My Biased (UTRC Centric) View of RC and EI

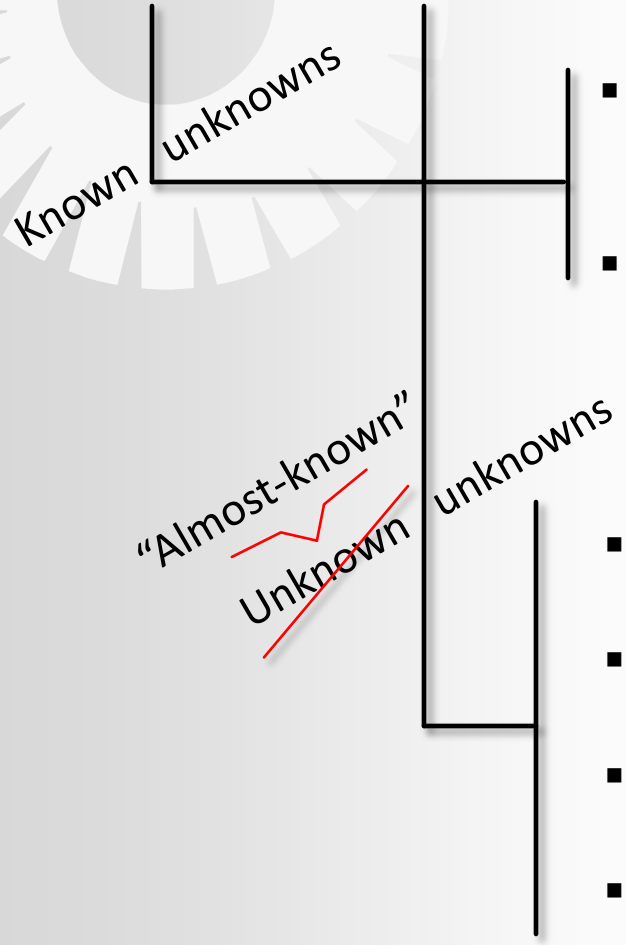
Alberto Speranzon

United Technologies Research Center

FORCES Meeting
June 16-17, 2014

Challenges from Industrial Perspective

- Robust ? …. Resilient?



- This is generally simpler to motivate and is fairly well understood by Business Units
- Aerospace generally more advanced than commercial
- It is believed to be a need …
- … however there is not agreement on why …
- … and if one finds agreement on why …
- … resilient to **WHAT** ?

Resilient to WHAT …

- Roughly this boils down to put the "right values" to the parameters of the following equation

$$Risk = Probability \cdot Impact$$

"Easy sells":

- Power network under attack: Likelihood small
  Impact humongous
  Risk is very High

"Medium ones":

- Aerospace, Physical security systems, Autonomy

"Difficult ones":

