FROM RESEARCH TO INDUSTRY

cea tech

Sim@SL : Simulation niveau système pour applications industrielles

Hadi Zaatiti and **Daniela Cancila,** Phd

Software Modules for System Security and Dependability Laboratory (L3S)
Architecture, IC Design & Embedded Software Division
Computing and Digital Systems Department

daniela.cancila@cea.fr

www.cea.fr

leti & list

CEA LIST

Outile

- Cyber Physical Systems
  - Examples, Main properties
- The importance of being a 3 dimensional tool
- Introduction of contract-based design in the 3D
- Demo
- Conclusion

What is a Cyber-Physical System?

Number of distributed and connected embedded systems is increasing

We are witnesses of a historical change in society

Technology is pervasive

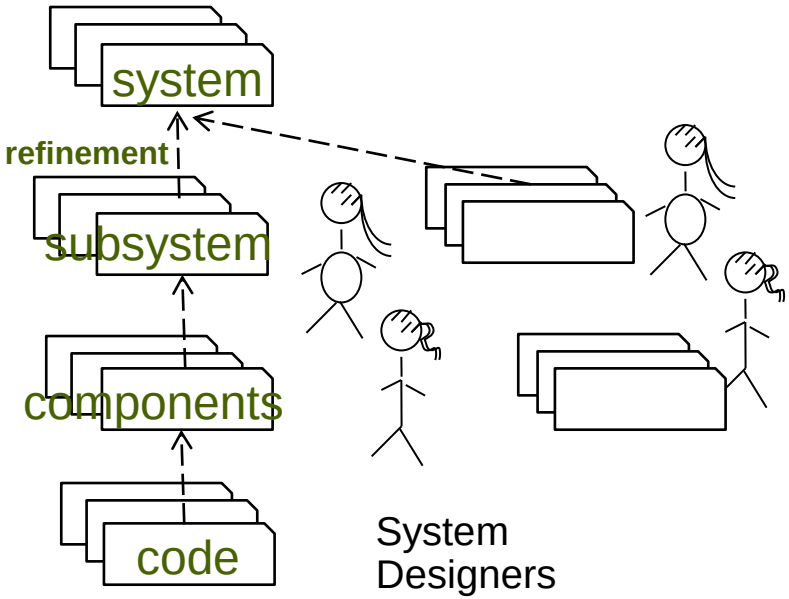
Properties of a CPS

- Autonomy
  - the system's ability of “being sufficiently independent in controlling its own structural and behavioral properties” [Cyphers]

Properties of a CPS

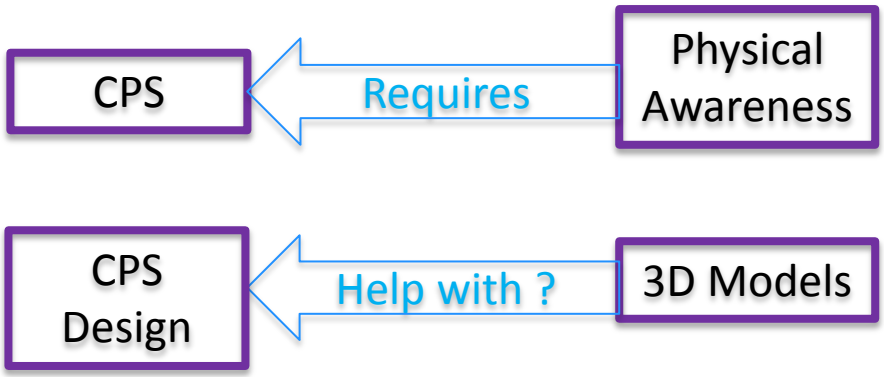
- CPS involve mixed-criticality

- mixed-criticality impacts
  - safety and certification
  - design



How we can deal with CPS?

