The State of Software Design for Safety and Security

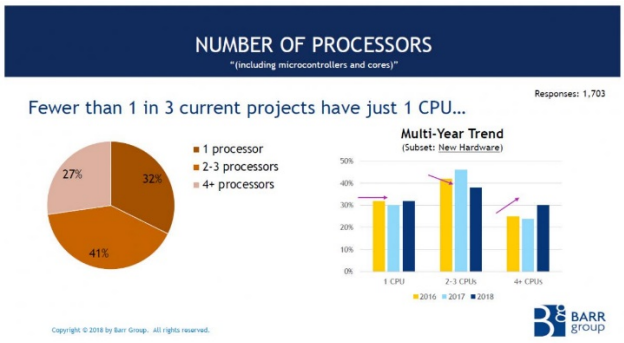
By Michael Barr

Each year, Barr Group conducts an independent industry survey of embedded systems designers to assess the state of product safety and security from the bottom up. Barr Group's 2018 Embedded Safety and Security Survey was completed by more than 1,700 professional product designers from all over the world. In this technology brief, we present key findings relevant to lawyers engaging in litigation over the design of electronics and software.

From toothbrushes and light bulbs to automobiles, pacemakers and satellites, software is now integrated into almost every aspect of our lives. Because of the risks associated with product failures and hacking, consumers thus increasingly rely on the developers of computerized products to protect their safety and security. While many engineering teams do take appropriate measures to design safety and security into their products, Barr Group's *2018 Embedded Safety and Security Survey* shows that there are still a significant number of design teams that do not.

Embedded Software Design Trends

An embedded system is a combination of electronics and software designed to perform specific, pre-defined tasks. Over the last decade, the number of processors (including microcontrollers and cores) in such systems has grown substantially. While less than one-third of new product designs have just a single processor, more than one-quarter of new projects have four or more processors, and the largest group now has two or three processors. Also, looking at annual data going back to 2016, there is an increasing number of single projects being designed with four or more processors (aka, CPUs).



Source: Barr Group 2018 Embedded Systems Safety & Security Survey

More processors can enable greater product functionality, but also adds to the complexity of designs. This can significantly increase the number of points of malfunction of the product as well as broaden the potential surface for hackers to attack. As a result, products with more processors generally also suffer more risk of product malfunctions and security breaches.

The Internet of Dangerous Things

To reduce the risk of product failures and tampering, product designers can easily and inexpensively implement a small number of industry best practices such as defect tracking, peer code reviews, static analysis tools, and coding standards. Unfortunately, use of these software development processes is not universal.

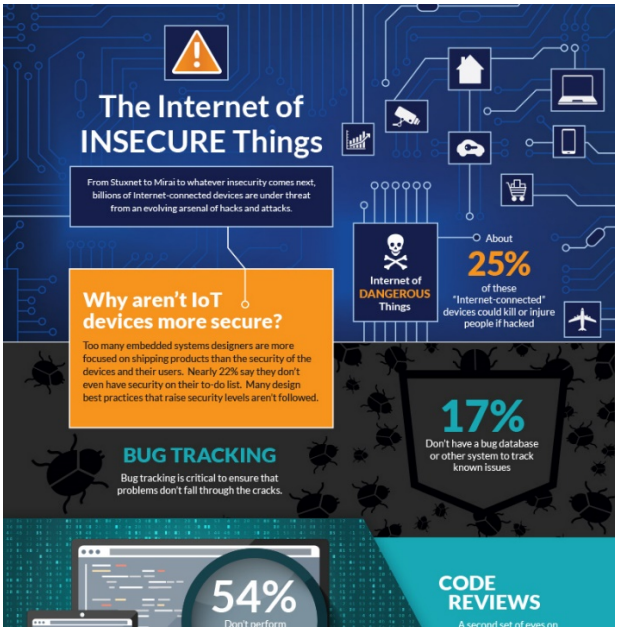
While it is logical that all product designers can benefit from implementing low cost best practices to reduce bugs in their software, it is reasonable to expect that the use of such practices would be universal among the designers of Internet-connected and safety-critical products. Shockingly, it is not.

Security Practices and Internet-Connected Products

For products always or sometimes connected to the Internet in this era, security is obviously a critical and necessary consideration for all their designers. And yet, our survey found that **more than 1 in 5 designers of Internet-connected products did not even put security on their project's to-do list**. Note that a failure to focus on security for a single Internet-connected product can put the reliability of the entire network at risk—as proven by some recent headlines about Distributed Denial of Service attacks, for example.

Furthermore, surveyed designers of Internet-connected products admitted:

- 17% don't have a database or other system to track known defects
- 54% don't perform regular peer code reviews
- 49% don't perform static analysis
- 33% lack a written coding standard
- MORE THAN 50% do not encrypt their data



View and download the complete infographic

Safety Practices and Dangerous Devices

According to the survey, nearly 30% of embedded systems designers make products that could kill or injure in the event of a malfunction. There is no one-size fits all approach to designing safe software. Safety has to be considered from many angles, including at the system level. However, software development best practices are still important for raising the level of safety. Unfortunately, too many designers of safety-critical systems are skipping one or more fundamental software development processes known to reduce the number of defects. Included in these statistics are the following:

- 43% don't perform regular peer code reviews
- 41% don't perform regression testing
- 38% don't comply with a formal safety standard
- 33% don't perform static analysis
- 17% lack a written coding standard

Click for higher-resolution version

Software Product Liability

Products that have been designed with insufficient attention paid to safety and security are more likely to malfunction or be hacked and thus also more likely to wind up in litigation.

To maximize the chances of determining the root cause behind alleged product failures or security breaches, it is extremely important that the electronics and software experts who are assigned to the case be skilled in:

- Analyzing the relationship between the electronics and software of complex computer systems and networks
- Identifying the use of state-of-the-art industry best practices for software development processes relating to safety and security
- Identifying potential insecurities in electronics and software systems
- Performing effective and cost-efficient analysis of software source code

With over 20 years of industry-leading experience in analyzing electronics and computerized systems for safety and security, Barr Group's testifying software experts bring these skills to every litigation project.

Barr Group provides testifying expert witnesses and software source code analysis teams to support complex litigation, including litigation involving product liability and infringement of intellectual property such as patents and software copyrights. CONTACT US

Michael Barr is a former adjunct professor of electrical and computer engineering with over a decade of software design and implementation experience. Internationally recognized as an expert in the field of embedded software process and architecture, Barr has been admitted as a testifying expert witness in the U.S. and Canada.

