CP-SETIS Workshop – The Way Forward

Stockholm, Hipeac CONFERENCE, Jan. 23, 2017

Erwin Schoitsch

UPDATING THE CP-SETIS/ARTEMIS STRATEGIC AGENDA FOR STANDARDIZATION OF CPS: WHAT ARE NEW TOPICS IN THE 2017 STRATEGIC AGENDA FOR STANDARDIZATION?
Background: ARTEMIS/ProSE Strategic Agenda for Standardization

ARTEMIS Goal: Not just another funding scheme – but building together an open sustainable innovation ecosystem!

Not isolated projects but groups of projects building on each other towards a common goal – IOS is one example.

ARTEMIS conceptual model of an innovation eco-system – 7 pillars

ARTEMIS Standardization WG:
- 2007/08 First Strategic Standardization Agenda, to support the ARTEMIS SRA
- Since 2008: Standardization mandatory part in all ARTEMIS proposals, EC concern
- Support Action ProSE: 2008 – 2010
- ProSE Strategic Standardization Agenda paving the way forward!
Background: ARTEMIS/ProSE
Strategic Standardization Agendas

2007/08

ICT 2010, Brussels

Available at https://cp-setis.eu/documents/
Background: 2010 ARTEMIS/ProSE Strategic Standardization Agenda

Version 2010 provides:

- Collection of standards and standardization organizations in all major areas of embedded systems (now: CPS) (Facts)
- How to identify gaps in the existing standards landscape
- The way forward: Process guidelines and criteria for prioritization of standardization activities – to focus on the most promising topics and approaches
- Table of ProSE criteria for standardization candidate assessment
- Four stakeholder groups identified, different approaches recommended

ProSE (FP7 Support Action, contract n° 224213) Promoting Standardization for Embedded Systems
Two tasks to fulfill:

1. **Inclusion of the CP-SETIS Findings concerning IOS (Interoperability Specifications) Framework:** → *presented in the first session*

   Coherent setting of Standards and Specifications for Tool Operability covering the full set of requirements identified, sustainable maintenance process and evolution process, way to identify and implement such structures (ICF Forum as an example), influence on existing established standards with respect to requirements for tools and tool chains (as initiated in IEC 61508 and ISO 26262 for single tools only).

2. **Update of the overview on maintained standards, on new standardization areas, evolving technologies, and of new standardization groups tackling CPS and SoS (Systems of Systems):**

   • What’s new in established standards implemented through the maintenance process? (e.g. security-awareness in functional safety standards, guidance on new software paradigms)

   • New standardization areas because of evolving technologies (e.g. Cloud, IoT, open adaptive systems/SoS)

   • New standardization Groups e.g. IEC TC65 Ad-hoc Groups, ISO and others: discussing Smart Manufacturing, Smart Grids, Robotics (new paradigms like autonomy, perception, decision taking, and V&V of these properties), Human Factors and Functional Safety
BRANDNEW:

AIOTI: Alliance for Internet of Things Innovation
→ now AISBL Association, becoming a cPPP?

• IoT becomes a more and more intriguing issue.
• IoT landscape even more fragmented than Embedded Systems 10 years ago
• The recently founded AIOTI have worked in 11 (now 13) Working Groups on Recommendations for an IoT Research Program for the European Commission, a first IoT Calls were issued for this year.

Sources:

IERC (European Research Cluster on the Internet of Things) 2015, AIOTI Alliance for the Internet of Things Initiative Reports, Nov. 2016
BRANDNEW:

AIOTI: Alliance for Internet of Things Innovation

WG 3 on “Standardization” has issued three documents:

- IoT LSP Standard Framework Concepts (LSP means “Large Scale Pilots”, an EC Large Projects’ Initiative)
- IoT High Level Architecture
- Semantic Interoperability (need for appropriate tools and semantic interoperability addressed)

IERC and AIOTI – close cooperation with international standardization organizations, including ETSI, ITU-T, CEN/ISO, CENELEC/IEC, IETF, IEEE, W3C, OASIS, oneM2M and OGC.

