EPoSS SRA: Relevant Parts for Generic IoT Infrastructure and the IoT LSPs

Cees J.M. Lanting (CSEM)

Co-Chair of the

EPoSS Working Group Smart Communications & IoT

EPoSS Working Group Smart Communications & IoT

Recently renamed to reflect importance of EPoSS activities on IoT

Co-Chair: Cees J.M. Lanting (CSEM)

Co-Chair: Antonio Lionetto (STMicroelectronics

EPoSS SRA update: Disclaimer

The EPoSS SRA update is Work in progress, the IoT section is new

Today's presentation is not more than input into the process:

- editor of the EPoSS SRA chapter on IoT, the open development and review process has only just started
- presentation somewhat coloured by personal input and views

EPoSS SRA update: scope

EPoSS is about Smart System Integration, focusing on the externally visible behaviour of systems, i.e. sensing, actuating, communications and functionality, incl. interpretation and control algorithms, and the realisation of these systems.

Much of what is presented is applicable to the concepts of ‘smart systems’ as well as ‘CPS’, where the latter can be seen as a generalisation of the former concept

Some observations: what is IoT

Preferred definition
«The Internet of Things is the combination of sensors, actuators, distributed computer power, wireless communication on the hardware side, and applications and big data/analytics on the software side.»
Source: Morgan Stanley Research (contributed by Luca Petricca of Broentech)

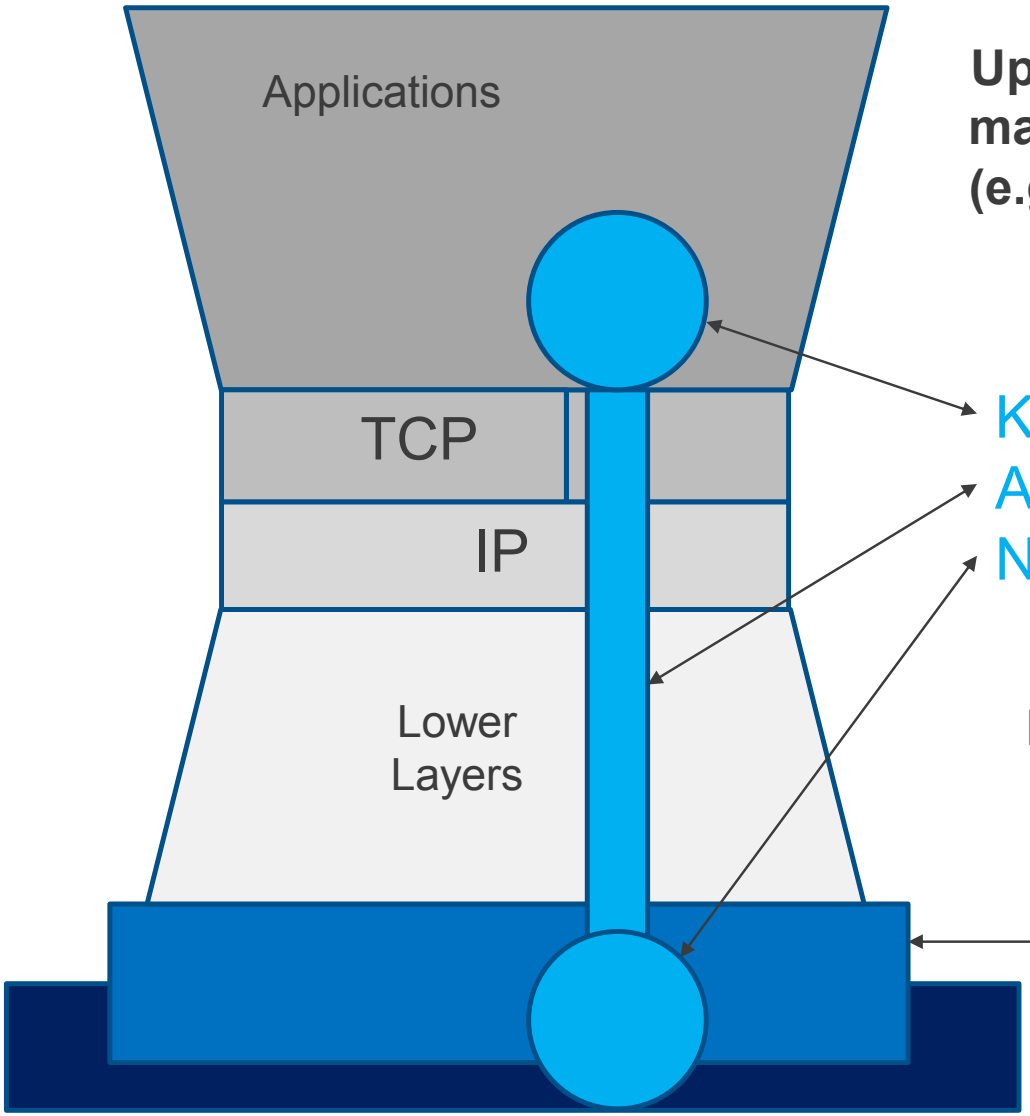
Notes that apply:

- IoT will likely use 'the internet' and IP, but in an appropriate way
- Wireless communications: extra degree of freedom, not required

If everything is seen as IoT, then some structuring would be helpful

In the following we will focus on the IoT hardware and infrastructure

Compacted model, incl. IoT node



Upper protocol stack: may vary significantly (e.g. collapsed layers)

IoT node:
- Knowledge base
- Actual protocol stack
- Node specificity

Lower protocol stack: may be simplified

Sensors and actuators

Metrology

Some observations: On networking aspects 1/2

How many connected devices?