- HVAC, Elevators

- **What are the "right" models ?**

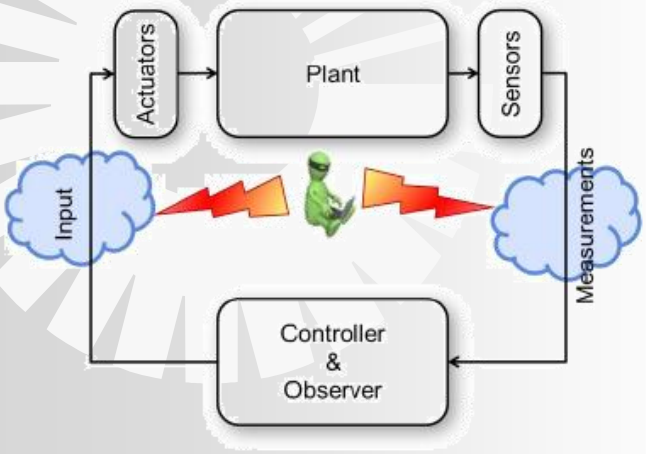
… and maybe more importantly …

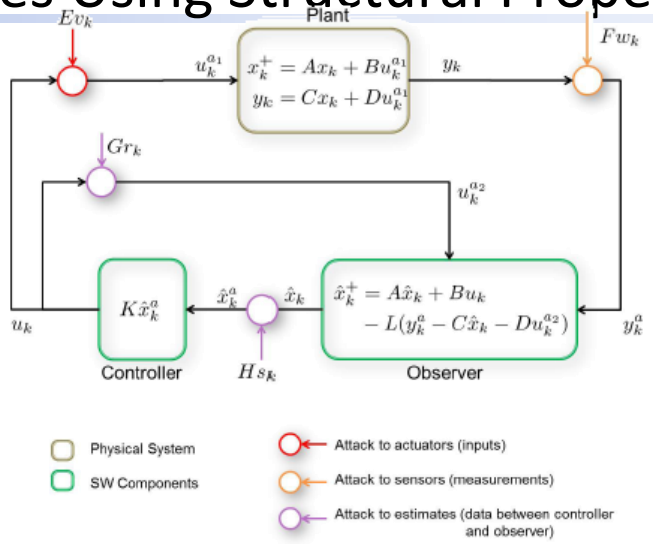
- **What is the "right" metric ?**

Important Aspects for Resilient Control

- Models of “unknown unknowns” VS model of the system
  - What if the system has very complex dynamics that we (designers) only partially understand? How can we detect the system is under “attack” ?
  - What if the system is under-instrumented and/or under-actuated ? How can we detect and react ?
- Design more than analysis
  - Good to know that some “unknown unknowns” can create “issues” … how do we design resilient system ?
- Design space exploration
  - Optimal solution is generally not very good in an area where graceful degradation of performance is all one can promise
  - How much will it cost to update the system to be resilient VS how much resilient will it be ?

Example:
Design of Stealth-Attack Cyber Defenses Using Structural Properties





Theorem (Necessary and sufficient condition)

*Stealth attack exists ⇔ **D** is full column rank*

$$\mathbf{A} = \begin{bmatrix} A & BK \\ -LC & A + BK + LC \end{bmatrix}$$

$$\mathbf{B} = \begin{bmatrix} BE & 0 & 0 & BH \\ -LDE & -LF & LDG + BG & BH \end{bmatrix}$$

