

# Design of Integrated Networked Embedded and Dynamical Systems

A Position Paper

Submitted To  
The National Workshop on  
**Beyond SCADA**  
Networked Embedded Control for Cyber Physical Systems  
November 7–8, 2006

Andrzej Banaszuk  
United Technologies Research Center  
BanaszA@utrc.utc.com  
860-610-7381

Clas A. Jacobson  
United Technologies Research Center  
JacobsCA@utrc.utc.com  
860-610-7652

Jerrold Marsden  
California Institute of Technology  
marsden@cds.caltech.edu  
626-395-4176

Igor Mezić  
University of California, Santa Barbara  
mezic@engineering.ucsb.edu  
805-893-7603

Alberto Sangiovanni-Vincentelli  
University of California, Berkeley  
alberto@eecs.berkeley.edu  
510-642-4882

# 1 Summary

The current practice of engineering control systems for physical systems that utilize distributed embedded systems for implementation cannot cope with the complexity demanded by cyber-physical applications. The applications are dominated by overlapping dynamics of the physical processes under control and the dynamics of the computational and communication systems underpinning the control implementation. Moreover, the increased spatial connectivity presents unprecedented complexity in the design and implementation of control systems. The current design methodologies cannot consider a priori sources of uncertainty that must be addressed in the design process to ensure robust operation. The need is to develop technology roadmaps and research programs that include the elements of (a) design flows with tool chains that can address the spatial and temporal complexity, (b) multiscale modeling and analysis tools that specifically include dynamics of the physical as well as embedded software systems and (c) methodology to include uncertainty in the modeling and analysis.

## 2 Situation

In the traditional top-down approach to the design of control systems for physical systems the embedded controls and communication networks are typically designed and implemented in an ad hoc way at the end of the design cycle. A typical — and often implicit — assumption is made in design that justifies a purely top-down approach is that the computation and the network dynamics are orders of magnitude faster than the dynamics of the physical world and that the communications are reliable. However, there are many examples of the deployment of networked embedded systems in which the time scale separation assumption was not achieved and network communication latency caused systems failure. The failure was only discovered late in the design cycle where hardware was deployed and resulted in costly redesign and redeployment.

Moreover, in many emerging applications for networked embedded systems that are found in diverse application areas including aerospace, automotive, and building security, the time scale separation and reliable communications assumptions that have been made to date can no longer be justified. For instance, consider an embedded real time emergency response system designed for fire protection. Such an emergency response system found in buildings will include signal processing and data fusion from many distributed heterogeneous sensors, for example, video cameras and smoke detectors. It could also include model based estimators of fire and smoke propagation and tracking the locations of people. This information is vital to provide solutions that are based on algorithms to control fire suppression, smoke fans, and active signaling systems tasked to optimally routing people to safe exits. A challenge is the complexity of such a networked system in terms of the number of sensor and actuator points as well as the spatial extent of the problem domain. A more fundamental issue is that, given the fact that the system is spatially distributed and evolving on very fast time scales that involve both smoke and people dynamics, a distributed embedded system is necessary to implement the estimation and control functionality. The dynamics of smoke and people egress ranges from seconds to minutes and, at least for low bandwidth wireless or inexpensive wired networks, the communication latencies are in the same range. Hence, for this

example, which can be expanded to the broader situation of protecting critical infrastructure, the fire suppression and evacuation performance cannot be guaranteed without taking into account the latencies in the implementation in the networked embedded system of the desired estimation and control function.

A method to enforce time scale separation is to utilize fast computation and expensive high bandwidth networks. This solution though does not scale up as complexity increases, moreover, for widespread implementation such an approach does not present an economically viable approach for most commercial applications where increased functionality must be provided. Moreover, the communication delays across the networks will scale linearly with the size of the network. In the early stages of design for networked systems that fully exploit the potential of information technology — networks and increased sensor coverage at low cost — the latencies associated with distributed embedded systems will impose constraints on the control functionality and will impose fundamental limits on guaranteed performance that must be explicitly addressed.

In addition to the interaction of the physical and network dynamics the design of control systems that provide increased functionality must explicitly address the significant challenge of managing uncertainty. There is the stochastic nature of the dynamics (for example the behavior of people), unreliable communications (interference, congestion, node failure), and often uncertain computing platforms (especially in early design). Sampling-based methods (e.g. Monte Carlo) are used in many cases to estimate average performance. Unfortunately these methods are not feasible when addressing large software intensive systems as they suffer from the curse of dimensionality.

Finally, the current situation in the area of design methodologies cannot cope with the network design problems. A general method for the design of distributed embedded systems, namely, platform based design is a design methodology that is able to cope with the spatial and temporal complexity of large heterogeneous systems by abstracting the functionality and the available architectures for implementation to focus on critical points in the design chain. However, the current state of the design methodology has not had a wide applicability in what could be termed communication based design — meaning that the networks used for sensing and actuation are critical — which can be utilized for the design of control systems of spatially interconnected and complex physical systems.