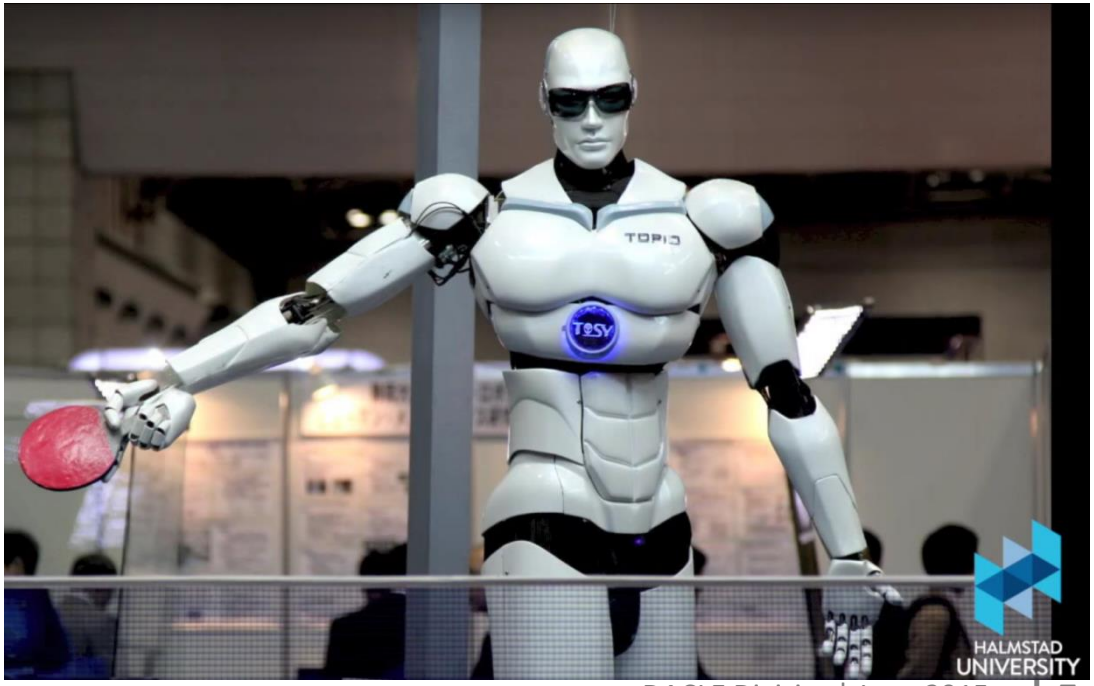
- CPS involve disruptive technologies



W. Taha

http://www.cs.rice.edu/~taha/

http://www.effective-modeling.org/p/walid-taha.html



3D and Contract based Design

- We need combine 3D with formal methods to address “properties”

- Contract-Based Design Approach
  - Individual components with safety-related, included timing, properties specified via *contracts*

Contract Based Design

- A contract is a pair assumptions and guarantees

- A component is fully defined by their assumptions and guarantees
  - guarantees are the services which are provided by a component to its environment
  - Assumptions are those services which are required by a component from its environment to accomplish its guarantees

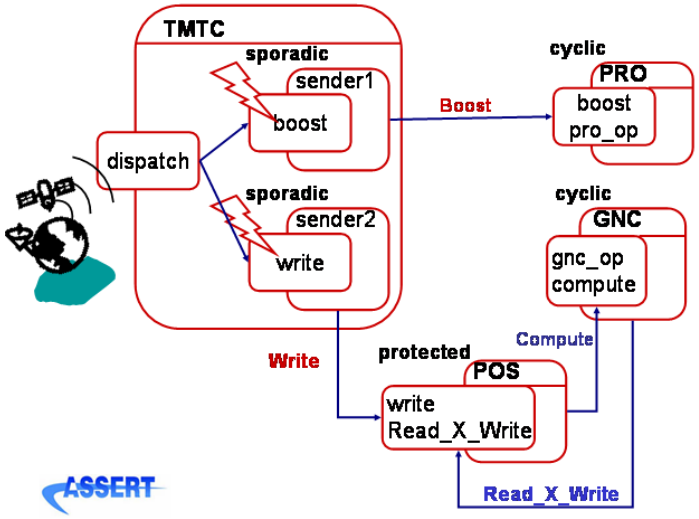
Consider two interface automata $P = \langle V_P, V_P^{init}, \mathcal{A}_P^I, \mathcal{A}_P^O, \mathcal{A}_P^H, \mathcal{T}_P \rangle$ *and* $Q = \langle V_Q, V_Q^{init}, \mathcal{A}_Q^I, \mathcal{A}_Q^O, \mathcal{A}_Q^H, \mathcal{T}_Q \rangle$. *A relation* $\preceq \subseteq V_P \times V_Q$ *is an alternating simulation relation from* Q *to* P *if for all* $v \in V_P$ *and* $u \in V_Q$ *such that* $v \preceq u$ *we have:*

