Introduzione alla sicurezza funzionale nei sistemi elettronici

Massimo Violante

Dip. Automatica e Informatica

Politecnico di Torino

Before we start

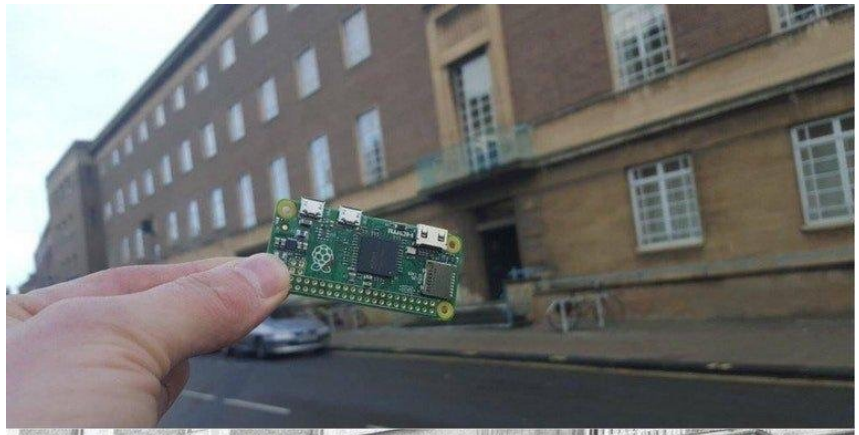
- Massimo Violante
  - Associate Professor of Computer Engineering at Politecnico di Torino, Torino, Italy
  - Active in the field of design and validation of dependable Embedded System
  - Consultant for companies in automotive, avionic, and industrial markets: ELDOR, Magneti Marelli, Ideas & Motion, IVECO, CNH Industrial, FPT, ITT Motion Technologies, Boeing Satellite Systems, European Space Agency, Thales Alenia Space, Leonardo, EADS/Airbus, AROL Group
  - Passionate mountaineer

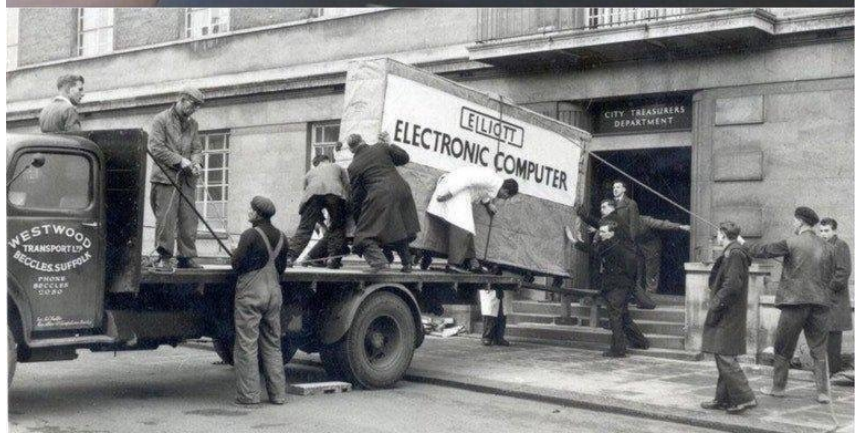
Introduction

- Technological evolution made possible the diffusion of embedded systems in a huge number of applications

- Many of these applications are safety critical (e.g., if somethings goes wrong, someone gets harmed)

Electronic steering wheel lock





An example (1)

- 2000: Toyota adopts an electronic throttle control system (ETCS)
- 2007: A person is killed when a Toyota Camry accelerating out of control hits his car at 120 mph (Camry's driver unable to slow the vehicle for 23 miles)
- 2013: Bookout/Schwarz v. Toyota: first trial in the US in which the plaintiffs allege that the UA was caused by a malfunction of the ETCS, as well as the lack of a brake override system that would have allowed the driver to slow or stop the vehicle

By CBSNEWS / AP / *May 25, 2010, 7:08 PM*

Toyota "Unintended Acceleration" Has Killed 89

A 2005 Toyota Prius, which was in an accident, is seen at a police station in Harrison, New York, Wednesday, March 10, 2010. The driver of the Toyota Prius told police that the car accelerated on its own, then lurched down a driveway, across a road and into a stone wall. (AP Photo/Seth Wenig) / AP PHOTO/SETH WENIG

An example (II)

- What happened in-field:
  - Recursion was used resulting in stack overflow
  - No mitigation for stack overflow resulting into overwriting operating system areas
  - Stack overflow leads to the loss of a critical functionality not detected by improperly managed watchdog
  - The vehicle accelerates suddenly
- Investigations identified issues:
  - In the ETCS product
  - In the development process that led to the conception, design and production of ECTS
- Outcome:
  - More than 80 persons experienced fatal injuries
  - The cost for Toyota was in the range of few Billions USD