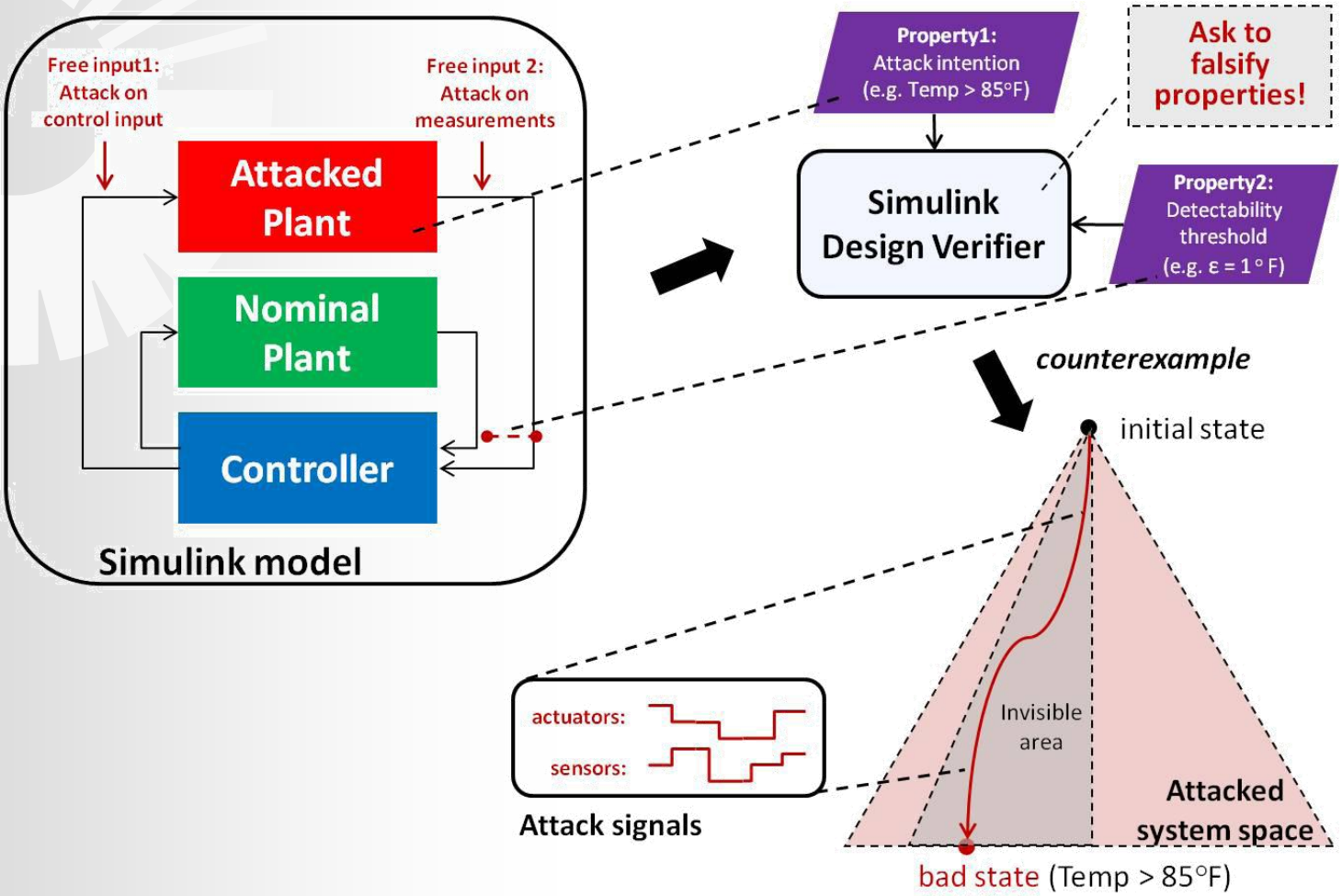
$$\mathbf{C} = \begin{bmatrix} C & DK \end{bmatrix}$$

$$\mathbf{D} = \begin{bmatrix} DE & F & 0 & DKH \end{bmatrix}$$

- Need to ensure cyber defenses are allocated to the information channel from controller to observer
- Then, select sensors/actuators to secure so that *D* has full column rank
- Useful for legacy systems

S.D. Bopardikar and A. Speranzon, "On Analysis and Design of Stealth-resilient Control Systems", Resilient Week, 2013

