Dependable Embedded Systems and Services: A Personal Crystalball Outlook

Neeraj Suri
Department of Computer Science
TU Darmstadt, Germany
Email: suri@informatik.tu-darmstadt.de

Abstract

The concept of embedded systems gets transformed as one starts considering their increasing usage in a networked information technology world. This write up outlines some corresponding and emerging research areas that arise when dependability is interlinked as a fundament for embedded system operations.

1. Introduction

The ubiquity of computing devices in daily life (banking, e-commerce, communication, transport, medical etc) that drives the Information Society (IS), also implies that the real value of the services they deliver arises, in part, based on the dependency (real or perceived) we are willing to put into them i.e., the implicit or explicit assurance of trust we put in them for sustained delivery of desired services. In a very fundamental sense, the IS helps transcend the archaic connotation of embedded systems to be hardware intensive and standalone computing devices to the wider notion of "**embedded services**" spanning distributed or networked connectivity. Basically, computing technology per se is just the facilitator behind embedded systems and services; it is the impact and provisioning of "dependable and usable" services to the user that makes it meaningful for the user to "trust" these services. As before, dependability entails the sustained delivery of services, be they service-critical or cost-critical, regardless of the perturbations encountered during their operation.

We **do** know how to build large, complex and (expensive) customized dependable embedded systems, protocols and perhaps even the basic IS infrastructure. What we still need to develop is how to provide for services, at a level usable to the consumer, that appear simple, usable and dependable hiding the underlying complexity of the IS. Equally needed are generic and structured design guidelines such that embedded systems and services can be developed in an evolvable manner and ideally independent of a specific technology or domain. Of course, the difficult issues are in developing paradigms (yes, this is indeed a paradigm shift from building specific systems) that are (a) generic to support future enhancements of services and technology changes, (b) evolvable to provide for emerging services and (c) cost-effective. As embedded services, it is perhaps easier to articulate the high-level and holistic technological directions that warrant R&D considerations to achieve a dependable IS structure.

The subsequent write up enumerates a short list of topic areas (by no means a comprehensive one) of some emerging challenges in the broad area of dependable embedded systems and services. Three notable exceptions not detailed here, given their broad scope, being SW, Security/Privacy and HCI issues. For brevity, the themes are restricted to Design stage (Composition) and V&V challenges including:

Composition of Services: This is an extensive area which opens the field for an "open and evolvable" IS infrastructure and services. The compositional aspect needs to develop beyond the conceptually simpler (though very challenging) compositional approaches of physical composition to the more abstract nuances of composition of functional and non-functional attributes such as (a) dependability, (b) safety, (c) security, (d) temporal predictability etc. The issues are to ascertain if modularization of entities, reusability of component/functions or even design-experiences even applies to provisioning of services? Can a large IS infrastructure incrementally or compositionally define "safe" blocks such that they add up to a "safe system"? Similarly is time a composable entity that can be abstracted? How do we compose services and components with the intent to obtain "emerging" properties, if attributes of the services being composed are orthogonal in nature e.g., dependability, real-time and performance? Also, how do we compose heterogeneous services such as the integration of services of varied criticality?

Connectivity, Autonomy and Scale: The role of communication media in provisioning of dependable services (and those requiring temporal predictability) over (a) heterogeneous – wired vs. wireless, different protocols – and (b) unreliable media, represents a major R&D challenge with the need being to develop QoS nuances of dependability. The broad arena of sensor networks and smart devices only exacerbates the problems. Going beyond the current definition of smart sensors/smart devices is the area of autonomic computing with fully functional discrete and small smart embedded systems with a high degree of heterogeneity and mobility (a fleet of smart cars and intelligent highways is a trivial and real example). Consider discrete OS kernels in these smart devices. For a loosely structured – dynamic and ad-hoc – communication structure, linking these devices, a case become of individual devices being altering their functionality through on-line upgrades or patches. How does one provide for deterministic properties (temporal guarantees or dependability attributes) in an environment that has mobility, ad-hoc, asynchrony and continual evolvability as its desired "usability" attributes? How does one provide for basic dependability aspects of group communication, data consistency, replica determinism, P2P and similar primitives in a dynamic environment with minimal stable connectivity and communication attributes? How are autonomous devices configured as a group? How do autonomous devices recover and adapt to perturbations in the environment? The support technology of run-time diagnosis and recovery/re-configuration becomes a technological thrust as well. It is equally worthwhile to keep in perspective that the scale of interconnecting smart devices will range in millions and billions rather than the classical smaller scoped academic targets.

SW, SW, SW: This is too large a discipline to discuss here and do even minimal justice to it! As a comment, the classical perception of embedded systems gives the connotation of hardware intensive systems. With SW nowadays pre-dominantly determining system functionality, the challenges of development of robust SW arise. The wide arena of robust SW development – defensive design, wrappers, SW reliability, SW testing, robust/predictable OS and middleware design are just some basic thrust areas to develop.

HW-SW Integration: Classically embedded systems imply hardware intensive functionality. Although SW is determining more and more of the functionality, the performance of SW-based services brings HW actively back in the loop. With embedded systems representing a tighter and tighter coupling of SW and HW for cost, performance or power considerations the meshing of SW and HW keeps increasing. Ironically, a fundamental principle of dependability call for a clear segregation of functions of varied criticality to minimize the impact of perturbations, i.e., minimal coupling. This represents an ongoing dependability challenge of HW-SW integration with the orthogonal constraints of efficiency, performance, dependability etc.

Verification & Validation (V&V) is a standalone topic. The emphasis on modular, incremental and cost-effective V&V techniques for ensuring trust in upcoming dynamic and evolving systems warrants substantial research efforts. Currently, we possess a vast suite of specialized V&V techniques, though they are best suited for static and specific systems, not an IS infrastructure. The role of componentized and still industrial strength formalization of specifications is likely to be a key challenge for being able to conduct efficient and cost-effective V&V for large systems. This is especially true as the safety and security connotations of the IS reach high levels and consequently make the use of conventional V&V ineffective from both cost and coverage perspective. How does one validate and certify services that are based on dynamic, ad-hoc, mobile environments and evolvable components?

IS works based on the user being able to "use" the palette of available and interlinked IS services. In this respect, **Human Computer Interaction** (HCI) is a key research area for its interplay on system dependability (e.g., disruptions, misuse – passive incorrect usage and active security attacks, intrusions etc) and for driving IS utility The links between users and services is a key area, meaning that the users must be able to use the services in a "secure" and "safe" manner, such that they don't pose a threat to the continued provisioning of services by themselves.

The intent has been to articulate emerging topic areas in need of research – a number of themes represent standalone topic areas which have been and are the topic of extensive research. Needless to say, the context of embedded systems and dependability requirements does re-orient a number of existing research thrusts – robust SW development and connectivity being a case in point. This document takes an approach that embedded systems need to be re-thought not just as classical discrete systems but as infrastructure elements and services in the so called distributed networked ubiquitous computing environment.