A long story made short

- Complexity of embedded system is growing dramatically
- Complexity cannot be avoided! It is needed to provide the features clients ask for
- "Things can go wrong" unexpectedly, in not trivial manner, possibly after many years after the product is introduced to the market
- Only through a disciplined approach to safety the risk for harming end-users can be kept under control → functional safety standards
  - Beware: this is a much broader concept than intrinsic safety, i.e., the restriction of available electrical and thermal energy in the system so that ignition of a hazardous atmosphere (explosive gas or dust) cannot occur

Functional safety

- Functional Safety is the way to determine the risk of using complex and simple circuit to perform a safety function. The safety function must always be performed under normal/undisturbed conditions and under fault conditions

- A safety function can be defined as a function intended to achieve or maintain a safe state, with respect to a specific hazardous event

- Functional Safety is achieved when there is the absence of unreasonable risk due to hazards caused by the malfunctioning of electrical / electronic systems

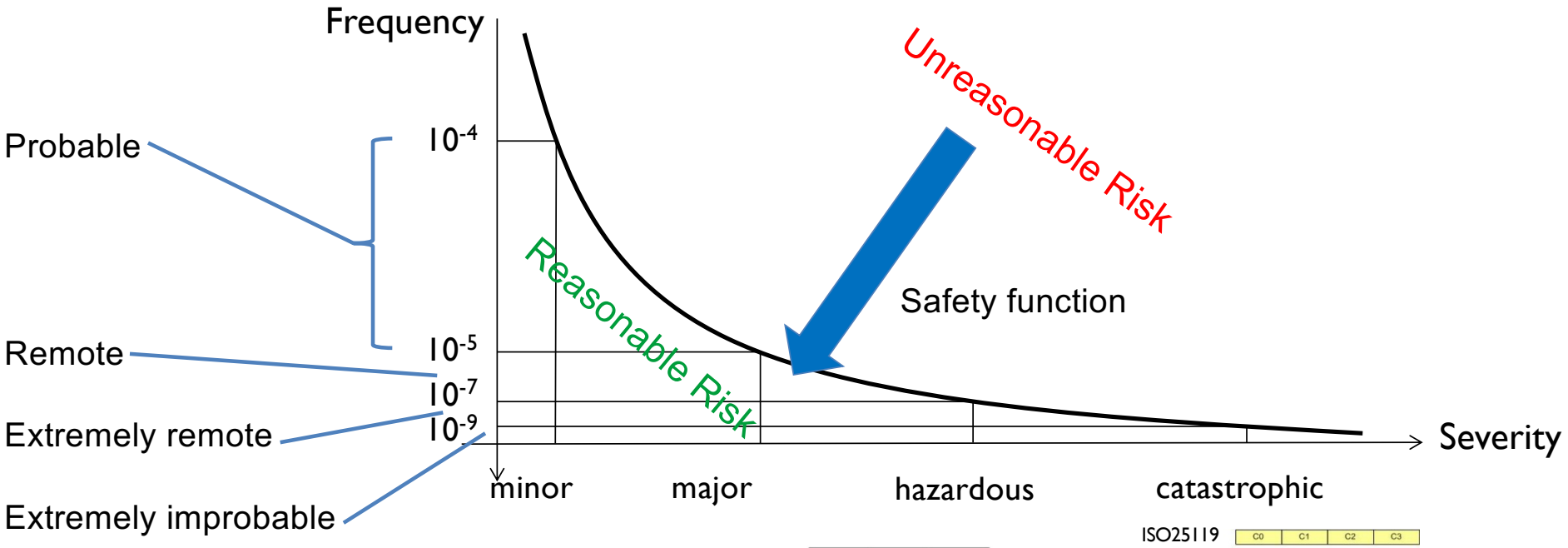
Safe systems vs functionally safe systems

Safe system

Functionally safe system

Credits: John Favaro

Reasonable vs Unreasonable Risk



IEC 61508

Frequency	Severity of Consequence 1	2	3	4	5
5	SIL3	SIL4	X	X	X
4	SIL2	SIL3	SIL4	X	X
3	SIL1	SIL2	SIL3	SIL4	X
2	-	SIL1	SIL2	SIL3	SIL4
1	-	-	SIL1	SIL2	SIL3

