System of Systems (SoS) Strategies for the LHC

Jeff Joyce, Critical Systems Labs Ltd. (UK)

September 10, 2014

Abstract

“Systems of Systems" are systems whose components are themselves complex systems such that the combined behavior of these components cannot be easily understood or explained in terms of the behaviors of the individual components. Examples of such systems are increasingly common across a variety of technological domains including aerospace, defense, automotive and energy generation/distribution. Many of the distinguishing characteristics of Systems of Systems are also exhibited by the CERN Large Hadron Collider (LHC). Technical challenges faced by engineers responsible for the development or modification of Systems of Systems in other technological domains are also likely to be challenges for CERN engineers, especially as the accelerator technology is pushed towards operation at higher energy levels. Following a brief introduction to the Systems of Systems concept, this seminar will describe some on-going research by Critical Systems Labs with industry partners to address specific challenges of developing and modifying Systems of Systems. This includes the use of computer-readable modelling languages such as AADL to represent the high level architecture of a System of Systems at an appropriate level of abstraction.

Critical Systems Labs

- Provides clients with expertise in critical systems across a variety of technical domains including aerospace, defence, automotive, energy, rail signalling, medical, ….
- Previous CERN interactions include
  - Seminar on critical systems verification (2005)
  - LHC BIS technical audit (2009)
  - LHC BLMS technical audit (2010)
  - LHC SMP system specification (2011)
  - ITER Magnet Interlock System specification (2012)

What are “Systems of Systems”?

August 14, 2003

- Second most widespread blackout in history
- Affected an estimated 10 million people in Ontario and 45 million people in eight U.S. states.

"What would have been a manageable local blackout cascaded into widespread distress on the electric grid."

- 12:15 p.m. Incorrect telemetry data renders inoperative the state estimator, a power flow monitoring tool operated by the Indiana-based Midwest Independent Transmission System Operator (MISO). An operator corrects the telemetry problem but forgets to restart the monitoring tool.
- 1:31 p.m. The Eastlake, Ohio generating plant shuts down. The plant is owned by FirstEnergy, an Akron, Ohio-based company that had experienced extensive recent maintenance problems.
- 2:02 p.m. The first of several 345 kV overhead transmission lines in northeast Ohio fails due to contact with a tree in Walton Hills, Ohio.
- 2:14 p.m. An alarm system fails at FirstEnergy's control room and is not repaired.
- 3:05 p.m. A 345 kV transmission line known as the Chamberlin-Harding line sags into a tree and trips in Parma, south of Cleveland.
- 3:17 p.m. Voltage dips temporarily on the Ohio portion of the grid. Controllers take no action.
- 3:32 p.m. Power shifted by the first failure onto another 345 kV power line, the Hanna-Juniper interconnection, causes it to sag into a tree, bringing it offline as well. While MISO and FirstEnergy controllers concentrate on understanding the failures, they fail to inform system controllers in nearby states.
- …

- ...
- 4:10:34 p.m. Many transmission lines trip out, first in Michigan and then in Ohio, blocking the eastward flow of power around the south shore of Lake Erie from Toledo, Ohio, east through Erie, Pennsylvania, and into the Buffalo, New York, metropolitan area. Suddenly bereft of demand, generating stations go offline, creating a huge power deficit. In seconds, power surges in from the east, overloading east-coast power plants whose generators go offline as a protective measure, and the blackout is on.
- …
- 4:12:58 p.m. Northern New Jersey separates its power-grids from New York and the Philadelphia area, causing a cascade of failing secondary generator plants along the New Jersey coast and throughout the inland regions west.
- …
- 4:13 p.m. End of cascading failure. 256 power plants are off-line, 85% of which went offline after the grid separations occurred, most due to the action of automatic protective controls.

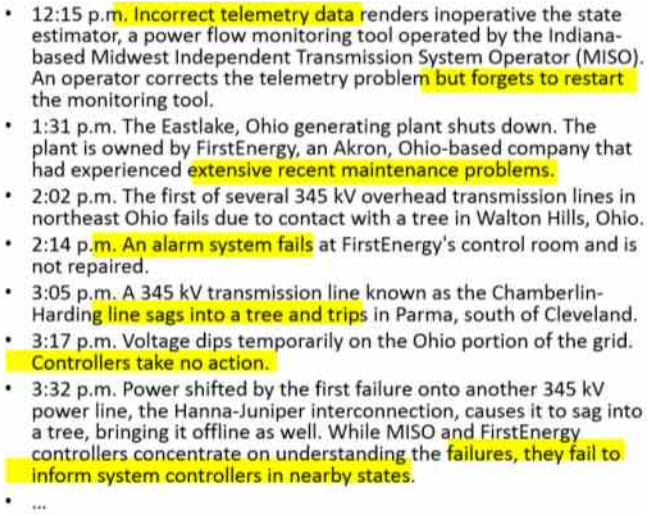
Effects beyond disruption of electrical grid

- Water supply
- Transportation
- Communication
- Industry

At least eleven fatalities

Exceptional (or not?)

