The Intersection of IoT and CPS

Chris Greer
Senior Executive for Cyber-Physical Systems
chris.greer@nist.gov
Credit

• Edward Griffor – Framework, Mathematical models

• Marty Burns – Framework, Pivotal Points of Interoperability

• David Wollman – Framework, Physical and Logical Interactions
Outline

• Definitions

• Illustrative Scenarios

• Mathematical Models

• Framework
CPS: Examples of Current Definitions

Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components. 

US National Science Foundation

Cyber-physical systems integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other.

CPS Virtual Organization

Cyber-physical systems (CPS) are smart systems that include engineered interacting networks of physical and computational components.

CPS Public Working Group (NIST)

In such technical systems, which are often called cyber-physical systems (CPS), real-time computing elements and physical systems interact tightly. …The merging of IoT and CPS into closed-loop, real-time IoT-enabled cyber-physical systems is seen as an important future challenge.

PICASSO Project Opportunity Report
**IoT: Examples of Current Definitions**

An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.

**ISO/IEC JTC1, 2015**

The Internet of Things (IoT) has been defined in Recommendation ITU-T Y.2060 as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

**ITU-TY.400/Y.2060**

IoT refers to any systems of interconnected people, physical objects, and IT platforms, as well as any technology to better build, operate, and manage the physical world via pervasive data collection, smart networking, predictive analytics, and deep optimization.

**IEEE-SA IoT Ecosystem Study 2015**
Relationship Between CPS and IoT: Examples

In most academic and project activities, the difference between “Internet of Things” and “Cyber-Physical Systems (CPS)” is not made clear and it is difficult to find a source that draws a clear-cut distinction … Yet, identified objects in an IoT system can still be networked together so as to control a certain scenario in a coordinated way, in which case an IoT system can be considered to grow to the level of a CPS.

IEEE (2015) Towards a Definition of the Internet of Things

According to the PICASSO definition, the IoT is seen as an enabling technology for CPS or CPSoS (System of Systems) … The merging of IoT and CPS into closed-loop, real-time IoT-enabled cyber-physical systems is seen as an important future challenge.

PICASSO Project Opportunity Report
Outline

• Definitions

• Illustrative Scenarios

• Mathematical Models

• Framework
CPS vs IoT From the Examples: Home Energy Management System

Cyber Security

IN

Networks

Data

Software

Hardware

Compute
- Platforms
- Functions

Physical Interaction

Logical Interaction

Dependency

Sensors

Motion Model

Economic Model

Actuators

IN

OUT

IN

OUT

IoT Views

CPS Views
ABS Schematic

- Automatic Cruise Control (ACC)
- Inertial Measurement Unit (IMU)
- Power Unit (PU)
- Steering Wheel Angle Sensor (SWA)
- Master-cylinder reservoir
- Hydraulic Electronic Control Unit (HECU)
- Disc Brake Speed Sensor (WSS)
- Brake Pedal

Physical connections:
- Direct logical connection
- CAN (logical connection bus)
- Physical element
- Logical element
- Physical & logical system
Outline

• Definitions
• Illustrative Scenarios
• Mathematical Models
• Framework
• **Logical State of a CPS** is a vector of *logical state parameters* \(<L_1, \ldots, L_n>\)

• The Logical State is acted upon by algorithms \(TL_1, \ldots, TL_k\) (each can be viewed as an operator on \(<L_1, \ldots, L_n>\), resulting in \(<L'_1, \ldots, L'_n>\);

• **Physical state of a CPS** is a vector of *physical state parameters* \(<P_1, \ldots, P_m>\);

• a physical state vector is a solution to an algebraic system of differential equations (each equation describing a *waveform* for a choice of free variables)

• The Physical State is acted upon by energy exchange processes, represented by algebraic systems of ODEs, \(T_{e1}, \ldots, T_{ek}\)
Representing CPS: Symmetric Monoidal Categories

• For purposes here systems will be viewed as processes and interactions between them (process algebra in the sense of Milnor for example)

• We distinguish two sorts of interactions between processes:
  o Logical interactions (exchanges of information)
  o Physical interactions (exchanges of energy)

• Math model of physical interactions is algebraic systems of ODEs

• Math model of logical interactions are formalizations of agent-based models such as complex adaptive systems (J. Holland)

• We choose symmetric monoidal categories (SMC) as an example of a model of systems in category theory
Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic.

Examples include a smart grid, a self-driving car, a smart manufacturing plant, an intelligent transportation system, a smart city, and Internet of Things (IoT) instances connecting new devices for new data streams and new applications.

Common notions of IoT have emphasized networked sensors providing data streams to applications.

CPS concepts complete these IoT notions, providing the means for conceptualizing, realizing and assuring all aspects of the composed systems of which sensors and data streams are components.

