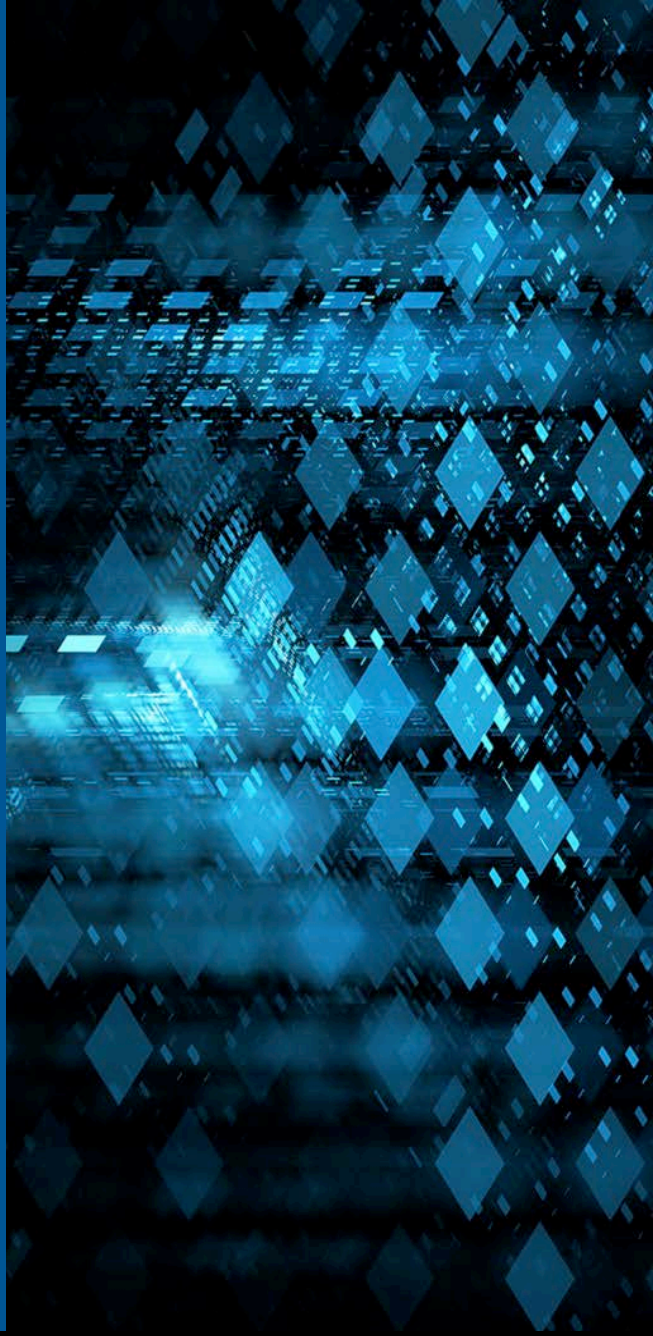
AADL for Secure & Safe Systems Design & Analysis

Part 1 - Introduction

Julien Delange

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0003990

Tutorial Agenda

Introduction: required background, role of MBE, tutorial overview

AADL Concepts: learn enough to use AADL and OSATE

Flow Latency: how to capture flow characteristics? How can I generate a flow analysis from my architecture model?

Safety Analysis: how to capture safety in an AADL model? What types of reports can I generate? How can I generate them?

Security Analysis: representation of security aspects. How to detect security issues? What type of reports can we generate?

Who is the presenter?

Master (UPMC) and PhD (TELECOM ParisTech) in France – main topics embedded, real-time systems with emphasis on safety and security

Previous ESA software engineer with experience in validation and **certification standards** (DO-178C, ECSS)

Experience with **Real-Time operating systems** (VxWorks, RTEMS), **design and coding standards** (MISRA-C, etc.)

AADL contributor since 2008: author of ARINC653 annex, contributor and main sponsor of AADL v2.2

Lead developer of OSATE, create and develop many analysis plugin (e.g. safety & security tools)

More information on http://julien.gunnm.org (personal website)

Disclaimer

Some of the following slides are based on the AADL tutorial at MODELS15

Tutorial delivered by **Jerome Hugues** and **Julien Delange**

Overlap of concepts/topics

The 2015 tutorial covers code generation

This tutorial covers more safety analysis and include security!