- depending on how and what counted, estimate: 250 Billion @2020

'The internet' is more complex than it is often presented, also for IoT

- there exists a concatenation of internets and intranets
- IP may be overlay network, in particular in the access networks
- many IP enabled devices
  - are in intranets behind firewalls and gateways
  - don't have proper IP addresses, but temporary and multiplexed

IoT communications is more than BT(LP), Wifi and IP

- many IoT applications will require
  - longer distance (LORA, CGS/UMTS, ... , Satellite)
  - higher reliability, better security support
  - even wired connection for different reasons, incl. pragmatic

Some observations: On networking aspects 2/2

IoT devices may behave differently from ‘normal IP enabled devices’, resulting from their functionality and from constraints

- may be irresponsive
- may not be always connected
- may not always have anything to communicate
- may not be implementing a ‘full IP stack’ (e.g. RFID)

Will likely require intermediate nodes and ‘platform support’ as their ‘representatives’.
IoT applications will more likely communicate with the ‘representatives’ (platform, generic applications, etc.)

Some observations: Sensing and actuating 1/2

Sensing and actuation

- Metrology & sensing, control &actuation, sciences by themselves

IoT requires dedicated sensing and actuating infrastructure

- Smart use of other infrastructure may not be a full replacement
  - Example: estimating traffic status from GSM/UMTS positions

Sensors and actuators are not necessarily small

- most measurements are ‘difficult’, only few are ‘simple’
- many measurements are indirect and at a distance, not ‘on-chip’
- Examples of size and distance:
  - environmental measurements
  - energy consumption measurement
  - pitot tube airspeed meter

Some representative examples

Representative air pollution measurement system

Representative thermal energy counters

Some observations: Sensing and actuating 2/2

IoT infrastructure is about systems designed to measure and control, using sophisticated components, techniques, algorithms, software

- specialised IoT systems
- embedded IoT (sub)systems in enhanced systems

Smart System Integration (SSI) is the overall key enabler for IoT infrastructure and hence IoT applications

Smart System Integration (SSI) applied to IoT makes use of all available technologies and techniques, incl. other Key Enabling Technologies (SSI itself is considered a KET)

SSI in IoT characterisation: application environment constraints

	IoT node	IoT node	environment	size limitation	energy option	communic.
outside	stationary		rough	< proportional	autonomous	L(ong) range
		mobile	rough	mobility	autonomous	L range
inside	stationary		protected	< proportional	auton./parasit.	S/M/L range
		mobile	protected	mobility	auton./parasit.	S/M/L range
embedded	stationary		as host	as host	auton./parasit.	S/M/L range
		(mobile)				
on-body	stationary		as body	small	autonomous	S range
		(mobile)				
in-body	stationary		biocompatible	small(est)	autonomous	S range
		mobile	biocompatible	smallest	autonomous	S range

SSI in IoT: Specific priorities 1/2

- Development of sensors
  - variety of sensors and multi-parameter sensors
  - alternative sensing methods
  - simplifications and minimising ‘conditioning’ such as sampling
  - miniaturisation
  - minimising energy consumption
- Actuator development
  - integration of power electronics
  - integration of other actuators, e.g. pneumatic, hydraulic, etc.
- Optimised communications: reach, bandwidth, power and size

SSI in IoT: Specific priorities 2/2

- Optimised energy management
- Design and packaging adapted to the application
- Miniaturisation of systems, optimising integration in packaging of
  - sensors and actuators and control subsystem
  - energy provision and management subsystems
  - communication subsystems, in particular antennae

SSI in IoT: General priorities

- lowest power consumption, as close as possible to minimal energy required
- energy scavenging options
- increasing processing power
- increased reliability
- security at minimal ‘costs’ (a trade-off)
- increased manufacturability: the large expected # of IoT nodes is at least challenging for manufacturing

(we expect a discussion at EPoSS Annual Forum in October 2015)

SSI in IoT: initial view on priorities versus LS-Pilots

	Infrastr.	Pilot 1 Aging ++	Pilot 2 Farm&Food	Pilot 3 Wearable	Pilot 4 Reference	Pilot 5 Autonom.	Pilot 6 Water
Sensors	+	++	+++	+++	++	+++	+ / +++
Actuators	+	(+)	++	+	+	++	++
Energy mgnt	++	+	+++	++	++	+	+++
Communic.	++	+	+++	+	++	++	+++
Design + Pack.	+	++	++	+++	++	++	++
Miniaturisation	+	+	+	++	+	+	+

SSI in IoT: obstacles, general and specific

- Development cost, in particular for small numbers / niche applications
- Manufacturing costs, in particular for small series, and upscaling
- Maintenance costs (diagnostics, identification, retrieval, etc.)
- Product lifecycle, including removal and disposal
- Security measures, in particular against hacking into sensors and actuators
- Data access and ownership management
  - ownership, sharing and transfer
  - access control, privacy
  - security
- Agreement on need for and use of standards, at least per sector

Some food for thought

Will ‘the internet’ as we know it last till 2035?

- need to distinguish between
  - name space(s), address space, services, overlay networks
  - supporting protocol-suite
  - example: POTS, ISDN, GSM, UMTS, e.g. in ‘all IP’

‘Zero delay networking’ an illusion with current networking & trends

- Current trend is better and longer delay
- Especially difficult to achieve with frame based transmission, store and forward, media access with contention, IP, etc.

Measurement without affecting the measured item does not exist

- This is even true for the ecological aspects: longer term, also for IoT ‘leaf’ infrastructure the target needs to be biocompatibility and biodegradability.