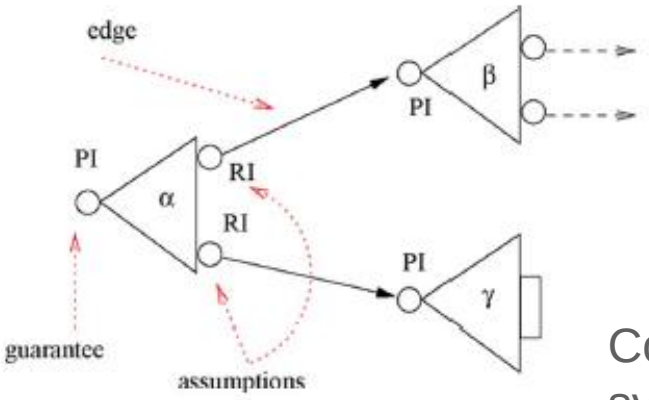
1. *for every* $(u, a, u') \in \mathcal{T}_Q^O$, *there is* $(v, a, v') \in \mathcal{T}_P^O$ *such that* $v' \preceq u'$;
2. *for every* $(v, a, v') \in \mathcal{T}_P^I$, *there is* $(u, a, u') \in \mathcal{T}_Q^O$ *such that* $v' \preceq u'$;
3. *for every* $(u, a, u') \in \mathcal{T}_Q^H$, *there is* $(v, b, v') \in \mathcal{T}_P^O$ *such that* $v' \preceq u'$.

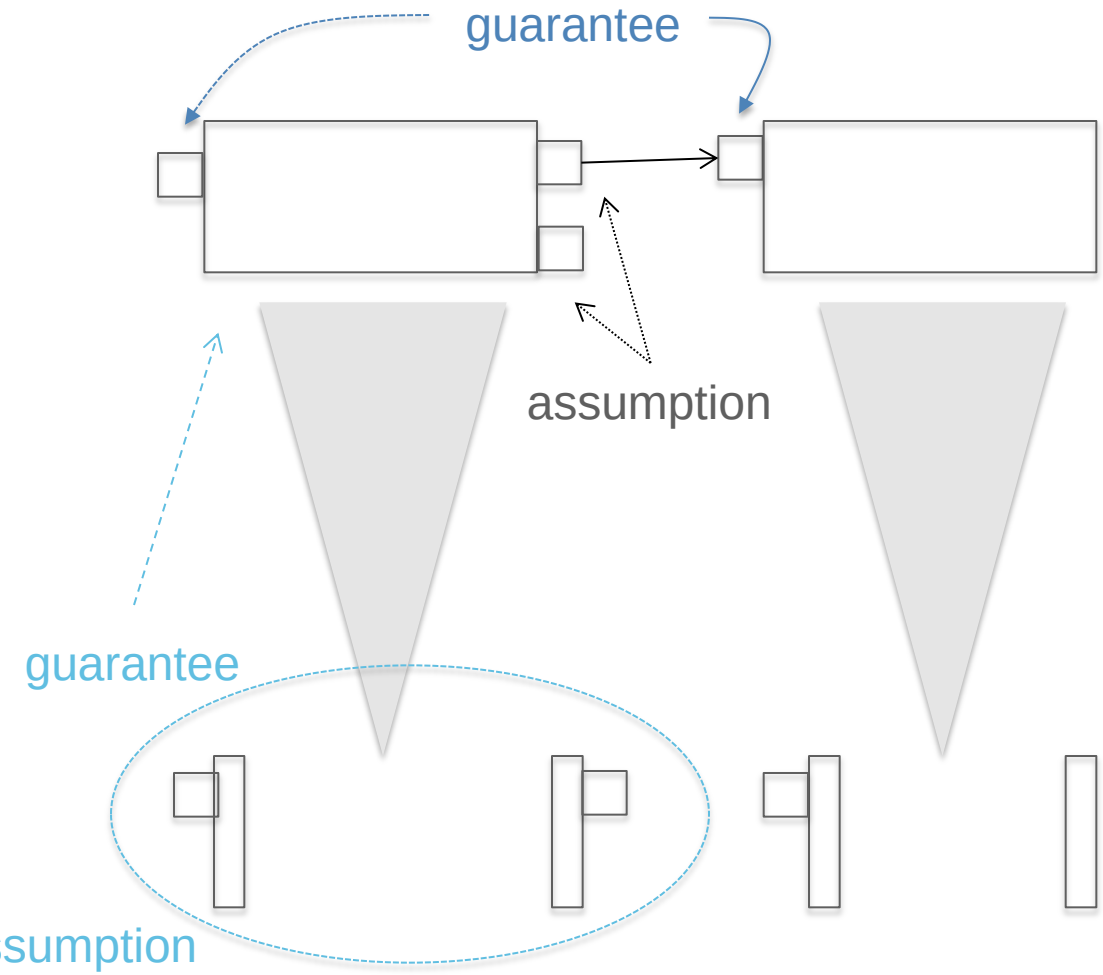
The interface automaton Q *refines the interface automaton* P, *written* $P \preceq Q$, *if there is an alternating simulation relation* $\preceq$ *from* Q *to* P, *together with* $v \in V_P^{init}$, $u \in V_Q^{init}$ *such that* $v \preceq u$.

