Panel

Secure and Safety-Critical vs. Insecure, Non Safety-Critical Embedded Systems: Do they Require Completely Different Design Approaches?

Panel Organizer
Peter Marwedel
U. of Dortmund + ICD, Germany

Panel Moderator, Author
Catherine Gebotys
U. of Waterloo, Canada

ABSTRACT

As we move forward into the era of ubiquitous pervasive computing, the design of secure safety-critical systems will become increasingly complex. For example, future automobiles will become the ultimate mobile wireless device containing a distributed network with multiple vendor software and hardware. However the car's embedded software which is expected to increase in size by 100 fold, will create a significant impact on the overall system safety. Furthermore wireless communications may create the possibility of terrorists or attackers gaining control of the automobile, hence security is also an important issue. How will designers cope with this complexity while at the same time ensure safety and security? Will new design approaches be required? Or can current design methodologies be used with new metrics, safety and security? This panel will bring together experts from the safety-critical industry, security industry, and experts from the insecure non-safety critical industry.

Categories and Subject Descriptors

C.3 [**Special-Purpose and Application-Based Systems**]: Real-time and embedded systems

General Terms: Design, Reliability, Security

Keywords: Safety-critical, Security

1. INTRODUCTION

This paper will first provide a brief introduction to safety and security. Section 2 describes some complexities in designing a safety-critical system, specifically the future automobile. Section 3 details security issues in the design of embedded systems, and examines some parallels to design for safety. Finally the paper concludes questioning how these secure safety-critical systems can be designed given their complexities and highly constrained environments.

A safe system may fail frequently as long as it fails in a safe way, in contrast to a reliable system which does not fail often, but when it does it makes no guarantee of what would happen should it fail. Safety not only applies to avoiding physical harm to humans but could also imply avoiding financial disasters. In order to design a safe system one first has to identify the possible hazards and then determine how to remove the hazard or reduce its associated risk [2]. Hence the interaction of all components of a system is crucial in design for safety. For example the interaction of hardware, software, packaging, mechanical, and network determines the safety of the system. Designing safe systems, in addition to testing, involves not only analyzing possible device failure, but also components which may not fail, such as software.

Existing security developed for desktop and enterprise systems may not suffice for embedded systems due to their challenging constraints[6]. For example security is a necessity in RFID tags, smart cards, and many other devices including automobiles, which may involve severe energy, cost, or performance constraints. Security involves not only authentication, confidentiality, integrity, and non-repudiation but also resistance and/or response to denial-of-service-type attacks, tampering attacks and non-invasive (ie. electromagnetic wave) attacks. Safety and security have some interesting common aspects. For example design of secure software (for resistance to attacks) has also involved risk analysis analogous to design for safety[7]. Similar to safety, security involves ensuring the entire embedded system is secure (including interaction of all parts from SoC technology[8] to software) and must be considered at all stages of the design cycle.

2. SAFETY-CRITICAL AUTOMOBILES

An excellent example of a safety-critical system is the future automobile, an ideal mobile device with telematic capabilities. For example, future automobiles will talk to your smart card, support automatic service notification and appointment setup, have internet access ports (for automated software upgrades, real-time systems diagnosis, road condition monitoring, etc), satellite transmission capabilities, biometric ignition, etc.

The currently introduced high end automobiles utilize a fly-by-wire system. For example in order to brake, a signal is sent from the user onto the bus over the network to finally the braking system, where the brakes are activated. Nevertheless today the fault-tolerant requirements in automobiles are minimal [4]. The reason for this is the presence of a back up mechanical system, so if the brake signal over the network fails the mechanical backup system works. However the mechanical backup system is costly, not flexible and limits performance. Hence future automobiles must support highly reliable, fault-tolerant fly-by-wire systems with hard real-time requirements at a reasonable cost.

New standards are already being formed to reduce the microprocessors from up to 60 to about 20 (including large SoCs),

CODES+ISSS'04, September 8–10, 2004, Stockholm, Sweden.
ACM 1-58113-937-3/04/0009.

however the software is expected to increase100 fold in terms of number of lines of code[3]. These software modules support the fly-by-wire and telematic features of the future. The hardware and software components are typically designed by a multitude of firms. The software modules are in fact IP which must be integrated at the systems level with a software architecture[1]. Clearly safety in future automobiles will be a challenging quest, heavily dependent upon software. The software alone fulfills the three 'Trinities of Trouble'[7], complexity, connectivity, and extensibility which directly contribute to difficulties in managing security risks in software.

3. EMBEDDED SECURITY

Security is crucial for many embedded systems ranging from smart cards, cell phones, to any embedded device which supports internet connectivity, software complexity, or extensibility[7]. Analogous to safety, design for security requires knowledge of the different types of attacks. For example a denial of service attack on an embedded system may involve wirelessly downloading a 'power virus' which drains the battery on a portable device or damages components which exceed maximum heat dissipation (possibly causing a fire, etc). Some of the most highly publicized attacks involves smart card attacks, satellite TV theft, phone card theft, identify/financial theft, etc. More recently it has become evident that tampering may not be essential for many of these attacks. EM waves emissions from embedded systems have been shown to leak secure information and conversely EM waves directed at devices have been shown powerful enough to overwrite data in memory. Although many aspects of security, such as authentication, integrity, are essential for control of safety critical systems, these newer non-invasive attacks are highly feared.

The smart card industry is perhaps one of the most focused areas of active research in secure embedded systems. Open smart card design must support multi-vendor IP software similar to the safety-critical automobile. A combination of Java-based design, formal methods[5] and consideration of security at all levels of the design process have been crucial in the evolution of design of these embedded systems.

4. PANEL QUESTIONS

Do security and safety simply require a new extension of the existing design methodologies, where new safety and security metrics must be considered at all stages of the design? Or is this approach not sufficient? Is it time for a new design methodology to be developed to ensure future designs are safe and secure? What will this new methodology and tools look like? Will risk and hazard analysis become a crucial aspect of this methodology? What role will formal methods play throughout the methodology?

5. REFERENCES

[1] J.Axelsson "HW/SW Codesign for Automotive Applications: Challenges on the Architecture Level", Proc. 4th Intl Symp on O-O R-T Distribtd Comp , 2001

[2] B.Douglass, "Safety-Critical Systems Design", http://www-md.e-technik.uni-rostock.de/ma/gol/ilogic/scriptd.pdf, 1998.

[3] R.Allen "Gentlemen, start your electronically enriched automobiles", Electr.Des. June 14, 2004.

[4] M.Baleani, et al. "Fault-tolerant platforms for automotive safety-critical applications" CASES, 2003.

[5] P.Paradinas "Smart cards a(s) safety critical systems", Wkshp on Formal Des of safety critical embd sys, 2001.

[6] P.Koopman "embedded system security" IEEE Computer, July 2004.

[7] P.Kocher etal. "Security as a new dimension in embedded system design", DAC 2004.

[8] C.Gebotys etal. "Security Wrappers and power analysis for SoC Technologies", CODES+ISSS 2003.