- While the effects were truly exceptional, the individual causes were not exceptional, e.g.,
  - "… incorrect telemetry …"
  - "… forgets …"
  - "… maintenance problems …"
  - "… alarms systems fails …"
  - "… line sags into a tree …"
  - "… take no action …"
  - "… fails to inform …"



- 12:15 p.m. Incorrect telemetry data renders inoperative the state estimator, a power flow monitoring tool operated by the Indiana-based Midwest Independent Transmission System Operator (MISO). An operator corrects the telemetry problem but forgets to restart the monitoring tool.
- 1:31 p.m. The Eastlake, Ohio generating plant shuts down. The plant is owned by FirstEnergy, an Akron, Ohio-based company that had experienced extensive recent maintenance problems.
- 2:02 p.m. The first of several 345 kV overhead transmission lines in northeast Ohio fails due to contact with a tree in Walton Hills, Ohio.
- 2:14 p.m. An alarm system fails at FirstEnergy's control room and is not repaired.
- 3:05 p.m. A 345 kV transmission line known as the Chamberlin-Harding line sags into a tree and trips in Parma, south of Cleveland.
- 3:17 p.m. Voltage dips temporarily on the Ohio portion of the grid. Controllers take no action.
- 3:32 p.m. Power shifted by the first failure onto another 345 kV power line, the Hanna-Juniper interconnection, causes it to sag into a tree, bringing it offline as well. While MISO and FirstEnergy controllers concentrate on understanding the failures, they fail to inform system controllers in nearby states.
- …

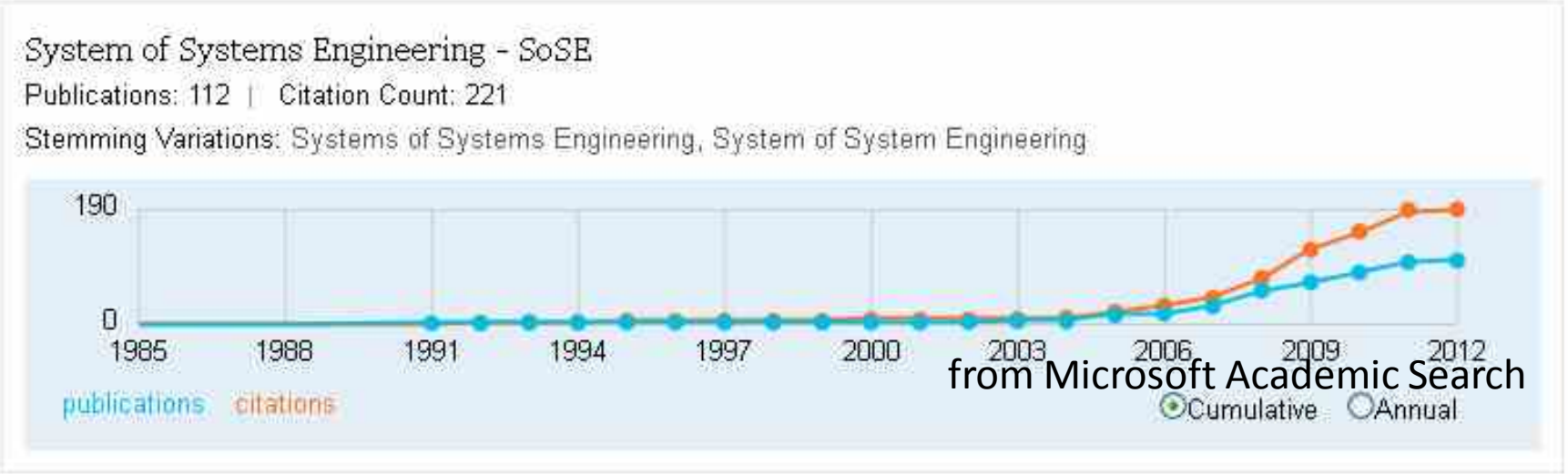
(A) Definition

- **System of Systems** is a system whose components are themselves complex systems such that the combined behavior of these components cannot be easily understood or explained in terms of the behaviors of the individual components

Wikipedia Definition

- **System of systems** is a collection of task-oriented or dedicated systems that pool their resources and capabilities together to create a new, more complex system which offers more functionality and performance than simply the sum of the constituent systems

History



from Microsoft Academic Search

Maier's Five Criteria (1998)

1. Operational Independence
2. Managerial Independence
3. Geographic Distribution
4. Emergent Behavior
5. Evolutionary Development

Operational Independence

- A system of systems is composed of systems that are independent and useful in their own right.
- If a system of systems is disassembled into the component systems, these component systems are capable of independently performing useful operations independently of one another.

Sage and Cuppan (2001)

Managerial Independence

- The component systems not only can operate independently, they generally do operate independently to achieve an intended purpose.
- The component systems are generally individually acquired and integrated and they maintain a continuing operational existence that is independent of the system of systems.

Sage and Cuppan (2001)

Geographic Distribution

- Geographic dispersion of component systems is often large.
- Often, these systems can readily exchange only information and knowledge with one another, and not substantial quantities of physical mass or energy.

Sage and Cuppan (2001)

Emergent Behavior

- The system of systems performs functions and carries out purposes that do not reside in any component system.
- These behaviors are emergent properties of the entire system of systems and not the behavior of any component system.
- The principal purposes supporting engineering of these systems are fulfilled by these emergent behaviors.

Sage and Cuppan (2001)

Evolutionary Development

- A system of systems is never fully formed or complete.
- Development of these systems is evolutionary over time and with structure, function and purpose added, removed, and modified as experience with the system grows and evolves over time.

