristics of CPS with respect to how they are used by humans.	
Identity	Concerns related to the ability to accurately recognize entities (people, machines, and data) when interacting with or being leveraged by a CPS.	
Integrity	Property of accuracy and completeness.	
Logical time	Concerns related to the order in which things happen (causal order relation) or event driven.	
Maintainability	Concerns related to the ease and reliability with which the CPS can be kept in working order.	
Manageability	Concerns related to the management of CPS function. For example, managing timing in a complex CPS or SoS is a new issue with CPS that did not exist before.	
Measurability	Concerns related to the ability to measure the characteristics of the CPS.	
Monitorability	Concerns related to the ease and reliability with which authorized entities can gain and maintain awareness of the state of a CPS and its operations. Includes logging and audit functionality.	

Concern	Description	Source
Networkability	Concerns related to the ease and reliability with which a CPS can be incorporated within a (new or existing) network of other systems.	
Operability	Concerns related to the operation of the CPS when deployed.	
Operations on data	Concerns related to the ability to create/read/update/delete system data and how the integrity of CPS data and behaviors may be affected.	
Optimization	Concerns related to the ability of systems or resources to perform optimally.	
Performance	Concerns related to the ability of a CPS to meet required operational targets.	
Physical	Concerns about purely physical properties of CPS including seals, locks, safety, and EMI.	
Physical context	Concerns relating to the need to understand a specific observation or a desired action relative to its physical position (and uncertainty). While this information is often implied and not explicit in traditional physical systems, the distributed, mobile nature of CPS makes this a critical concern.	
Policy	Concerns related to the impacts of treaties, statutes, and doctrines on a CPS throughout its lifecycle.	
Privacy	Concerns related to the ability of the CPS to prevent entities (people, machines) from gaining access to data stored in, created by, or transiting a CPS or its components such that individuals or groups cannot seclude themselves or information about themselves from others. Privacy is a condition that results from the establishment and maintenance of a collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information within or among systems or through the manipulation of physical environments.	
Procureability	Concerns related to the ease and reliability with which a CPS can be obtained.	
Producibility	Concerns related to the ease and reliability with which a CPS design can be successfully manufactured.	

Concern	Description	Source
Quality	Concerns related to the ease and reliability of assessing whether a CPS meets stakeholder (especially customer) expectations.	
Regulatory	Concerns related to regulatory requirements and certifications.	
Relationship btw. data	Concerns related to how and why sets of data shall, may, or may not be associated with each other and the value or harm that can be derived from those associations.	
Relevance	Concerns related to interpretation of fit based on situational context and significance.	
Reliability	Concerns related to the ability of the CPS to deliver stable and predictable performance in expected conditions.	
Resilience	Concerns related to the ability of the CPS to withstand instability, unexpected conditions, and gracefully return to predictable, but possibly degraded, performance.	
Responsibility	Concerns related to the ability to identify the entity or entities authorized to control the operation of a CPS.	
Safety	Concerns related to the ability of the CPS to help ensure the absence of catastrophic consequences on the life, health, property, or data of CPS stakeholders and the physical environment.	
Security	Concerns related to the ability of the CPS to help ensure that all of its processes, mechanisms (both physical and cyber), and services are afforded internal or external protection from unintended and unauthorized access, change, damage, destruction, or use. Confidentiality: Preserving authorized restrictions on access and disclosure. Integrity: Guarding against improper modification or destruction of a system, and includes ensuring non-repudiation and authenticity. Availability: Ensuring timely and reliable access to and use of a system.	
Sensing	Concerns related to the ability of a CPS to develop the situational awareness required to perform its function.	

Concern	Description	Source
Standardization	Concerns related to the availability and applicability of standards and the need for standards. Standards can help to achieve compatibility, safety, security, repeatability, and quality. Standards can also facilitate commoditization of technologies and processes.	
States	Concerns related to the states of a CPS. For example, the functional state of a CPS is frequently used to allow for variation in the CPS response to the same set of inputs. Variation in response based on state is sometimes referred to as functional modes.	
Synchronization	Concerns for synchronization are that all associated nodes have timing signals traceable to the same time scale with accuracies as required. There are three kinds of synchronization that might be required: time, phase, and frequency synchronization, although frequency synchronization is also called syntonization.	
Time awareness	Concerns that allow time correctness by design. The presence or absence of time explicitly in the models used to describe, analyze, and design CPS and in the actual operation of the components. This is a lifecycle concern as well as a concern for the ability to build devices without the need for extensive calibration of the timing properties.	