Materials are online, worth to check it out!

http://www.openaadl.org/blog.html

We Rely on Software for Safe Aircraft Operation

Quantas Airbus A330-300 Forced to make Emergency Landing - 36 Injured

Written by htbw on Oct-7-08 1:48pm

From: soyawannaknow.blogspot.com

Thirty-six passengers and crew were injured, son
in a mid-air drama that forced a Qantas jetliner t
emergency landing, the Australian carrier and pc
Tuesday.

The terrifying incident saw the Airbus A330-300 i
mayday call when it suddenly changed altitude duri
from Singapore to Perth, Qantas said.

Embedded software systems introduce a new class of problems not addressed by traditional system safety analysis

Oct. 15 (Bloomberg) -- **Airbus SAS** issued an alert to airli
after Australian investigators said a computer fault on a
Ltd. flight switched off the autopilot and generated false
jet to nosedive.

The Airbus A330-300 was cruising at 37,000 feet (11,277
computer fed incorrect information to the flight control sy
Australian Transport Safety Bureau said yesterday. The
650 feet within seconds, slamming passengers and crew
ceiling, before the pilots regained control.

`This appears to be a unique event," the bureau said, a
Toulouse, France-based Airbus, the world's largest maker
aircraft, issued a telex late yesterday to airlines that fly A
fitted with the same air-data computer. The advisory is `
minimizing the risk in the unlikely event of a similar occurr

FAA says software problem with Boeing 787s could be catastrophic

By **Dan Catchpole**

@dcatchpole

The Federal Aviation Administration says a software problem with Boeing 787 Dreamliners could lead to one of the advanced jetliners losing electrical power in flight, which could lead to loss of control.

- **The Buzz**: Hipster's dilemma
- Boeing & aerospace news
- Aerospace blog

The FAA notified operators of the airplane Friday that if a 787 is powered continuously for 248 days, the plane will automatically shut down its alternating current (AC) electrical power.

Software Problems not just in Aircraft

Expert • Independent • Nonprofit
ConsumerReports.org

This article appeared in May 2010 Consumer Reports Magazine.

Many appliances now rely on electronic controls and operating softw But it turned out to be a problem for the Kenmore 4027 front-loader, which scored near the bottom in our February 2010 report.

Our tests found that the rinse cycles on some models worked improperly, resulting in an unimpressive cleaning.

When Sears, which sells the washer, saw our February 2010 Ratings (available to subscribers), it worked with LG, which makes the washer, to figure out what was wrong. They quickly determined that a software problem was causing short or missing rinse and wash cycles, affecting wash performance. Sears and LG say they have reprogrammed the software on the models in their warehouses and on about 65 percent of the washers already sold, including the ones we had purchased.

Our retests of the reprogrammed Kenmore 4027 found that the cycles now worked properly, and the machine excelled. It now tops our Ratings (available to subscribers) of more than 50 front-loaders and we've made it a CR Best Buy.

If you own the washer, or a related model such as the Kenmore 4044 or Kenmore Elite 4051 or 4219, you should get a letter from Sears for a free service call. Or you can call 800-733-2299.

May 7, 2010

Lexus GX 460 passes retest; Consumer Reports lifts "Don't Buy" label

Consumer Reports is lifting the Don't Buy: Safety Risk designation from the 2010 Lexus GX 460 SUV after recall work corrected the problem it displayed in one of our emergency handling tests. (See the original report and video: "Don't Buy: Safety Risk--2010 Lexus GX 460.")

We originally experienced the problem in a test that we use to evaluate what's called lift-off oversteer. In this test, as the vehicle is driven through a turn, the driver quickly lifts his foot off the accelerator pedal to see how the vehicle reacts. When we did this with our GX 460, its rear end slid out until the vehicle was almost sideways. Although the GX 460 has electronic stability control, which is designed to prevent a vehicle from sliding, the system wasn't intervening quickly enough to stop the slide. We consider this a safety risk because in a real-world situation this could cause a rear tire to strike a curb or slide off of the pavement, possibly causing the vehicle to roll over. Tall vehicles with a high center of gravity, such as the GX 460, heighten our concern. We are not aware, however, of any reports of injury related to this problem.

Lexus recently duplicated the problem on its own test track and developed a software upgrade for the vehicle's ESC system that would prevent the problem from happening. Dealers received the software fix last week and began notifying GX 460 owners to bring their vehicles in for repair.

We contacted the Lexus dealership from which we had anonymously bought the vehicle and made an appointment to have the recall work performed. The work took about an hour and a half.