Sage and Cuppan (2001)

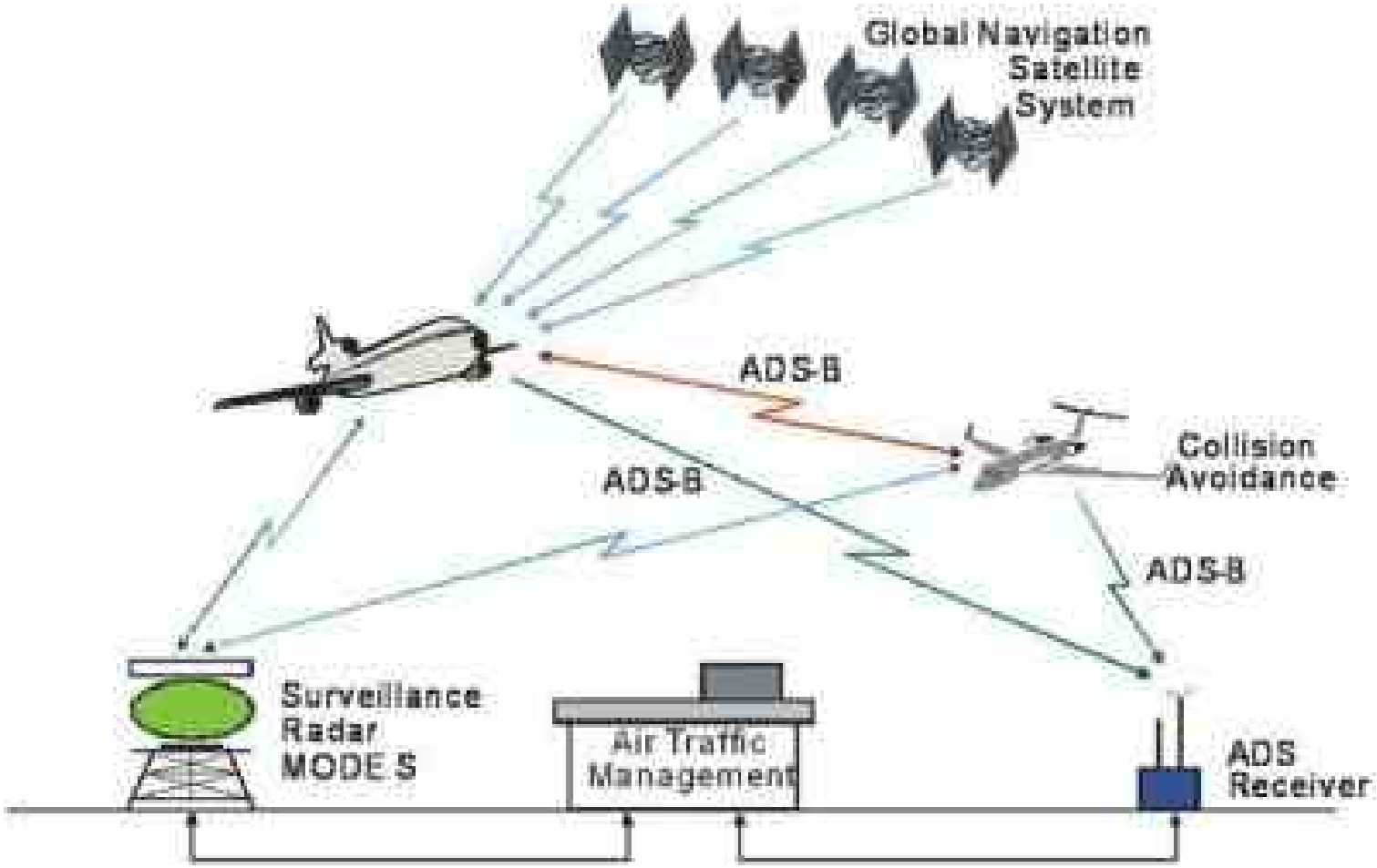
Additional SoS Characteristics

- Uncertain, indefinite boundary
- Details of components system limited
- Heterogeneous
- Interdisciplinary
- Other?

August 14, 2003

1. Operational Independence ✓
2. Managerial Independence ✓
3. Geographic Distribution ✓
4. Emergent Behavior ✓
5. Evolutionary Development ✓
6. Uncertain, indefinite boundary ✓
7. Details of components system limited ✓
8. Heterogeneous ✓
9. Interdisciplinary ✓

Air Traffic Management (ATM)



Controller Pilot Data Link Communication (CPDLC)