### **3 Problem**

There is currently a lack of model based design methodologies that could provide guaranteed performance for complex networked embedded systems for control of physical systems with complex spatially distributed dynamics operating in uncertain environments. The cyber-physical systems in the general area of providing security to critical infrastructure — extending from the fire situation outlined above — are likely to emerge as dominant applications that exhibit dynamic behaviors that are more complicated than the individual component behavior; that is, the system has emergent behavior arising from the interconnections that define the system. In fact the desired network behavior often involves complex non-equilibrium dynamics (for example building or more generally city evacuation in the case of a dynamically evolving threat). The problem is that the

non-equilibrium dynamic behaviors of very large systems are at best difficult, if not impossible, to predict and control with the current analysis methodology. The situation is compounded when uncertainty is considered in the analysis or, also importantly, is considered in the design of networks that are robust against the uncertainty. Analytical methods as well as the supporting computational infrastructure for guaranteeing performance and robustness of large dynamic networks in the presence of uncertainty simply do not exist.

The analysis required to guarantee robust performance of cyber-physical systems currently relies on exhaustive high-cost simulation but has no guarantee of providing insights into the worst-case situations where failure occur. To locate these sensitivities, analysis should complement simulation capabilities. In general, the analysis targets worst and average cases, with specific attention to the probability distribution functions, which are providing significantly more detail about the Quality of Service (QoS) provided by a component, module or system. The current analysis also neglects the specific interconnection structure inherent to the cyber-physical network. This simulation approach results in an inability to predict the root cause of malfunctioning. Deriving bounds on available QoS from several perspectives (e.g. communication, and computation) is necessary but not sufficient. In addition, the certification or approval processes applied today to highly-integrated systems are not sufficient and other approaches must be considered.

Examples in nature such as the dynamics of DNA and other biomolecules and in engineering, such as suppression of oscillations in jet engines (flutter and screech) show how important the intrinsic dynamics enabled by physical interconnections of systems are. Modern designed networks typically include IT, in addition to physical interconnections. Often because of non-integrative design procedures, one can only do so much with control wrappers to correct design defects. The software tools chosen to address such problems must have dynamical and optimization capabilities that produce fast and reliable coarse simulations that are robust to uncertainty and noise; they must be compatible with the problem at hand, such as having accurate energy behavior for relatively long time simulations, even if the simulation is coarse; and they must be capable of reliable, parallelizable, asynchronous, refined simulations once a design has been chosen. In addition, there must be theoretical insight into the expected intrinsic dynamical behavior and how this may be captured by an integrated software infrastructure and controlled using sensors and actuators that work in concert with the natural dynamics of the system.

## 4 Need

The integrated design of all the components of the cyber-physical systems must be addressed from the beginning of the design cycle. The design and optimization of future complex networked embedded systems for control of physical systems with complex spatially distributed dynamics will require the tight integration of information technology (IT) systems (including multi-scale modeling and simulation of the physical and embedded and software subsystems as well as control algorithms which can be used at different stages of design with consistency, the computational architecture that is chosen for implementation of algorithms, and the network communications which link the sensing and computational elements) with control, and the underlying dynamics of

the application. Most importantly, the system's intrinsic physical dynamics is strongly coupled to the networked embedded system dynamics via the interconnection structure.

## 5 Elements Of A Technology Roadmap

A National need is to develop a technology roadmap to address the technology gaps for the control of complex systems as found in the security of critical infrastructure. The need is to develop an integrated and multi-scale modeling, analysis, simulation, and design tool set for large heterogeneous cyber-physical systems enabling — via computations of order significantly smaller than  $N^2$  determined by the  $N$  network connections — robust execution of dynamic missions in presence of model uncertainty.

Specifically, the gap must address that of *design flows, multi-scale modeling with emphasis on dynamics* and *explicit methods that address uncertainty to ensure robust operation*.

Elements must be present in each area as follows.

### Design Flows.

- Design methodologies must specifically include both physical and IT elements;
- Design flows must contain levels of abstraction to enable software reuse and to reduce complexity of design through a systemic reduction of design choices.

### Multi-scale modeling with emphasis on dynamics.

- A unified modeling, simulation and optimization framework that includes interconnected models of physical components, computations, and communications;
- A probabilistic description of dynamically evolving variables;
- Graph theoretic description of the network and their coupling to dynamical systems methods for analysis of emergent phenomena and robustness;
- Asynchronicity in computation and communication.

### Uncertainty analysis and control design and analysis.

- Uncertainties in location and communication mechanism of physical components;
- Stochastic fluctuations of wireless channels throughput resulting in attenuation, interference;
- Robustness to disturbances,
- Reconfiguration to provide robustness to loss of sensors; computational nodes, and communication links;
- Seamless incorporation of new sensing or computing agents;

- Enabling multiple modes of operations including seamless switching (example: building control systems switching from energy and comfort optimization to evacuation control);
- Characterization of fundamental limitations on performance.

## **5.1 Challenge problems and hardware demonstrations**

A series of challenge problems should finalize with a model-based design of a cyber-physical systems using uncertain models and communications, complex computations, and performing a mission involving complex non-equilibrium dynamics. Two challenge problems are proposed: design of building evacuation control and design of an autonomous transportation network. An ultimate challenging problem that encompasses both is a city evacuation control.