Following that, we again put the SUV through our full series of emergency handling tests. This time, the ESC system intervened earlier and its rear did not slide out in the lift-off oversteer test. Instead, the vehicle understeered—or plowed—when it exceeded its limits of traction, which is a more common result and makes the vehicle more predictable and less likely to roll over. Overall, we did not experience any safety concerns with the corrected GX 460 in our handling tests.

How do you upgrade washing machine software?

How do you prevent your engine from cheating?

Other consideration about software issues

2015: Symbiq infusion pumps, recalled because of FDA safety issues. **This could allow an unauthorized user to control the device and change the dosage the pump delivers, which could lead to over- or under-infusion of critical patient therapies.**

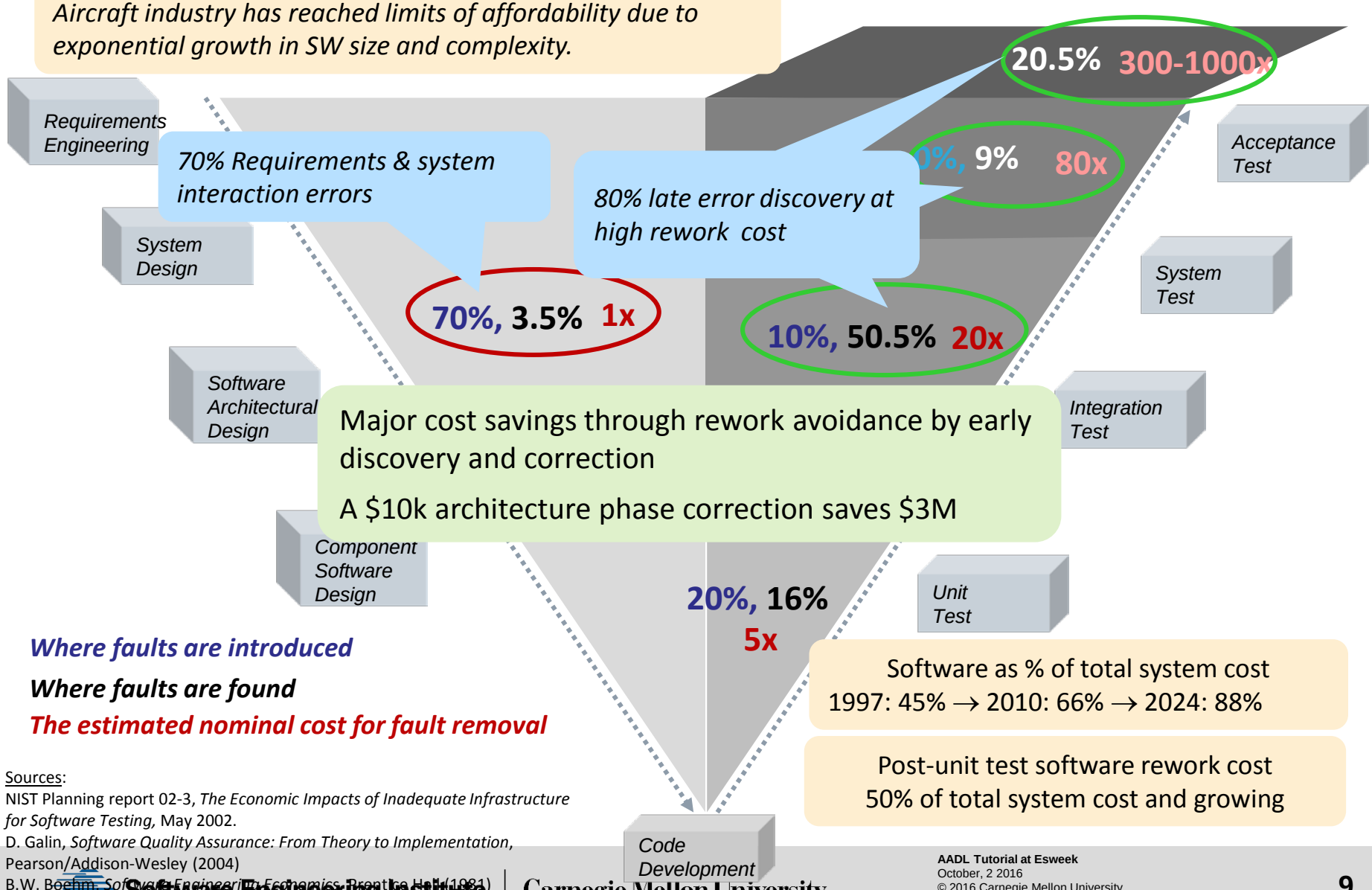
July 2015: **Ford recalls 433,000 cars because engines won't shut off**

July 2015: **Chrysler recalls 1.4M vehicles after Jeep hack**

August 2016: **Ford recalls 23.000 2017 Ford Escape vehicles to update power window software**. In the affected vehicles, the power window system configuration may exceed the regulatory requirement for remote actuation closing force, increasing the risk of injury.