Air Traffic Management System

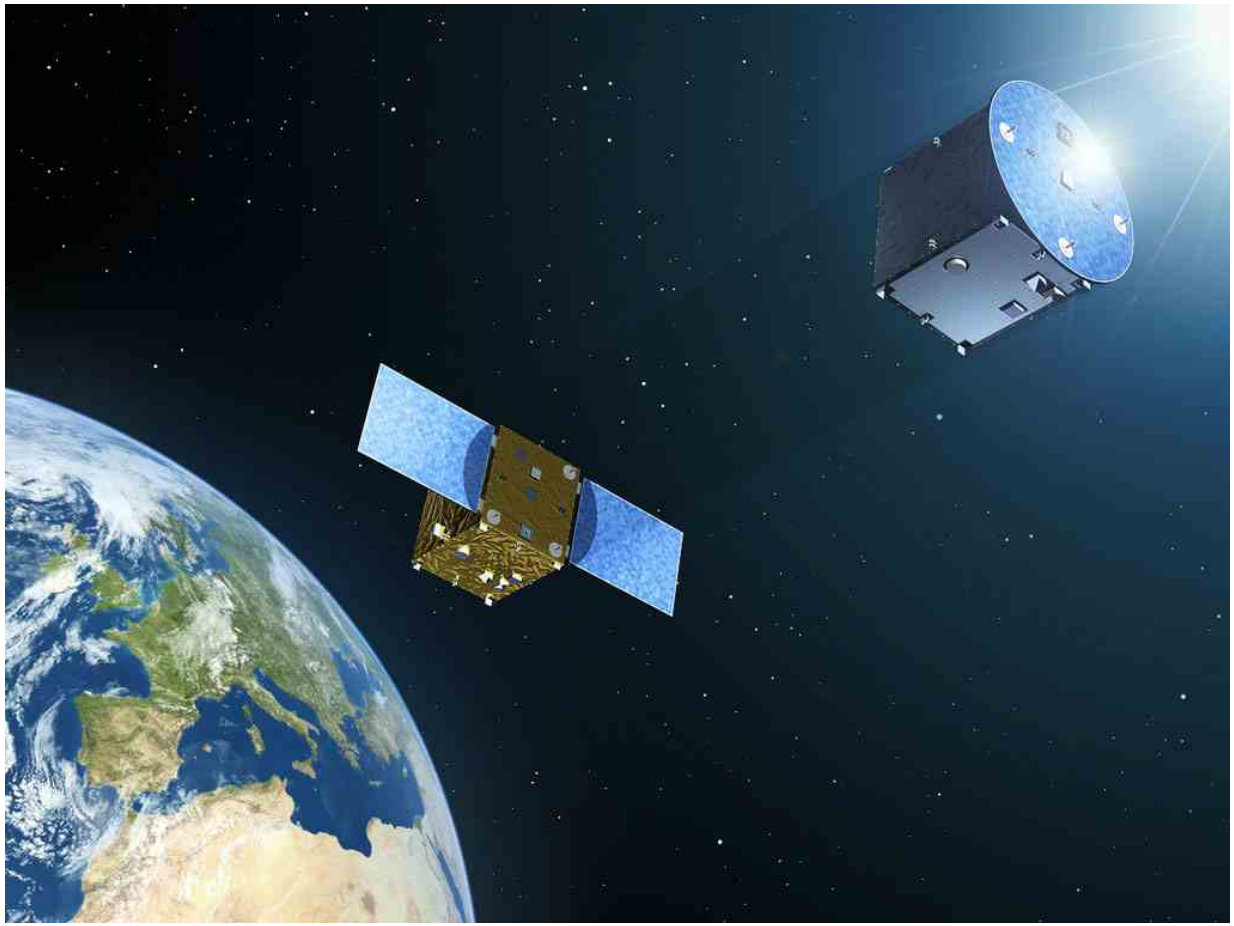
1. Operational Independence
2. Managerial Independence
3. Geographic Distribution
4. Emergent Behavior
5. Evolutionary Development
6. Uncertain, indefinite boundary
7. Details of components system limited
8. Heterogeneous
9. Interdisciplinary

Advanced Automotive

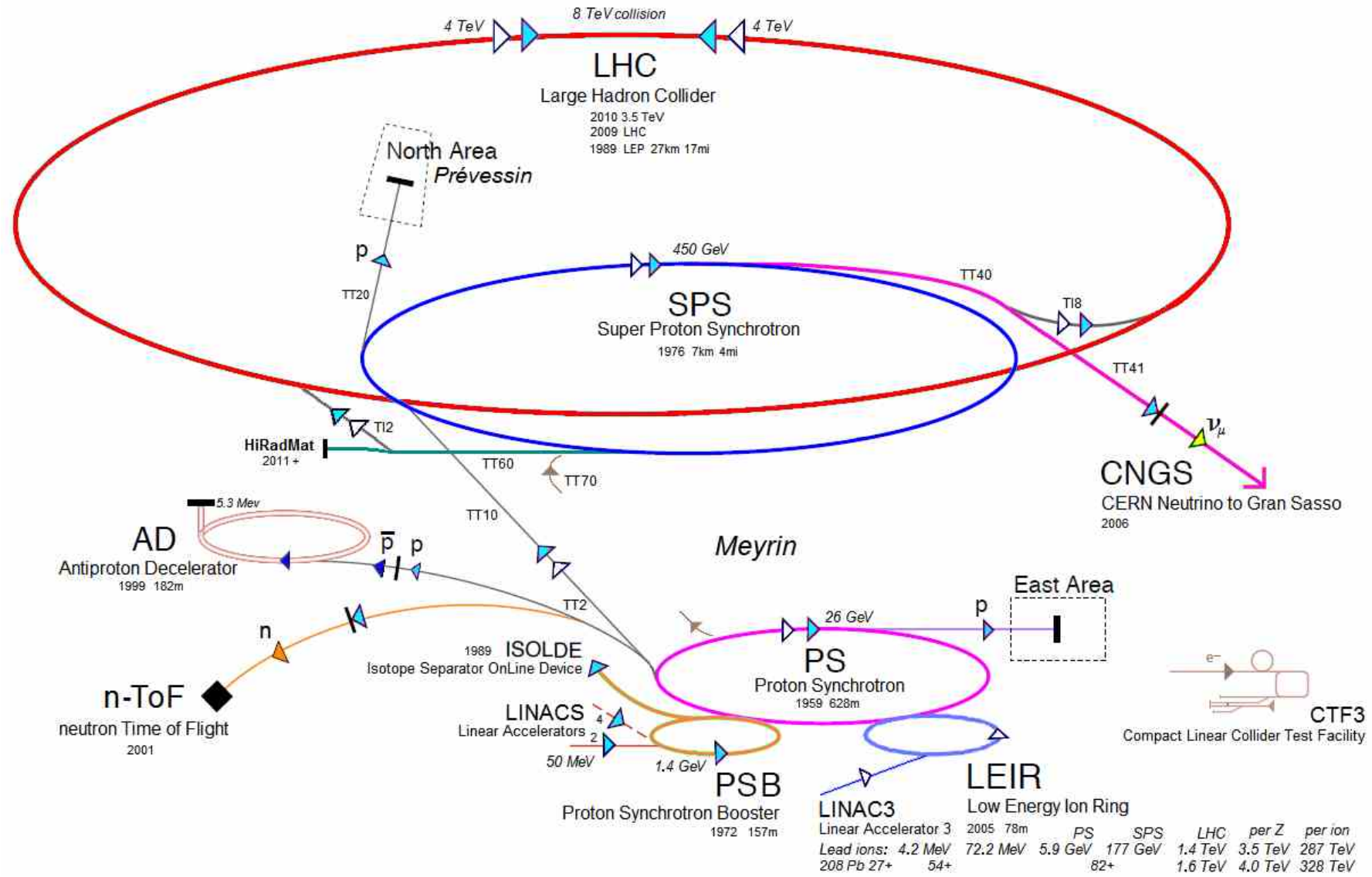
- Map/GPS for autonomous driving
- Vehicle to Road communication
- Vehicle to Vehicle communication
  - Collision avoidance
  - Bunches
- Driverless valet parking