Concern	Description	Source
Time to market	Concerns related to the time period required to bring a CPS from need realization through deployment.	
Time interval and latency	Specifying requirements for timing generally involves requirements for time intervals between pairs of events. A time interval is the duration between two instants read on the same time scale. CPS timing requirements are generally expressed as constraints on the time intervals (TI) between pairs of system significant events. These can be categorized in terms of bounded TIs or latency, deterministic TIs, and accurate TIs.	
Uncertainty	Managing the effects of uncertainties is a fundamental challenge in CPS. Sources of uncertainty in CPS can be grouped into statistical (aleatoric) uncertainty, lack of knowledge (epistemic) uncertainty, or systematic uncertainty. In CPS, statistical uncertainty is caused by randomness of accuracy of sensing and actuation, often caused by uncertainty of manufacturing processes. Systematic uncertainty is caused by incomplete knowledge either due to limits of acquired knowledge or due to simplification in modeling. Typical manifestations of epistemic uncertainty are limited validity of models of physical processes or limits of computability of properties of mathematical models.	
Usability	Concerns related to the ability of a CPS to be used to achieve its functional objectives effectively, efficiently, and to the satisfaction of users (see ISO 9241-210). The combination of physical and cyber into complex systems creates challenges in meeting usability goals. Complexity is a major issue. The diversity of interfaces creates a significant learning curve for human interaction.	
Utility	Concerns related to the ability of a CPS to provide benefit or satisfaction through its operation. Utility reflects a business concern, especially when considered as the numerator when computing value, which equals utility divided by costs.	

Chapter 2

A list of capabilities of "a thing" in IoT

An IoT component, or *thing* provides a (partial) set of the following capabilities:

Actuating capability: Provides the ability to make a change in the physical world, based on a digital input to the component. Errors may be introduced in the digital logic, the digital-to-analog converter, the analog electrical circuit, and the actuator transducer. There is a time delay between the input data arriving at the component and the change being made to the environment. Examples of actuating capabilities include heating coils, electric shock delivery, electronic door locks.

Application interface capability: Provides the ability for other IoT components (components, systems, etc.) to communicate with a given IoT component through an IoT component application. A widely-used type of application interface is an application programming interface (API).

Data storing capability: Provides the ability to store and retrieve data and information over time. Data persist for a finite period of time. There is a time delay between the input and output. Some examples of data-storing capabilities include databases, block storage, and data brokers (such as a message queue telemetry transport [MQTT] broker).

Data-transferring capability: Provides the ability to transmit data from one physical or logical location to another. The data-transferring capability provides the ability to "black box" a communication network and provide information about the network without having to understand the specific network topology. As the interactions of an IoT system with the physical world require the data-transferring network to meet latency, reliability, and security requirements, it is useful to be able to describe the network characteristics in this manner, so the capability is explicitly called out by the IoT general model. Some examples of specific data-transferring

capabilities include data networks based on Ethernet, IEEE 802.11™, and LTE.

Data-processing capability: Provides the ability to transform data based on a defined algorithm. There is a time delay between the input and output that should be accounted for. The transformation may be very simple, with a single input variable and a single output, or it may be complex with multiple inputs and outputs. Control algorithms are an important type of processing that take the output of sensor(s) andactuator(s) or pre-processor(s) and provide an output that can be fed into an actuator or post-processor. These control algorithms often are used within negative feedback loops, but not always. A proportional-integral-derivative (PID) control algorithm is an example of such a control algorithm. Some examples of processing include data aggregation, data analytics, and predictive analysis.

Human UI capability: Provides the ability for the component to exchange information directly with people. Not all IoT components will have a human UI capability (i.e., a processor component may only provide data through the network interface, while a cell phone has several human interface capabilities in the form of the touchscreen, audio, and camera. Examples of human UI capabilities include displays, touch screens, audio speakers, and microphones.

Latent capability: Capabilities that the IoT component could potentially provide, but are not currently enabled for access externally from the IoT component. For example, a component may have a USB port, but nothing is plugged into that port. In that state, the USB port is considered a latent capability. It has the potential to be used at any time, and if someone attaches something to it, that could enable any of the other capabilities. For example, if someone plugs a IEEE 802.11 adapter into the USB port, the IoT component would then have an additional network interface capability.

Network interface capability: Provides the ability to interface with a communication network. Every IoT component shall have at least one network interface capability and may have more than one. Some examples of network interface capability include: Ethernet adapter interface capability (includes IEEE 802.1™ and IEEE 802.3™, but not the frame interpretation), LTE radio interface capability, and IEEE 802.15™ radio interface capability.

Sensing capability: Provides an observation of a property of the physical entity of interest in the form of digital data. Information from sensor observations may be provided to other IoT components through the component's network interface for processing and storage. Sensing is "read only"; any change to the physical state is a side effect. Uncertainties in

the observation of the property may be introduced by the physical environment between the physical system and the sensor transducer, in the sensor transducer itself, in the analog electrical circuit, in the analog-to-digital (A/D) converter, and in the digital logic of the sensor. There is a time delay between the sensing function and the data becoming available at the component output. Examples include temperature sensing, spatial sensing, optical sensing, and audio sensing.

Supporting capability: Provide additional functionality that supports the functioning of the IoT component or IoT system and does not directly affect the process data. Note that some IoT components may only provide a supporting capability, such as orchestration, and not offer any transducer or data capabilities. Examples of supporting capabilities include time synchronization, data encryption, authentication, orchestration, and remote component management.