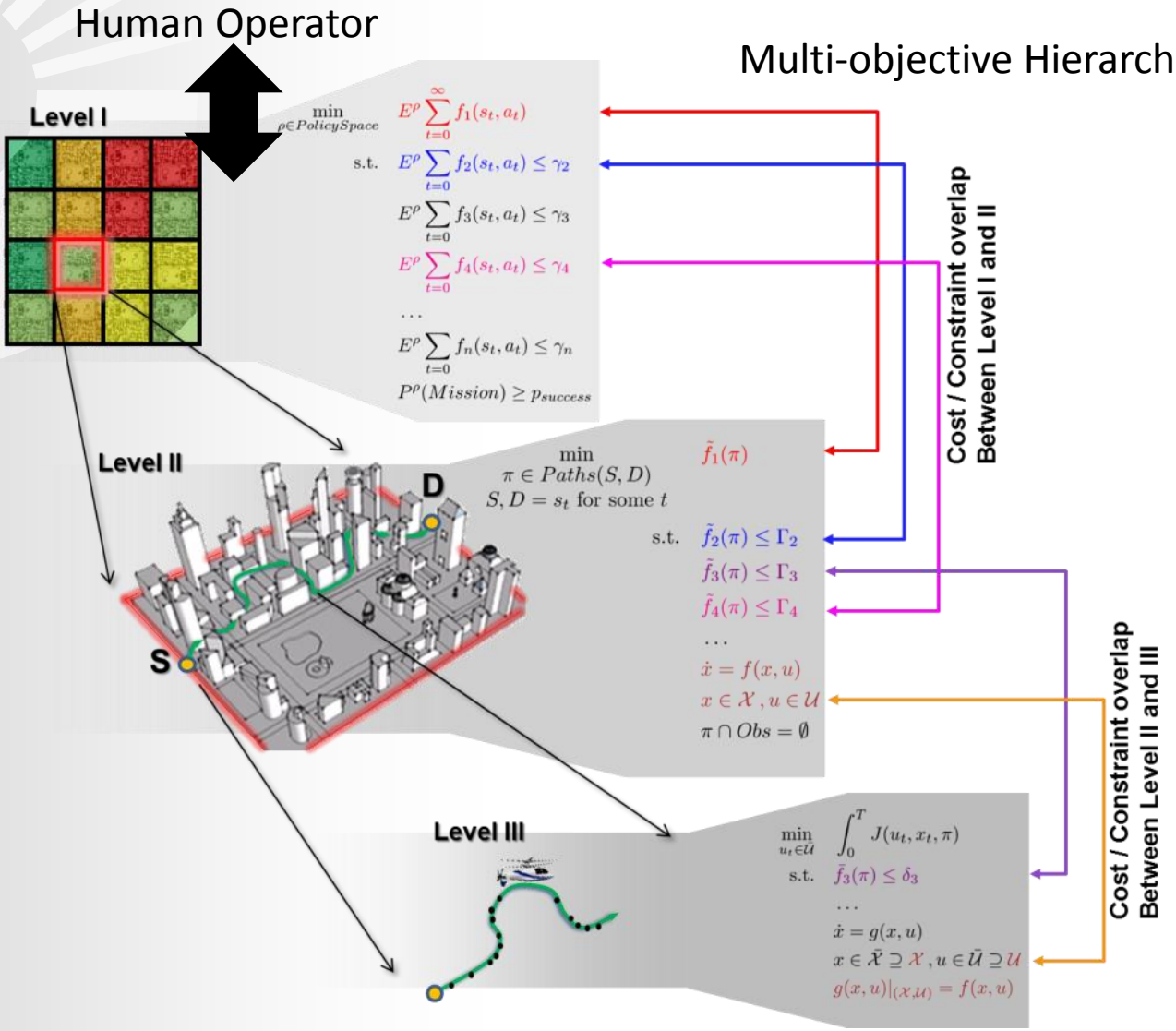
Example: Extension to Nonlinear/Hybrid Systems



Use of a branch-and-bound method to decide what sensors/actuators to secure

N. Trčka, M. Moulin, S. Bopardikar, A. Speranzon, "Formal Verification Approach To Revealing Stealth Attacks on Networked Control Systems," HICoNS'14

Example:
Contingency (Resiliency) Management in Autonomous Systems



X. Ding, B. Englot, A. Pinto, A. Speranzon and A. Surana, “Hierarchical Multi-objective Planning: From Mission Specifications to Contingency Management”, ICRA 2014

Economical Incentives

- Human aspects are becoming increasingly important
- Autonomy is driving the research at UTRC in interface design, attention allocation, V&V, etc.
- No much internal research on incentives

Open question:

- Incentives VS peer pressure
- How does one create “persistent” incentives? What are the “dynamics” of incentives?
- Privacy concerns