European Proba-3

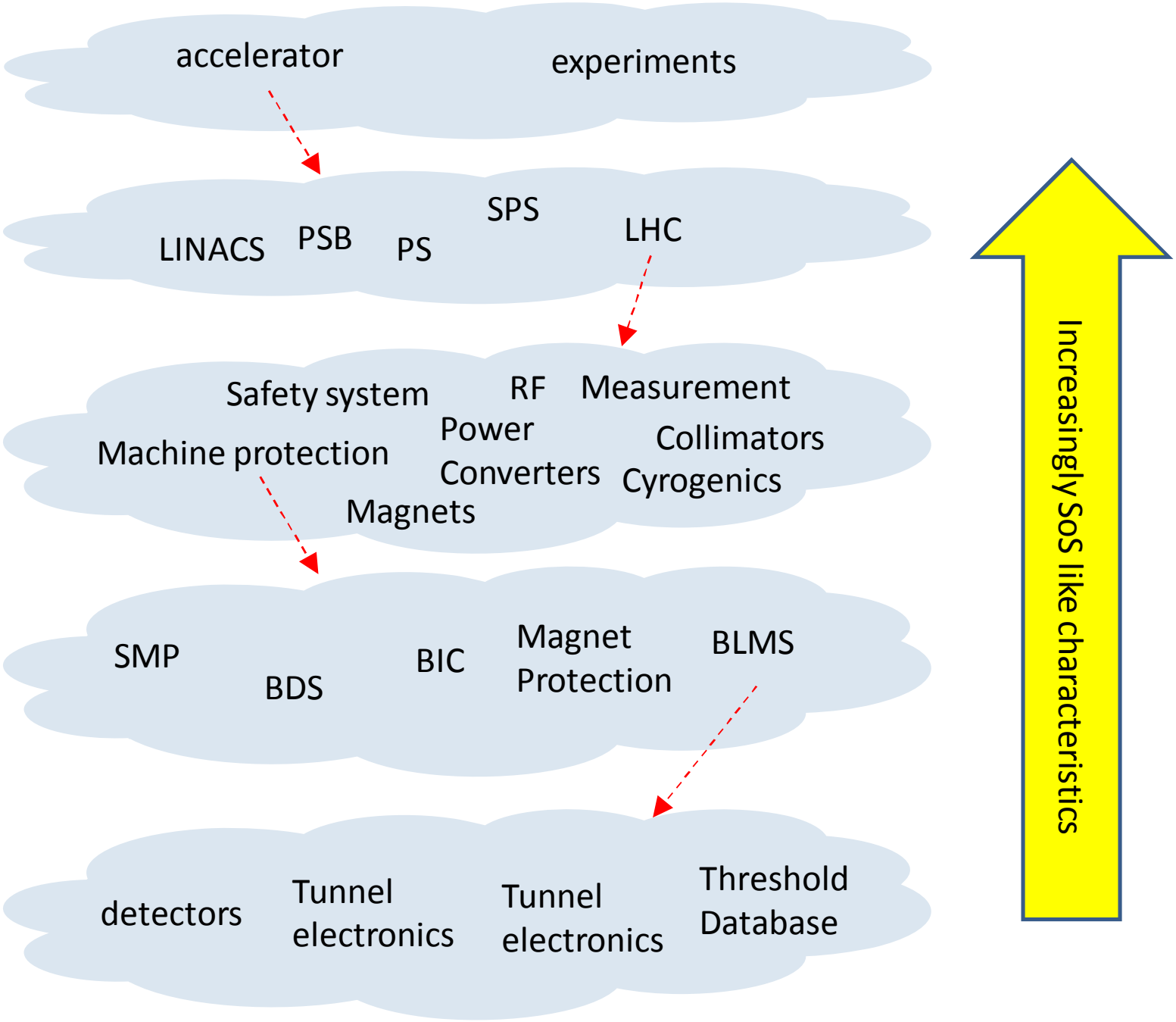
Two independent spacecraft flying close in close formation scheduled for launch in 2017