ISO26262

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

ISO25119

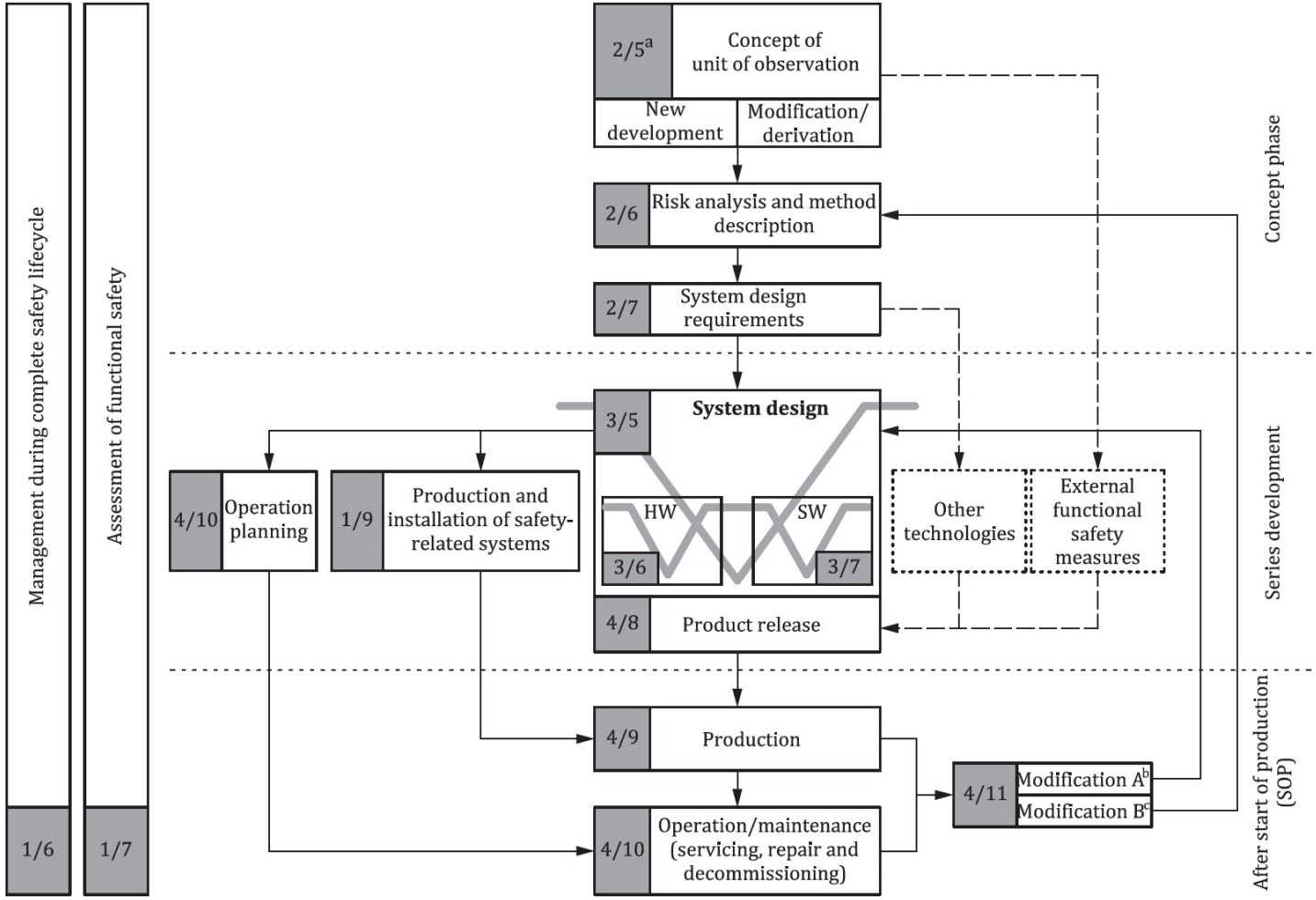
		C0	C1	C2	C3
S0		QM	QM	QM	QM
S1	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	a
	E3	QM	QM	a	b
	E4	QM	a	b	c
S2	E0	QM	QM	QM	QM
	E1	QM	QM	QM	a
	E2	QM	QM	a	b
	E3	QM	a	b	c
	E4	QM	b	c	d
S3	E0	QM	QM	QM	a
	E1	QM	QM	a	b
	E2	QM	a	b	c
	E3	QM	b	c	d
	E4	QM	c	d	e

Functional safety standards

- Several standards exist to achieve functional safety depending on the reference market:
  - ISO26262: Automotive
  - ISO25119: Tractors and machinery for agriculture and forestry
  - IEC61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
  - …

- Besides market-specific details, each standard provides:
  - Methods for estimating the risk
  - Methods for addressing risk reduction during the life cycle: product, and process
  - Targets to be achieved (definition of reasonable risk)

Safety lifecycle



Functional safety standards

- For each phase of the life cycle methods and measures are suggested

Methods and Measures		Risk level			
		1	2	3	4
1a	Method 1	o	+	++	++
1b	Method 2	+	+	+	+
2a	Method 3	o	o	+	+
2b	Method 4	o	+	++	++
3	Method 5	o	o	+	+

- Methods/measures address the process to be used as well as the product (hw/sw) being designed → it has a potentially disruptive impact on companies

Functional safety: why bothering?