→ in line with proposed ARTEMIS-IA – AIOTI Cooperation, new task for ARTEMIS-IA Standardization WG as mentioned before today; maybe another possibility to apply the IOS – ICF ideas in an fast evolving field
### AIOTI

**Alliance for Internet of Things Innovation**

**Basis**: Current Workinggroups = current topics of interest

WG reports of all WG’s (Except WG 10) completed

<table>
<thead>
<tr>
<th>WG 01</th>
<th>IoT European Research Cluster</th>
<th>Smart Living Environment for Ageing Well</th>
<th>Smart Farming and Food Security</th>
<th>Wearables</th>
<th>Smart Cities</th>
<th>Smart Mobility</th>
<th>Smart Water Management</th>
<th>Smart Manufacturing</th>
<th>Smart Buildings and Architecture</th>
<th>Smart Energy</th>
<th>SME Interests</th>
</tr>
</thead>
<tbody>
<tr>
<td>WG 02</td>
<td>Innovation Ecosystems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WG 03</td>
<td>IoT Standardisation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WG 04</td>
<td>IoT Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Notes

- Funded by the European Union
- Erwin Schoitsch (AIT)
- CP-SETIS WS Stockholm
- HiPEAC Conf. Jan. 23rd, 2017
ISO IoT Standardization Work

- ISO/IEC CD 20924 - Information technology -- Internet of Things (IoT) -- Definition and vocabulary
- ISO/IEC WD 30141 Internet of Things Reference Architecture (IoT RA)
- ISO/IEC FDIS 29341-30-2 Information technology -- UPnP Device Architecture -- Part 30-2: IoT management and control device control protocol -- IoT management and control device
- ISO/IEC FDIS 29341-30-1 Information technology -- UPnP Device Architecture -- Part 30-1: IoT management and control device control protocol -- IoT management and control architecture overview
- ISO/IEC FDIS 29341-30-10: IoT management and control device control protocol -- Data store service
- ISO/IEC FDIS 29341-30-11: IoT management and control device control protocol -- IoT management and control data model service
- ISO/IEC FDIS 29341-30-12: IoT management and control device control protocol -- IoT management and control transport generic service
- ISO/IEC 29161 Information technology -- Data structure -- Unique identification for the Internet of Things
- ISO/IEC AWI 18574 – 18577: Internet of Things (IoT) in the supply chain
IoT – Internet of Things

IoT Communications Standards environment:

- Application/Data Layer
- Application 1
- Application 2
- Application 
- Application #
- ONEM2M/ETSI M2M Service Layer
- HTTP
- CoAP
- SEP 2.0
- Transport Layer
- ZigBee
- TCP
- TCP/UDP
- NWK Layer
- RPL
- IPv6
- 6LoWPAN
- DataLink Layer
- IEEE 802.15.4
- Bluetooth 4.0 Low Energy
- Wi-Fi
- NFC
- PHY Layer
- 3GPP
IoT Internet of Things
Multiple service stacks

- Horizontal, vertical and transversal communication and control
- Example: OGC sensor web for IoT Interoperability (Open Geospatial Consortium)
IoT – Internet of Things

How to bring IoT requirements to communication standards?

→ Pre-standardization Groups: IRTF-ISOC, ITU-T-Focus Group, IEEE-SA Industry Connection Program, ETSI – ISG → No separate AIOTI Standards, utilizing existing organizations/groups → Multi-Standard-type Approach?!

Some results:

• FI-WARE now includes “Generic Enablers” for Future-Internet/IoT (OASIS eXtensible Acess Control Markup Language XACML provided to the IoT domain)

• Cybersecurity, privacy, identification, traceability, anonymization, semantic interoperability, interoperability/coexistence testing, performance characterization and scalability, auto-configuration, discovery, self-configuration, service robustness and resilience → IERC central reference for EC IoT pre-standardization

• M2M Service Layer in IoT (integrated horizontal approach instead of vertical-only approach) (transport and application layer) ETSI-M2M

• Cross-Vertical M2M Layer Standardization (integrate different verticals) ETSI-M2M
“NEW” Topic, promoters try to differentiate/separate:

- Many competing standardization activities, e.g.
  - ISO/IEC JTC1, WG 10, Internet of Things; SWG 5
  - ISO/IEC JTC1, WG 7, Sensor networks
  - ISO, IEC: Many IoT relevant related standards in the communication area
  - IEEE: many IoT related standards and standards projects
  - Particular protocols, e.g. the open AllJoyn protocol, now supported by the AllSeen Alliance (Qualcomm, Cisco, Linux, MicroSoft, …)
  - Open Interconnect Consortium (Intel, Atmel, Dell, Samsung, WindRiver, …)
  - Thread protocol (Google)
  - Particular protocols for e.g. home devices etc.
New Issues: Cloud and IoT

- **BRANDNEW:** Standards for the Cloud

  - The Joint Technical Committee of ISO and IEC, JTC1, Subcommittee 30 (“Distributed Application Platforms and Services”) has started foundational work on Cloud Computing Standards. These standards
    - ISO IEC 17788 – Cloud computing – overview and vocabulary
    - ISO/IEC 17789 - Cloud computing - Reference architecture
  - are recommended and supported by ITU-T, the International Telecommunication Union.
  - In the mean-time, related standards like ISO/IEC 19831:2015 have been published ("Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based protocol").
New Issues: Cloud and IoT

BRANDNEW:

Standards for the Cloud

• Joint Technical Committee of ISO and IEC, JTC1, Subcommittee 30 (“Distributed Application Platforms and Services”): New standardization projects are another window of opportunity for research project partners, particularly when not just file services but more complex digital industrial services should be addressed in future:
  • Service level agreements,
  • Interoperability and portability,
  • Data and their flow across devices and cloud services,
  • Security issues

• Besides ISO/IEC, a number of standards and specifications from IETF, W3C and OASIS are relevant in the area of Cloud and Web Services.
• For common security requirements standardized protocols and specifications can be used, like for example SSL/TLS (RFC 5246), IPsec (RFC 4301), XML Signature and XML Encryption, SAML, XACML and others.
Open Systems Dependability
IEC 62853/Ed1/CD © IEC:2015
There is a standard evolving towards open, adaptive systems!

• Open systems dependability is the ability of a system
  – operated for an extended period of time in a real-world environment to
    accommodate change in its objectives and environment,
  – to ensure that accountability in regard to the system is continually
    achieved, and
  – to provide the expected services to users without interruption. It
    systematizes and puts emphasis on post failure management.

• Is about adaptive systems as well!

• Standard provides four process views to achieve these goals:
  – Change Accommodation process view,
  – Accountability Achievement process view,
  – Failure Response process view and
  – Consensus Building process view.

• This International Standard requires a dependability case assuring these
  process views, and five assurance metacases:
  – Internal Consistency and External Consistency,
  – Validity, Adequacy and Confidence assurance metacases.
SoA Standardization
(Collaborative Automation, Local Clouds)

Service Oriented Architecture: Service Interoperability

- Factory description system
- Deployment system
- Configuration system
- Event handler system
- Historian system
- Meta service registry system
- User registry system
- Quality of Service system

→ Refer to ARROWHEAD, EMC², ...
→ Concerns many Engineering Standards!
SoA Standardization

Service Oriented Architecture based framework for integrating multi-vendor applications

Core Systems and Services

- Authorisation System
- Service Registry
- Orchestration System

Included in the Arrowhead Framework

Application Systems and Services

- Service providing system
- Service consuming system

www.arrowhead.eu
**Clause 7.4.4 in IEC 61508-3**: some general requirements for off-line support tools are:

- shall all be selected as a coherent part of the software development activities,
- shall be selected to be integrated to minimize the possibility of introducing human errors,
- selection and use shall be justified.

Support tools in classes T2 and T3 shall have

- a specification or product manual that defines the behaviour of the tool together with instructions and constraints on its use.
- to be assessed with the aim to determine the level of reliance that shall be placed on the tool, on potential failure mechanisms that may affect the executable software (T3 only).

Examples of how to achieve this:

- perform software HAZOP, restrict tool functionality, check tool output
- use diverse tools for the same purpose.

**Tool Chain issues insufficiently covered by Functional Safety Standards**

(SAFECOMP Paper 2012 by partner KTH)
Qualification requirements of software tools covered by Clause 11 of Part 8.

