Reconciling Safety with the Internet for Cyber-Physical Systems

Submitted by Edward Lee on Tue, 01/22/2019 - 7:46pm. Contributors:
Edward A. LeeMarten LohstrohMatt Weber

Overview. The Internet of Things (IoT) leverages Internet technology in cyber-physical systems, but the protocols and principles of the Internet were not designed for interacting with the physical world. For example, timeliness is not a factor in any widespread Internet technology, with Quality-of-Service (QoS) features having been routinely omitted for decades. Nevertheless, properties of the Internet could prove valuable in CPS, including a global namespace, reliable (eventual) deliv-ery of messages, end-to-end security through asymmetric encryption, certificate-based authenti-cation, and the ability to aggregate data from a multiplicity of sources in cloud-based warehouses. This proposal leverages recent developments that hold promise to bridge the gap, enabling the use of Internet technologies even in safety-critical, timing-sensitive applications such as factory automation and transportation. Specifically, we leverage time-sensitive network (TSN) technol-ogy; the use of smart gateways to isolate safety-critical services from best-effort services and to provide local proxies for cloud-based services; locally centralized, globally distributed authenti-cation and authorization; and the development of coherent time-based semantics for distributed real-time services. The focus of this project will be on sound concurrent models of computation, on type-theoretic methods for ensuring correct composition, and on the realization of these for-malisms in a software architecture that reconciles widely-used mechanisms in Internet services to hide uncontrollable latencies with the need for repeatable, testable, and robust real-time services in safety-critical systems. An open-source reference implementation will be delivered together with analytical papers on the formal properties of the models.

Intellectual Merit. Concurrency models used in Internet computing focus on hiding latency, whereas concurrency models used in safety-critical systems focus on determinacy, predictabil-ity, and timing. Although these methods have developed largely independently, we believe they can be reconciled. We intend to demonstrate this reconciliation by building open-source software that makes the best of both worlds accessible to application designers. We will approach this problem by focusing on the mathematical models and analytical tools that can bring these worlds together and on encapsulation of these models in executable software. The goal of the software framework is to gently introduce application designers to a new and rigorous paradigm of design. The overarching goal is friendly and accessible principled and verifiable design.

Broader Impact. Cyber-physical systems have exploded in the research and industrial landscape with the sudden sustained hype around the Internet of Things (IoT) and Smart Cities. This has drawn many creative people into the field, people who often have little training in security, safety, and real-time software. When poorly designed cyber-physical systems proliferate in our environ-ment and culture, we open ourselves to disastrous failures and to malicious misuse of the technol-ogy. While it is true that good tools do not automatically lead to good designs, it is also true that bad tools ensure bad designs. CPS and IoT designers today are using almost exclusively tools that have been designed for entirely different purposes such as Internet computing and information processing. The goal of this project is good tools, specifically ones that encapsulate state-of-the-art methods, that are accessible to creative non-experts. These tools will be open-source and usable in education and industry. Most importantly, by making friendly and accessible software tools and a truly cyber-physical regression testing framework, we will encourage creative people who may otherwise face insurmountable technical challenges to leverage the Internet of Things.

Keywords: IoT, software engineering, concurrency, safety-critical systems, design tools. **Primary Research Target Area:** Engineering of Cyber-Physical Systems

Edward A. Lee | Marten Lohstroh | Matt Weber

Other available formats:

Reconciling Safety with the Internet for Cyber-Physical Systems
Switch to normal viewerSwitch to experimental viewer

IoT software engineering Concurrency Safety-Critical Systems design tools CPS-PI Meeting 2018 2018 Poster Posters (Sessions 8 & 11) 1836601