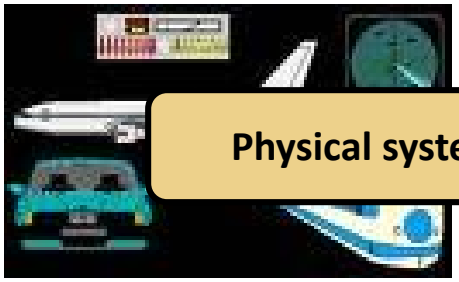
High Fault Leakage Drives Major Increase in System Cost

Aircraft industry has reached limits of affordability due to exponential growth in SW size and complexity.



Sources:
NIST Planning report 02-3, *The Economic Impacts of Inadequate Infrastructure for Software Testing,* May 2002.
D. Galin, *Software Quality Assurance: From Theory to Implementation,* Pearson/Addison-Wesley (2004)
B.W. Boehm, *Software Engineering Economics,* Prentice Hall (1981)

SAE Architecture Analysis & Design Language (AADL) to the Rescue

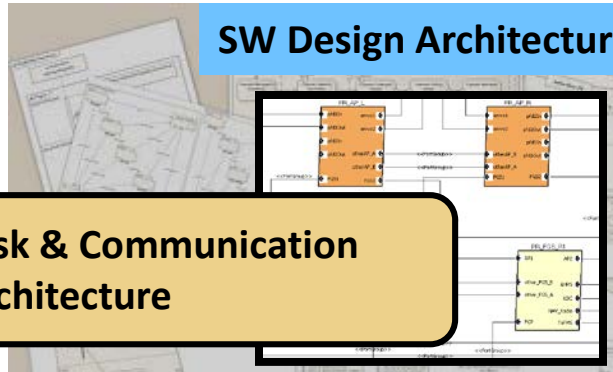


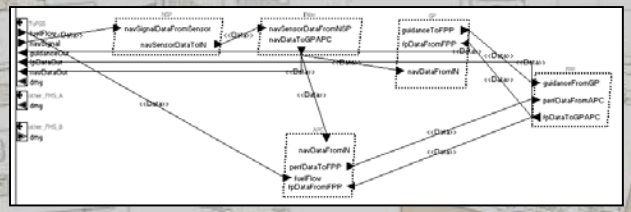
Physical system

Command & Control

Task & Communication Architecture

SW Design Architecture

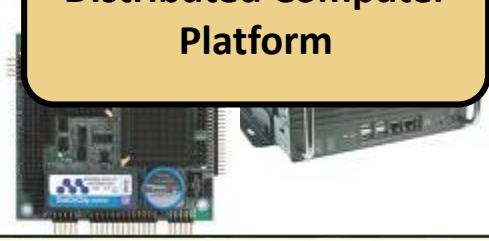




Deployed on

Physical interface