- General Requirements similar to IEC 61508 (documentation, version handling)
- A certain confidence is required in that these tools shall achieve:
  - the risk of systematic faults in the developed product due to malfunctions of the software tool leading to erroneous outputs is minimized
  - the (SW) development process is adequate with respect to compliance with ISO 26262, if activities or tasks required by ISO 26262 rely on the correct functioning of the tool.

Two metrics for confidence, needs analysis of the tool and its role in the development chain:

1. **TI (Tool Impact):** Can the malfunctioning tool and its corresponding output introduce or fail to detect errors in a safety-related item or element being developed (TI1 if no error/detection failure possible, supported by argument, else TI2)

2. **TD (Tool error Detection):** confidence in preventing or detecting such errors in the output of the tool
   a.) **TD1:** high confidence that malfunction/erroneous output will be prevented or detected
   b.) **TD2** medium confidence
   c.) **TD3** else

Qualification can be done independently from development, but confidence level has to be confirmed.
The CP-SETIS – IOS Approach

What is different, what is applicable?

Findings of CP-SETIS:

- IOS cannot be a single standard, specification or guideline
- IOS is rather a set of standards, guidelines and specifications
- It consists of items of different maturity level
- IOS defines a process of tracking, adoption and enhancement for standardization/specification candidates

The proposed approach:

- Creation of the ICF (Interoperability Coordination Forum) (= stakeholders)
- Finding a suitable Sustainable Hosting Structure

NEW: Can the „Multi-Standard“ Concept be generalized to resolve complex standardization issues where groups of consistent standards would be required?
Safety & Security Standards Framework
(Example by Bertrand Rique)
Multi-concern Issues: How to align all this?

BRANDNEW: IEC TC65 Ad Hoc Groups – Safety, Reliability, Cybersecurity, Smart Manufacturing, Human Factors, …. (Examples)


- IEC TC65 AHG2: “Reliability of Automation Devices and Systems”, looking at the demand of reliability design, test, verification and operational life of (safety related) automation devices and systems as handled by IEC TC65.

- IEC TC65 AHG3: “Smart Manufacturing Framework and System Architecture” (Kick-off April 2016); this group will address the issues of highly interconnected industrial automation systems for smart manufacturing in a multi-concern manner.

- IEC SC65E (Devices and integration in enterprise systems) AHG1 (started 2016) “Smart manufacturing information models”. This subcommittee SC65E looks at enterprise management systems from top level down to devices. Main concern: interoperability of models and data exchanged, how managed by smart items in enterprise context (safety, security and dependability will play an important role)

- IEC SC65A WG 17: Human factors – Functional Safety (IEC TR 62879)
Update of ARTEMIS Strategic Standardization Agenda

What is required from CP-SETIS partners? Input from audience today?

1. Inclusion of the CP-SETIS Findings concerning IOS (Interoperability Specifications) Framework:

   - Input required from “Multi-Standards Approach”:
     1. what is existing and part of the IOS now (“adopted”),
     2. which are the candidates and
     3. which standards are monitored now by CP-SETIS partners and the initial ICF (Interoperability Coordination Forum) (“tracked”) → Input from audience today?

   - Influence on existing established standards with respect to requirements for tools and tool chains (as initiated in IEC 61508 and ISO 26262 for single tools only) (status report, initiatives to transfer some results of IOS/ICF activities, done by AIT now, Input from audience today?)

2. Update of the overview on maintained standards, on new standardization areas, evolving technologies, and of new standardization groups tackling CPS and SoS:

   - At the moment one mainly by AIT in areas of ISO and IEC on Functional Safety and Security Awareness for Safety, key aspects from IoT and Cloud Standards → but maybe limited view!!

   - Needed: Input concerning other domains and standardization groups (e.g. OASIS, OMG, IETF, AutoSar, ProSTEP, … ??? Etc → Input from audience today?)
Time schedule (tentative):

- Consolidation until end of January 2017, inclusion of ARTEMIS Standardization WG
- February 2017: Reviews by partners and ARTEMIS Standardization WG (2 cycles?)
- Final version begin of March 2017, March/April Book preparation
- May 2017: Book distribution
Partners and Associated Partners

Coordinator:

Partners:

Associated Partners:

Additional Associated Partners welcome!
THANK YOU FOR YOUR KIND ATTENTION!