

## **Shades-of-High Confidence**

*Tariq Samad*

Honeywell Labs, 3660 Technology Drive, Minneapolis, MN 55418

Tel.: +1.612.951.7069

Fax: +1.612.951.7438

tariq.samad@honeywell.com

In approaching high-confidence software and systems (HCSS) from an industry-oriented, practical perspective, I would like to highlight three topics that I believe we in the research community should spend more time understanding and discussing:

- The diversity of HCSS
- The current state of technological sophistication in HCSS
- Guidance for research so it can be relevant to the various industry sectors dealing with HCSS

For present purposes I am considering a system, solution, or product to be “high confidence” if it could directly result in unanticipated “significant” injury, loss of life, or environmental damage. This is not intended to be a precise definition, but I intend it to exclude office automation, for example (carpal tunnel and related neuropathies notwithstanding).

### **HCSS today—extremes of scale, cost, safety and mission criticality**

High-confidence systems include all of the following;

- refineries, chemical plants, water treatment plants, ...
- oil and gas pipelines, power grids, communication networks, ...
- airports, hospitals, schools, ...
- commercial and military aircraft, unmanned aerial vehicles, air traffic management, ...
- automotive systems for safety, emissions, stability, ...
- biomedical implants, assisted living systems, healthcare monitors, ...

All of the above exhibit deep, intricate embedding of software, computing, and networks in physical systems, and the IT content is steadily increasing in all of them. However, these and other systems differ in several interdependent ways, such as:

- **Scale.** A refinery automation system can have 10,000+ sensors and actuators and 10 million lines of code. Automobiles today have tens or 100+ processors. A smoke detector may be based on the cheapest computational device available.
- **Safety criticality.** By definition, HCSS are safety critical. But the degree of safety criticality varies widely—failures can be more or less likely to be life threatening, for example. Such differences exist even within one domain such as avionics software (even flight-critical software—cf. military vs. civil aviation) or process automation.
- **Regulatory compliance and certification.** Many high-confidence products have to conform to legislations or be certified by agencies (e.g., FAA, FDA). Certifications are not always mandatory (e.g., UL).

### **HCSS—the state of the practice**

High-technology products today can be extremely complex; at the high end they can comprise thousands or more components and/or millions or more lines of software. It is obviously no accident that the vast majority of these are safe and reliable. Before discussing areas where new research is needed, it is important to recognize the engineering and scientific sophistication that is employed to ensure this safety and reliability. This sophistication includes the following (I note these because they are often underappreciated in the research community in my view):

- Systems engineering

- Extensive use of modeling and simulation
- Extensive testing and verification
- Safety-oriented protocols and practices

### **Research needs**

Much needs to be done by way of research to improve the design, analysis, and operation of high-confidence systems, but I emphasize one cross-cutting, “meta-research” need.

As discussed above, the variety of high-confidence systems is vast. A corollary is that one solution cannot fit all applications. In particular, high-confidence has very different connotations in different domains. Depending on if or how many lives may be at stake, on the potential for environmental catastrophe, on customer or end-user price sensitivity, on who gets to shoulder the liability, on the protection that certification provides, etc., the level of confidence required of a complex (or, for that matter, simple) engineering system before it can be deployed or employed can be dramatically different.

The upshot is that high confidence must often be traded off with the cost (of design, development, operation, etc.) of realizing it. The targeted level of confidence must be consistent with affordability constraints in the application and market. And, given affordability constraints, we must strive to attain the highest level of confidence feasible.

Some specific topics of research that are suggested by this argument include:

- Low-cost, easy-to-use high-confidence methodologies. “Heavyweight” high-confidence techniques will impose too much of a burden, financial or otherwise, on many systems, especially low-end embedded devices. As an example, model-based design and development can help reduce the likelihood of errors in translating architecture-level specifications to code.
- Design and analysis approaches that do not target “perfect” safety. Approaches that are focused on deterministic safety guarantees will, in my opinion, be forever limited in the scale and complexity of systems they can be applied to. Approximation methods such as statistical verification are relevant.
- Better ways of quantifying the safety and reliability of automation and control solutions. If we are to back off from deterministic assurances, we need to be able to meaningfully assess the degree of reliability and safety of admittedly imperfect designs and solutions. Greater emphasis on modeling operating environments, for example, would help.
- Domain-specific test-beds and “grand challenges.” Demonstrations that attempt to mimic real-world setups can help facilitate industry uptake of research results.

### **Author Bio:**

Tariq Samad is a Corporate Fellow with Honeywell Automation and Control Solutions. He has been with various R&D organizations in Honeywell for 20 years, during which time he has been involved in leading initiatives that have explored applications of new developments in automation and control to domains such as unmanned aircraft, complex network systems, process operations, building controls, and automotive engines. His specific areas of research interest include high-confidence systems, intelligent control, and autonomous systems. He was the editor-in-chief of IEEE Control Systems Magazine from 1998 to 2004. Dr. Samad received a B.S. degree from Yale University in 1980 and M.S. and Ph.D. degrees from Carnegie Mellon University in 1982 and 1986.