CERN Accelators



CERN
LHC


accelerator
experiments
LINACS
PSB
PS
SPS
LHC
Safety system
RF
Measurement
Machine protection
Power
Converters
Collimators
Cyrogenics
Magnets
SMP
BDS
BIC
Magnet
Protection
BLMS
detectors
Tunnel
electronics
Tunnel
electronics
Threshold
Database
Increasingly SoS like characteristics

Discussion

Which of these characteristics apply to the LHC?

1. Operational Independence
2. Managerial Independence
3. Geographic Distribution
4. Emergent Behavior
5. Evolutionary Development
6. Uncertain, indefinite boundary
7. Details of components system limited
8. Heterogeneous
9. Interdisciplinary

Related Terminology/Concepts

- Federated System
- Enterprise Architecture
- Multi-agent Systems
- Complex Systems

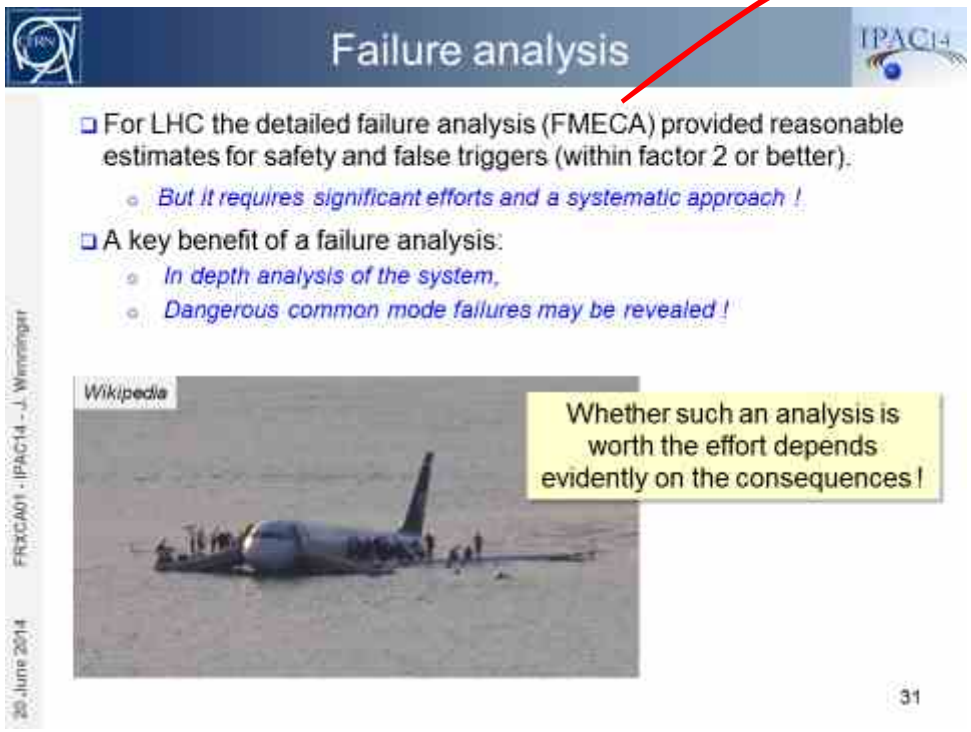
Systems of Systems Engineering

- Differs from systems engineering of monolithic, complex systems because design for System-of-Systems problems is usually performed with some uncertainty about the component systems.
- Whereas systems engineering focuses on building the system right, SoSE focuses on choosing the right system(s) and their interactions to satisfy the requirements.

(Some) Safety Challenges for SoSE

- Size and complexity
- Limited access to details of component systems
- Descriptions based on imprecise abstractions
- Emergent behaviors, including unforeseen interactions
- Insufficient tracking of assumptions
- Evolutionary development
- Conflicting safety objectives
- Risk mitigated locally not globally
- No redundancy of the entire SoS (as a whole)
- Cascading and multiplicative effects

Limitations of Traditional Methods



State of the art and Future Challenges for Machine Protection Systems
Jörg Wenninger, IPAC14, Dresden, 20th June 2014

FMEA, FMECA and other traditional methods are useful, but be aware of their limitations for complex systems including SoS's