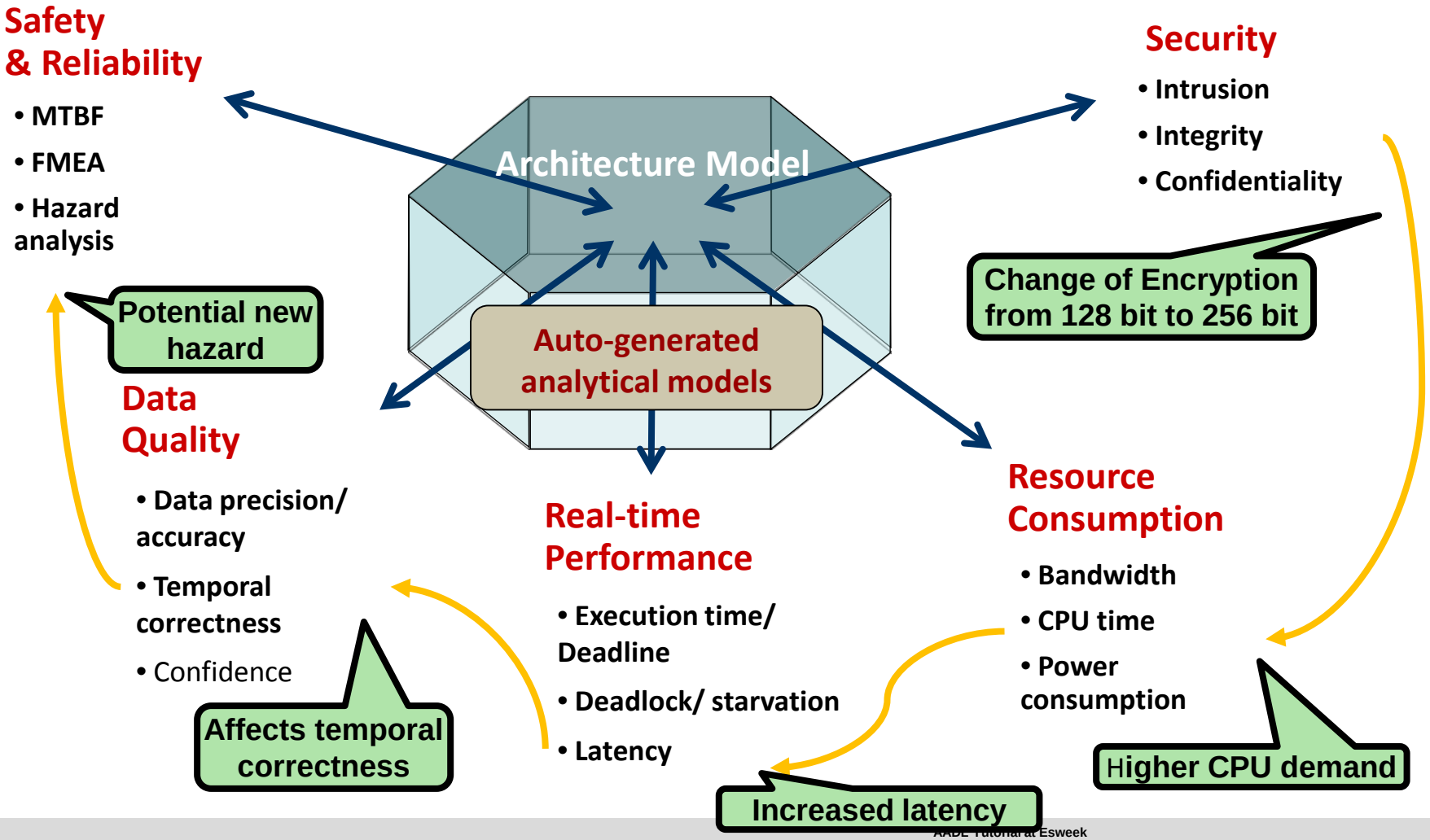
Distributed Computer Platform



AADL Addresses Increasing Interaction Complexity and Mismatched Assumptions

Analysis of Virtually Integrated Software Systems

Single Annotated Architecture Model Addresses Impact Across Operational Quality Attributes



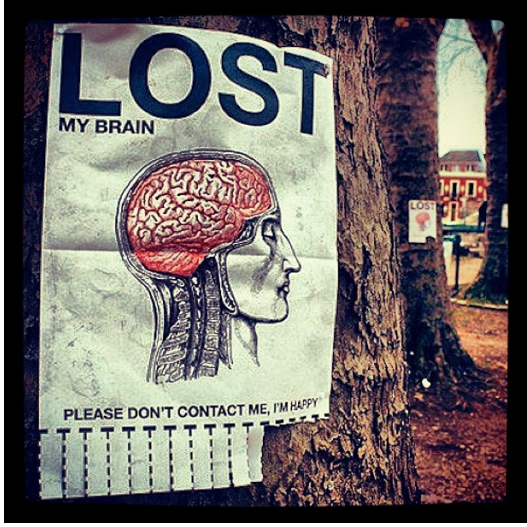
Objectives of this tutorial

AADL 101 – learn the basics and get started: the language, syntax and tools. What are the advantage of AADL? How you could use it for your own benefit?

Practice AADL analysis: what features of the language to use for each analysis, how to generate analysis reports using OSATE. Demonstrate this for latency, safety and security

What this tutorial is NOT about: design your own AADL extension, design a new OSATE analysis plugin

What you need?