_The Framework for Cyber-Physical Systems_ was released by the NIST CPSPWG on May 26, 2016.
CPS Mathematical Models

• Connecting logical and physical forms of concerns using interactions between the logical and physical states of a CPS
• Math of these interactions can provide a unified cyber-physical science.
• Sensing and Actuation ‘connect’ properties of the logical and physical elements of the CPS design
Outline

• Definitions

• Illustrative Scenarios

• Mathematical Models

• Framework
Analyzing and Developing CPS: Decomposition

CPS/Function Types

- Business Case
- Use Case ‘feature’
- CPS
- Logical
- Message
- Info
- Physical
- Influence
- Energy

Safety “Properties” of a decomposed Function: AEB

- AEB – vehicle provides automated collision safety function
- AEB – vehicle provides/maintains safe stopping
- AEB – braking function reacts as required
- AEB – messaging function receives distance to obstacles and speed from propulsion function
- AEB – distance and speed info is understood by braking function
- AEB – stopping algorithm provided safe stopping
- AEB – friction function provides appropriate friction

Apply Aspects/Concerns

Generate System Properties
The Framework for Cyber-Physical Systems was released by the NIST CPSPWG on May 26, 2016, see pages.nist.gov/cpspwg
CPS Concern Tree

Aspects

- Functional
- Business
- Human
- Trustworthiness
- Timing
- Data
- Boundaries
- Composition
- Lifecycle

Facets

Conceptualization | Realization | Assurance
A privacy protected message exchange might consist of the set of properties:

## Concern-Driven Analysis of a Standard

### Common Concern:
**Trustworthiness.Security.Cybersecurity.confidentiality**

### Clause in document:
**TS-0002 clause 6.4**

### Solution:
**Access Control and Authorization, TS-0003 clause 7**

<table>
<thead>
<tr>
<th>Concern</th>
<th>Aspect/Concern</th>
<th>Discussion of Concern</th>
<th>Discussion Reference(s)</th>
<th>Solution</th>
<th>Solution Reference(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional</td>
<td>Functional</td>
<td>in general</td>
<td>n/a</td>
<td>Use proper access control settings under control of the data subject (individual whose privacy is exposed by the data)</td>
<td>TS-0003 Clause 7</td>
</tr>
<tr>
<td>Trustworthiness</td>
<td>Trustworthiness</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>Privacy</td>
<td>authorization, privacy and all the security requirements are defined</td>
<td>TS-0002 clause 6.4</td>
<td>Perform proper risk and vulnerability assessment and mitigate unacceptable risks</td>
<td>Any Risk assessment methodology. See TR-0008</td>
</tr>
<tr>
<td>Reliability</td>
<td>Reliability</td>
<td>in terms of message delivery, yes</td>
<td>tbd</td>
<td></td>
<td>TS-0001 clause 6.2.2</td>
</tr>
<tr>
<td>Resilience</td>
<td>Resilience</td>
<td>in terms of message delivery, yes</td>
<td>tbd</td>
<td></td>
<td>TS-0001 clause 6.2.2</td>
</tr>
<tr>
<td>Safety</td>
<td>Safety</td>
<td>Every deployment requires a risk and vulnerability assessment</td>
<td>TR-0008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Security</td>
<td>all the security requirements are defined</td>
<td>TS-0002 clause 6.4, TR-0008</td>
<td>Definition of 4 protection levels suitable for different exposures. Definition of security frameworks to protect assets</td>
<td>TS-0003</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>Cybersecurity</td>
<td>all the security requirements are defined</td>
<td>TS-0002 clause 6.4</td>
<td>CPS security implies cybersecurity with additional challenges. Solutions exist to mitigate risks down to acceptable levels!</td>
<td>TR-0008, TS-0008</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Confidentiality</td>
<td>all the security requirements are defined</td>
<td>TS-0002 clause 6.4</td>
<td>Access Control and Authorization</td>
<td>TS-0003 clause 7</td>
</tr>
<tr>
<td>Integrity</td>
<td>Integrity</td>
<td>all the security requirements are defined</td>
<td>TS-0002 clause 6.4</td>
<td>Implement proper protection level</td>
<td>TR-0008, TS-0003</td>
</tr>
<tr>
<td>Availability</td>
<td>Availability</td>
<td>Risks related to Denial of Service must be mitigated</td>
<td>TR-0008</td>
<td>Some mitigation mechanisms exist</td>
<td>TR-0008, TS-0009</td>
</tr>
</tbody>
</table>
Foundation for Cooperation

<table>
<thead>
<tr>
<th>Concerns</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>... N</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>... N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Standard

PPI

Gap

PPI
Specs to Pivotal Points of Interoperability

Zone of Concerns = bundles of services that address a “vector” of concerns
Pivotal Points of Interoperability (PPI)

Independent technology deployments

Potentially large distance to interoperability

With Pivotal Points of Interoperability

Minimize distance to interoperability
e.g. Convert XML to JSON

Application Diversity

PPI
e.g. IPv6 address

PPI
e.g. TLS 1.2

PPI
e.g. REST APIs
## SynchroniCity Zones of Concern

<table>
<thead>
<tr>
<th>Security and privacy</th>
<th>Monitoring and management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Northbound uniform interface</td>
<td></td>
</tr>
<tr>
<td>Business ecosystem</td>
<td></td>
</tr>
<tr>
<td>Historical data</td>
<td>Open data</td>
</tr>
<tr>
<td>Context data management</td>
<td>IoT management</td>
</tr>
<tr>
<td>Southbound uniform interface</td>
<td></td>
</tr>
<tr>
<td>IoT devices</td>
<td>Sensor</td>
</tr>
</tbody>
</table>

**Smart city end-use applications**

- Northbound uniform interface
- Business ecosystem
- Historical data
- Open data
- Context data management
- IoT management
- Southbound uniform interface
- IoT devices
- Sensor
- User generated data

*Image: [SynchroniCity Zones of Concern](#)
ESPRESSO Zones of Concern

Access Services and Domain Services

Data Lake

Device Zone

Appl Zone

Other
For additional information

• Program Web Site:  
  www.nist.gov/cps

• CPS Public Working Group  
  pages.nist.gov/cpspwg

• Smart City Framework  
  pages.nist.gov/smartcitiesarchitecture

• Contact:  
  chris.greer@nist.gov