Interface Automata. Luca De Alfaro and Tom Henzinger.

Example

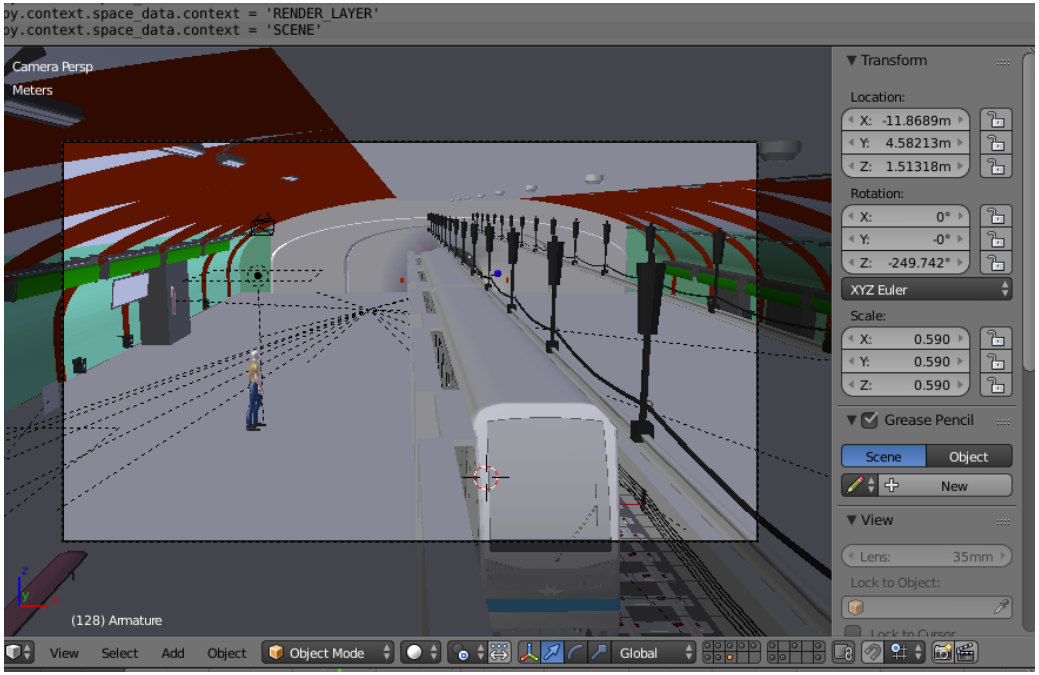




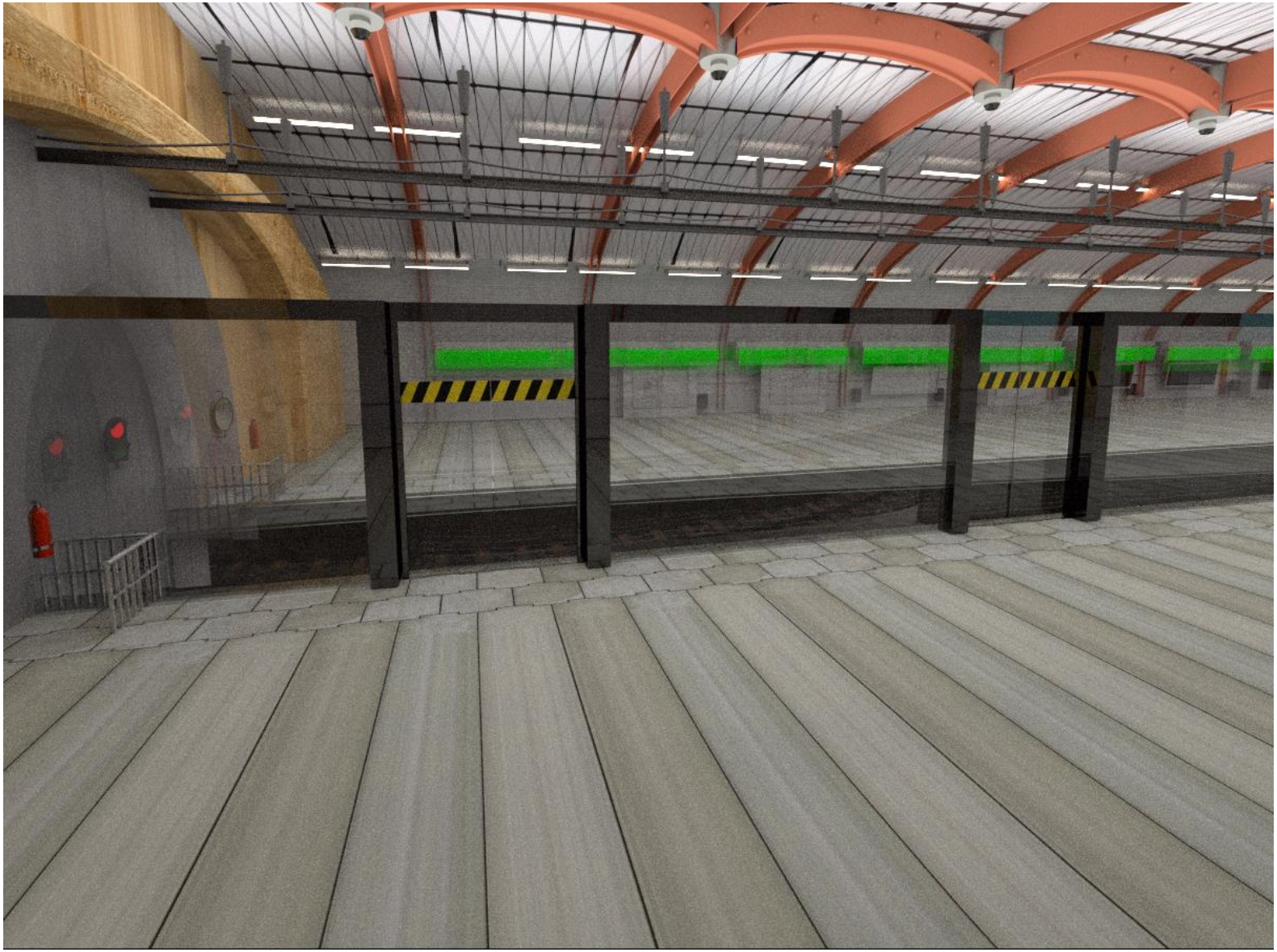


Code ravenscar is a tailored Ada profile to real-time systems

3D model



Video



Conclusion 1/2

- Fact: CPS is becoming a *must* in our society
  - 3 dimensional scenarios
  - Integration of human factors
  - Integration of contracts in the 3D

- Main goal: Advocating in CPS to respond to the needs of society and industry

Conclusion 2/2

eit Digital

CPS Summer School 2016

Thank you!

Challenges for Dependable and Cyber-Physical System Engineering - DeCPS

THALES

cea tech

SystemX
INSTITUT DE RECHERCHE TECHNOLOGIQUE

AXIOM

INTO-CPS

MERGE
SAFETY & SECURITY

CONCERTO

PROXIMA