- Some markets mandate the adoption of functional safety standards, otherwise products cannot be sold
  - DO254/DO178 for avionic applications

- Some other markets require the adoption of safety standards for mitigating the risk of liability (e.g., automotive)
  - Functional safety standards are collections of globally recognized best-practices for performing certain tasks
  - By applying functional safety standards, companies can claim they did everything that was conceivable to obtain the product with the highest possible quality
  - In case of legal actions, the use of best-practices avoid the risk of being considered liable of negligence

- If you haven't stumbled yet into functional safety standards, it will happen soon

Better be ready on time

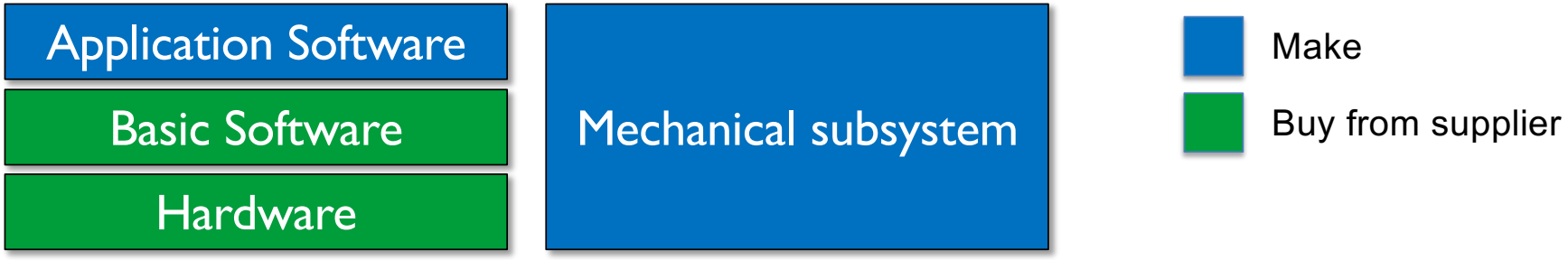
- Adopting functional safety standards impact the entire life cycle: the development process, supporting tools, the final product, its production, operation and maintenance
  - E.g.: requirement traceability, unit/integration/system testing (and accompanying metrics), use or safety-ready hardware, …

- It takes time and resources:
  - To identify where the company stands with respect to the standard: gap analysis
  - To train people on the the safety-aware life cycle
  - To acquire, deploy and master the supporting tools
  - To (partially) rethink the product
  - …

- Functional safety cannot be approached ex-post

An example

- Company X designs, manufactures and sells to OEMs a mechatronic system



- As the OEM application is not safety-relevant, no standard is applied
  - clients do not ask for it, so why paying the extra cost?
- Suddenly, for a new application where the same mechatronic system can be used as is, the OEM mandates the application of a functional safety standard
  - The company X is not ready: it must reshape the process & the product (6m/1y at least)
  - The company X must renegotiate the conditions with the supplier as safety-relevant data are needed, but the supplier is not providing them unless a (substantial) effort is rewarded

Recurring pattern when new technologies arrive

- What happened with hardware/software in mechanical designs?
  - Mechanical application developers: we don't need hardware/software, we can do better without them!
  - Look what happened to Diesel internal combustion engines with the introduction of Direct Injection. Embedded hardware/software is the only enabler of cost-effective solutions
  - Companies that invested in this disruptive technology won the market (Bosch, 2M pieces/year)
  - Companies that were skeptical (e.g., Infineon) lost the possibility of staying in the market

- What happened with embedded software?
  - Assembler programmers: we don't need C programming language for writing our applications, we can do better without it!
  - Is there any of you still using only assembler programming for writing applications longer than 100 lines of code?

Final thoughts

- Embedded systems are becoming more and more present in many applications replacing traditional products where functional safety is or will be mandatory!
- Functional safety must be addressed in each phase of the life cycle
- Functional safety is not a wagon you can jump on when already moving
- Get ready:
  - Increase your know-how by learning about functional safety in the market you are operating in
  - Progressively adapt your processes and your products to functional safety
  - Functional safety is a way to improve the overall quality of your products. It has a cost, but it is worth spending it!