

Formally Verifiable Architecture Patterns for Safe Medical Device Plug and Play (MD PnP)

NSF CPS Research Planning Workshops have identified that compositional system modeling, analysis, synthesis, and integration are at the frontier of engineering sciences. At the center of this development is the current transition from a reductionist approach to a compositional approach in engineering and science. The science of system composition has clearly emerged as one of the grand themes driving many of our research questions in networking and distributed systems. By *system composition* we mean that the QoS properties and functional correctness of the system can be derived from the system architecture structure, and the functional and QoS properties of constituent components.

Medical systems are an important class of network-controlled reconfigurable CPS systems with a high degree of complexity. Each year thousands of patient injuries and near-misses are caused by improper or unsafe medical device-device and/or device-human interactions. The Institute of Medicine (IOM) report¹ revealed that at least 98,000 annual hospital deaths are attributable to medical errors.

Networked medical devices systems have both loosely coupled and tightly coupled subsystems, including infusion pumps, respirators, robot-assisted surgery devices, monitoring and diagnostic devices, as well as medical information systems, and medical personnel. They have different degrees of safety, reliability and real time requirements. For example, after major surgery, a patient is allowed to "operate" an infusion pump with potentially lethal pain killers (patient controlled analgesia (PCA)). When pain is severe, the patient can push a button to get more pain medication. The use of PCA devices is an integral part of modern post-operative care. This is an example of a safety critical device controlled by a non-safety critical and error-prone operator (patient). In spite of operator errors, the operation of PCA system must be verifiably safe. Furthermore, the role of each device and their QoS requirements will change at different stage of a medical procedure. This raises many system composition challenges.

At the heart of compositional research is the development of formally specified and verified architecture patterns that can be deployed at scale. An architectural design is mature only if, under the proposed architecture, system requirements will be met without significant changes to component definitions, to interfaces and to the rules of interactions (protocols) during the development process. That is, lower level designs and implementations can unfold as planned. Matured software architectures are characterized by explicit stated assumptions and properties that we can predict and formally verify. In this regard, most building architectures are mature, while most software developments are not supported by matured architecture design patterns.

However, when there are no architecture patterns to follow, even in a matured engineering discipline, the system development is facing serious problems, such as the Tacoma bridge collapse² and the Sydney Opera House cost and schedule overrun³.

It is vital for our nation to develop the scientific and technological foundation upon which formally specified and verified MD PnP architecture patterns can be developed and deployed at

¹ Kohn LT, Corrigan JM, and Donaldson MS, eds. *To Err Is Human: Building a Safer Health System*, The National Academies Press, 2000.

² <http://www.wsdot.wa.gov/tnbhistory/Connections/connections3.htm>

³ The adjusted cost of the building increased almost fourfold, from 15 to 55 million Australian dollars - 20 million before Utzon's departure and 20 million after.

http://www.gsd.harvard.edu/research/publications/hdm/current/21_tombesi.html

scale. To this end, we need a national research initiative that includes medical community, computer science community, engineering community and the FDA to jointly develop:

- Domain models for dynamic composition (MD PnP), which capture the structure and dynamics of requirements and their changes during medical procedure workflow⁴.
- Advanced technologies to integrate the operational context with low level alarms to provide timely “situational awareness” for medical personnel, because operational contexts are different at different stages of a complex medical procedure.
- A coherent suite of formally verified QoS protocols for each domain model. We need to develop cross domain QoS protocol interferences model and then formally verify that candidate protocols for different QoS dimensions will not interfere with each others.
- Formally specified and verified architecture patterns that can ensure system level safety in spite of the faults and failures in non-safety critical components, because complex and unverifiable components, e.g., human operator and certainly highly complex (legacy) software components are difficult to avoid.
- Evidence based certification that utilizes formally specified and verified architecture patterns.
- Computer-aided configuration time verification tools to ensure that dynamically configured medical device networks is compliant with formally verified and certified architecture patterns.