Example: Economical Incentives For Comfort

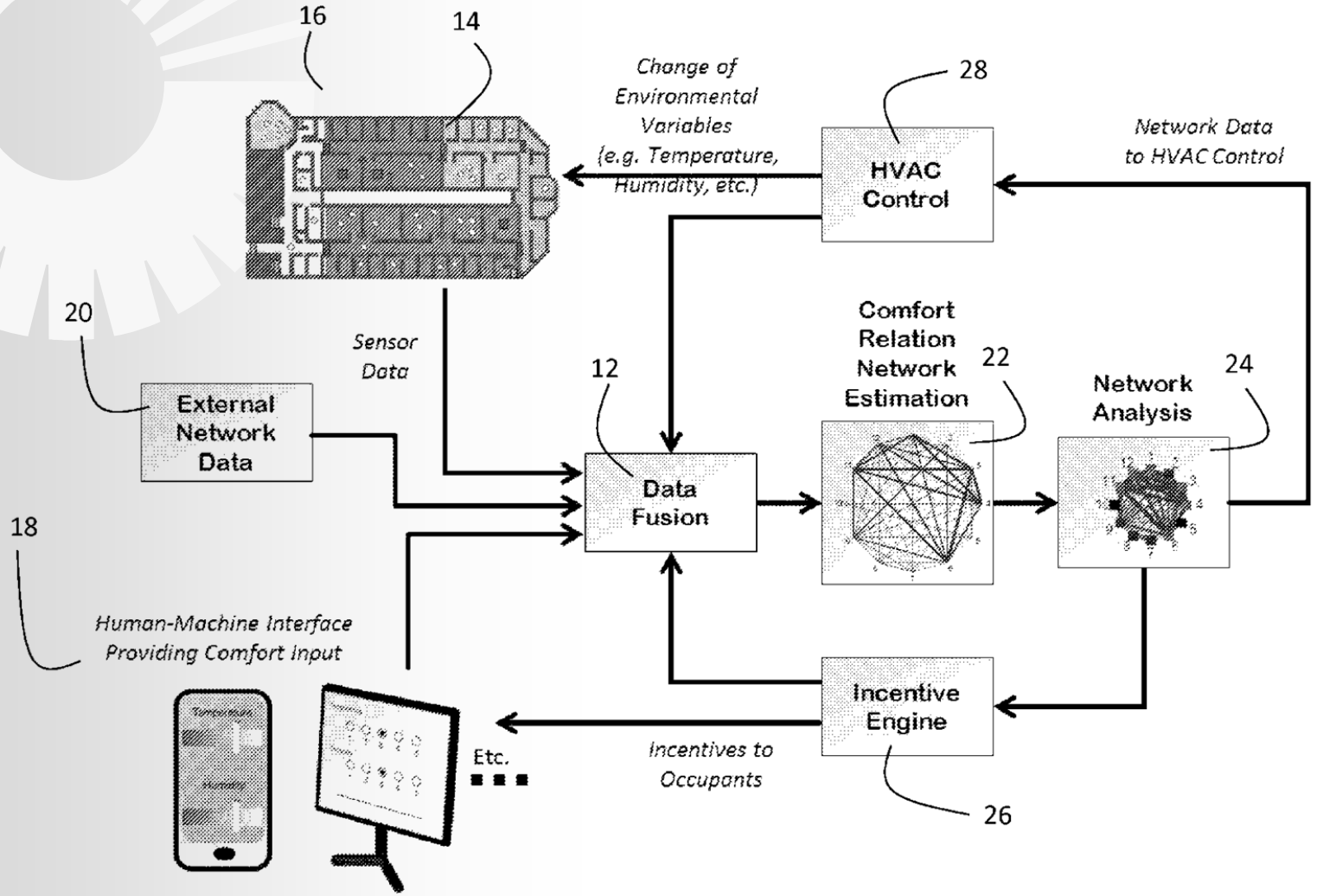


FIG. 1

A. Speranzon, T. Sahai and A. Banaszuk, "Comfort Estimation and Incentive Design For Energy Efficiency", WO/2014/084832, Patent Application

Conclusions

- FORCES aims at tackling very hard problems
- Not only there are no design tools but even a theoretical framework that combines RC and EI is missing
- Game theory and mechanism design seem to provide the right framework to tackle these problems:
  - Enables to consider both cyber and physical aspects
  - Not only analysis but also design
  - Challenge: computation …