A laptop with Windows, Linux or MacOS

OSATE version 2.2.1 update 01: www.osate.org

- Full product on http://www.aadl.info/aadl/osate/stable/2.2.1/products/

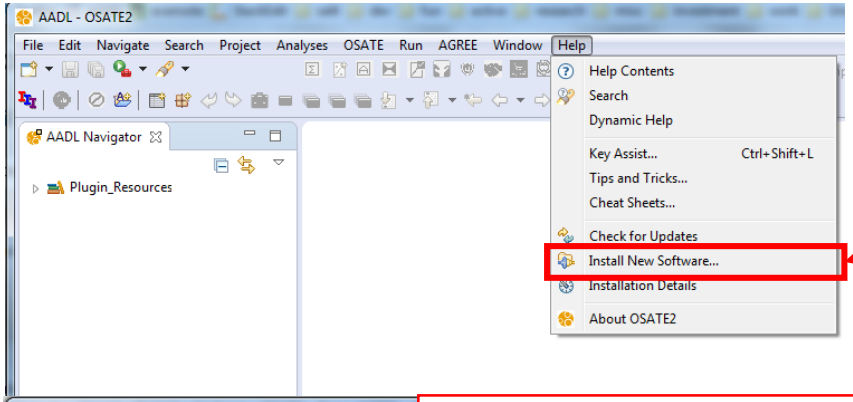
Install security tools, check OSATE experimental update site

- http://www.aadl.info/aadl/osate/experimental/

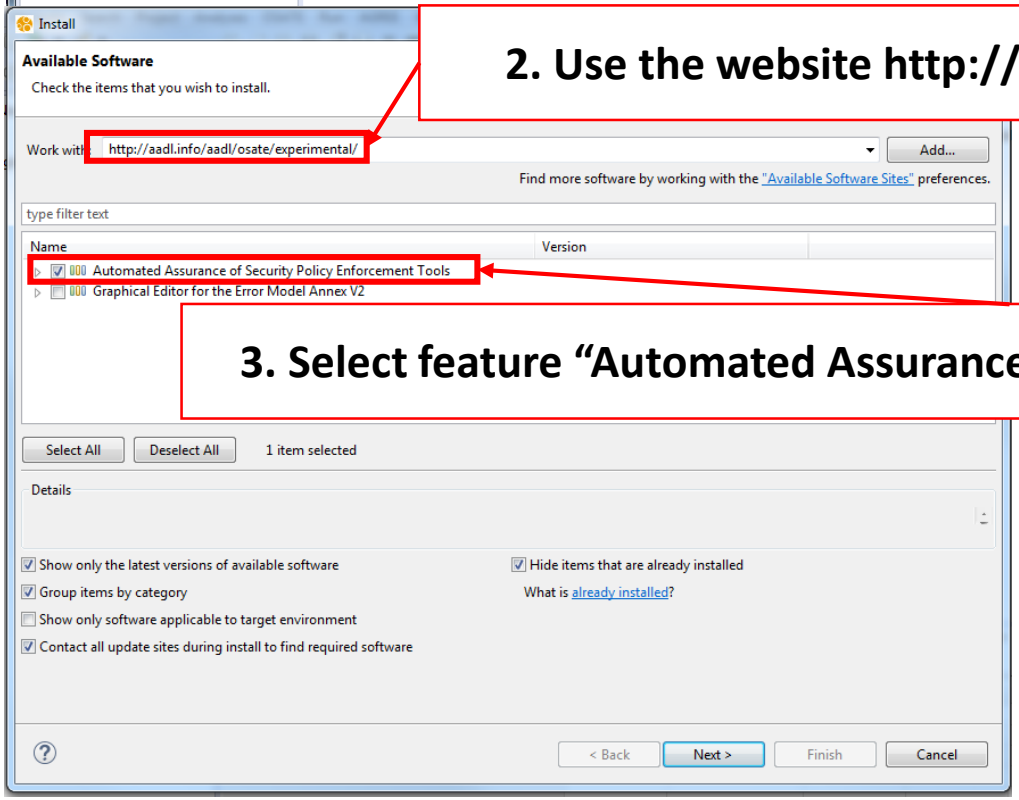
Example models on OSATE github examples repository

- Example are on https://github.com/osate/examples/tree/master/esweek2016-tutorial
- Close the following repository https://github.com/osate/examples.git

How to install security tools?



1. Select "Install New Software…"



2. Use the website http://aadl.info/aadl/osate/experimental/

3. Select feature "Automated Assurance of Security Policy Enforcement Tools"