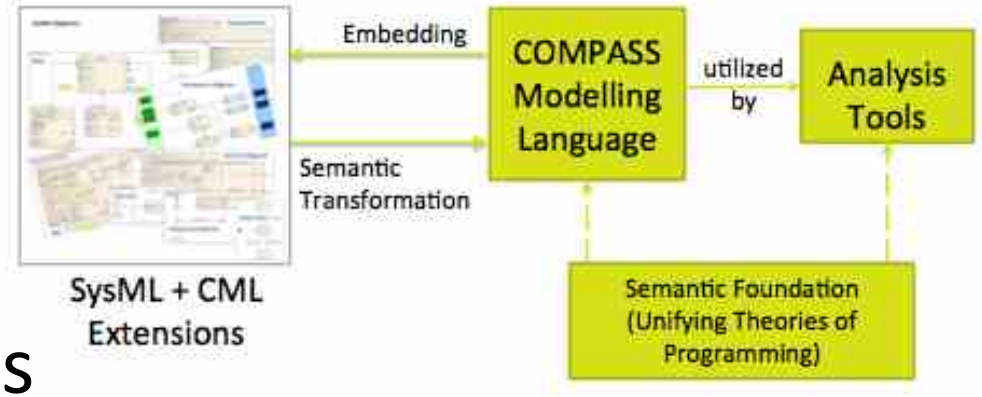
Limitations of Traditional Techniques

- Traditional techniques tend to focus on component failure
  - may overlook other causal factors such as unforeseen interactions, external factors, human error
- Also tend to focus on single causes rather than combinations of causal factors

Failure 1 → Effect1
Failure 2 → Effect2
Failure 3 → Effect3
…

Current & Future Directions

- Systems of Systems R&D is largely focused on modeling and simulation
- For example, COMPASS, a European consortium, is a group of researchers and companies committed to collaborative R&D on model-based techniques for developing and maintaining Systems of Systems



CERN LHC

- How has CERN successfully the SoS complexity of the LHC so far?
- From 2009 report on BIS technical audit …

> In particular, CSL very much appreciates that CERN is a research institution with a research-oriented culture that is very different from the typical culture of an industrial organization. It would be unreasonable, and also undesirable, to expect the development of the BIS to exactly follow the practices of industry used for the development of complex safety-related systems. Moreover, CSL has noticed how the research-oriented culture of CERN has benefited the development of the BIS. This is especially evident in the richness of various technical documents that have been produced in the course of developing the BIS. It is not common to see the same deep of thought in the technical documentation typically produced by industry for the development of complex systems. Nonetheless, it is useful for CERN to be aware of differences between the practices used by CERN for the development of the BIS and the common practice of industry for system similar to the BIS in regard to complexity and criticality.

CERN LHC

CERN is a remarkably collaborative environment that appears to have relied very much on …

1. organizational and individual enthusiasm for sharing understanding and insights
2. original developers remain available or at least reachable
3. continuing presence of exceptional individuals who “understand everything”

But will this continue for the lifetime of the LHC?

CSL's SoS Strategy

Result of a multi-year R&D effort on SoS safety engineering is a strategy that focuses on:

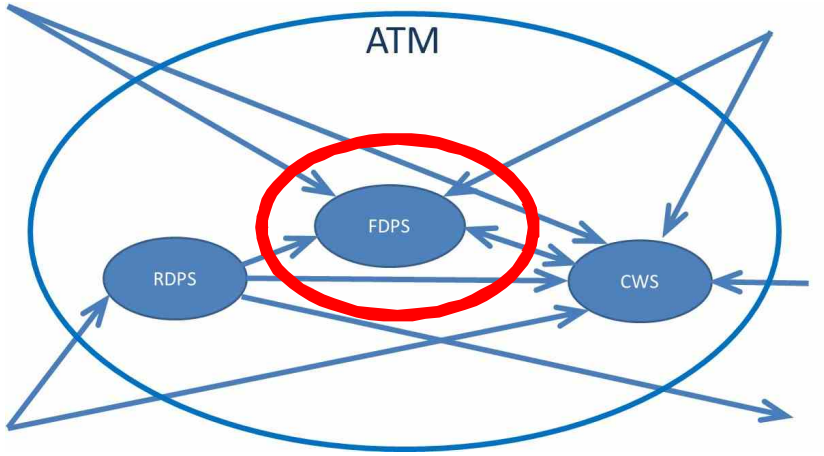
1. Describing the structure of the SoS in suitably abstract and precise manner
2. Specifying interfaces including behavioural constraints (using conservative approximations)
3. Developing structured arguments that can be independently checked and updated

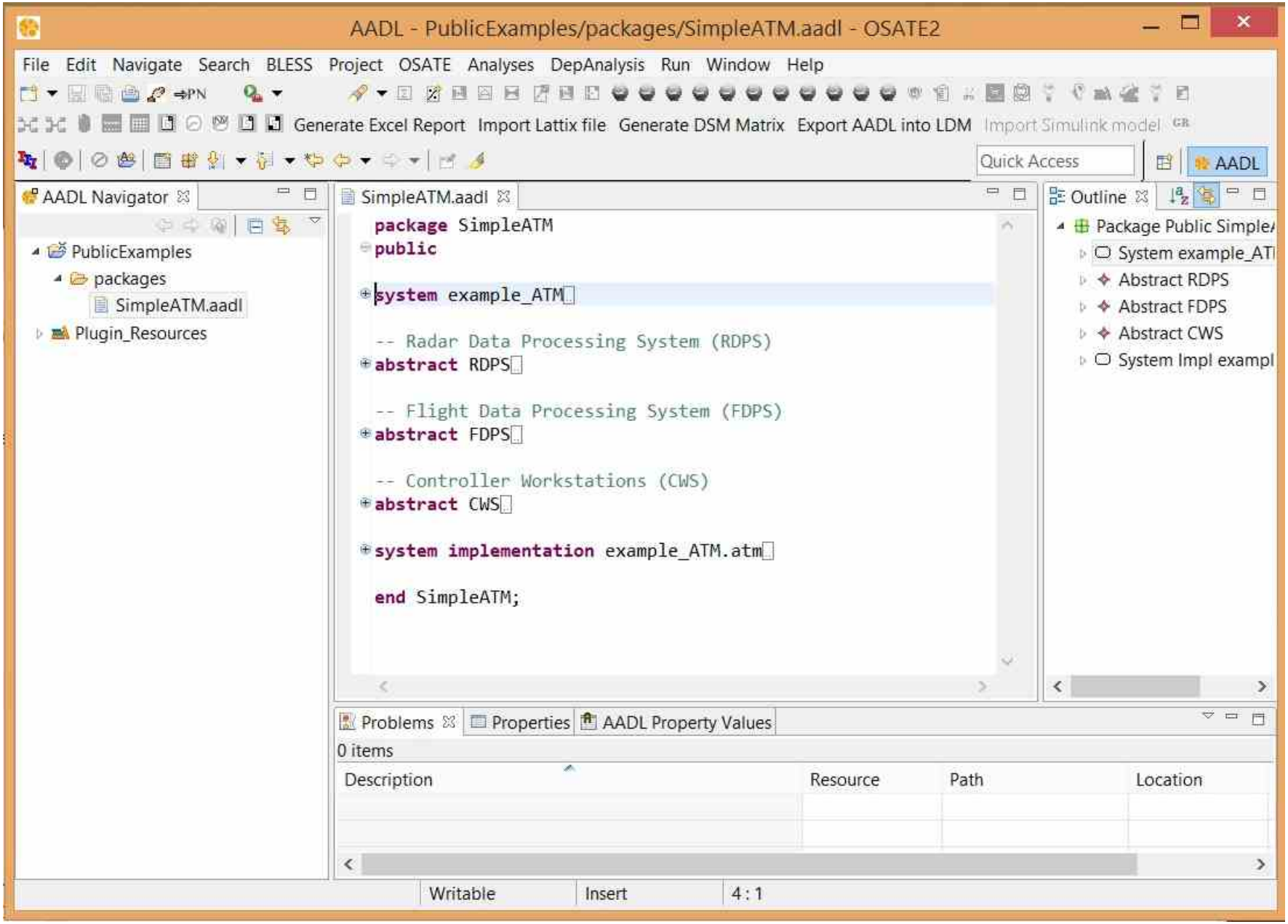
AADL

- The Architecture Analysis & Design Language (AADL) is a rigorous textual language
  - may be contrasted with graphical modelling languages such as UML and SysML
- R&D results show that AADL is very suitable for modelling an SoS at an appropriate level of abstraction
- Extensible, i.e., could be extended to support specification of (safety) constraints
- Open source tools, e.g., OSATE

```
-- Flight Data Processing System (FDPS)
abstract FDPS
features
  radar_tracks: in data port;
  radar_alerts: in data port;
  altimeter_settings: in data port;
  met_reports: in data port;
  position_reports: in data port;
  fpls: in out data port;
  clearances: in out data port;
  handoffs: in out data port;
  flight_updates: out data port;
  alerts_and_warnings: out data port;
end FDPS;

....
```




AADL - PublicExamples/packages/SimpleATM.aadl - OSATE2
File Edit Navigate Search BLESS Project OSATE Analyses DepAnalysis Run Window Help
Generate Excel Report
Import Lattix file
Generate DSM Matrix
Export AADL into LDM
Import Simulink model
Quick Access
AADL
AADL Navigator
PublicExamples
packages
SimpleATM.aadl
Plugin_Resources
SimpleATM.aadl
package SimpleATM
public
system example_ATM
-- Radar Data Processing System (RDPS)
abstract RDPS
-- Flight Data Processing System (FDPS)
abstract FDPS
-- Controller Workstations (CWS)
abstract CWS
system implementation example_ATM.atm
end SimpleATM;
Outline
Package Public SimpleA
System example_ATI
Abstract RDPS
Abstract FDPS
Abstract CWS
System Impl exampl
Problems
Properties
AADL Property Values
0 items
Description
Resource
Path
Location
Writable
Insert
4 : 1

System Safety Engineering Process

- Use AADL to capture the structure & interfaces of a SoS early in the system safety engineering process
- Start with a relatively high level of abstraction using features of AADL such as generic components
- Refine incrementally as understanding of the SoS evolves

Summary

- SoSs are increasingly common across a variety of technical domains
- Traditional systems engineering methods are not necessarily adequate
- Significant challenges for System Safety Engineering
- AADL can be used to describe a SoS at an appropriate level of abstraction

Take-aways

- Criteria for distinguishing a SoS from single monolithic systems
- Insights into challenges of system safety for SoSs
- Possibility of using AADL to improve system safety process

Maier's Five Criteria (1998)

1. Operational Independence
2. Managerial Independence
3. Geographic Distribution
4. Emergent Behavior
5. Evolutionary Development

(Some) Safety Challenges for SoSE

- Size and complexity
- Limited access to details of component systems
- Descriptions based on imprecise abstractions
- Emergent behaviors, including unforeseen interactions
- Insufficient tracking of assumptions
- Evolutionary development
- Conflicting safety objectives
- Risk mitigated locally not globally
- No redundancy of the entire SoS (as a whole)
- Cascading and multiplicative effects