Fault Injection for AUTOSAR Systems: Challenges and Solution

Antonio Pecchia
Critiware s.r.l.

11th Automotive SPIN Italy Workshop
Milan, November 7, 2013

Fault injection and AUTOSAR

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

- Fault injection is the deliberate introduction of faults in a target system.
- Critiware has a long lasting experience with fault injection:
  - commodity software;
  - operating systems;
  - middleware platform;
  - hardware;
  - …

AUTOSAR

But what it can be done with AUTOSAR?

Background and rationale

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

- Automobiles are increasingly incorporating a large amount of Electronic Control Units (ECUs)
- Some vehicles contain up to 70+ ECUs
- Variety of functionalities:
  - navigation devices
  - audio devices
  - dynamic stability control
  - anti-lock breaking systems
  - …

Background and rationale

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

- Cost of electronics and software can amount to 40% of a vehicle's overall cost
- Issues found in vehicles after release can also have considerable cost
  - Toyota*: recall issued between 2009-2010 after several vehicles experienced unintended acceleration problems
  - Honda issued a recall for ~1 million CR-V and Accord sedan manufactured between 2005-2007 in 2011

*http://articles.timesofindia.indiatimes.com/2011-09-06/india-business/30118005_1_faulty-part-city-sedan-global-exercise

Background and rationale

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

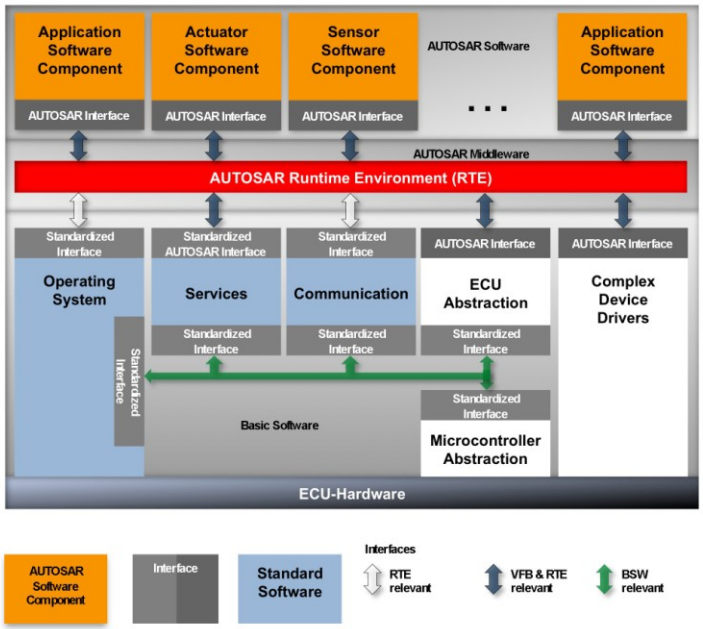
- ECU traditional development approaches
  - developer-dependent
  - proprietary architectures for both HW and SW
  - low maintainability
  - low reusability
  - high cost of ownership
  - …

AUTOSAR and ISO26262

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

AUTOSAR® - AUTomotive Open System ARchitecture

"Driven by the advent of innovative vehicle applications, contemporary automotive E/E architecture has reached a level of complexity which requires a technological breakthrough in order to manage it satisfactorily and fulfill the heightened passenger and legal requirements."



AUTOSAR

"To achieve the technical goals modularity, scalability, transferability and re-usability of functions AUTOSAR® will provide a common software infrastructure for automotive systems of all vehicle domains based on standardized interfaces for the different layers in the architecture."

from AUTOSAR® web site

AUTOSAR and ISO26262

- ISO 26262 is a functional safety standard tailored from the IEC 61508 relating to automotive systems
- ISO 26262 provides automotive SW development guidance
  - a tailored safety lifecycle including management, development, production, operation, service and decommissioning
  - a risk-based approach for defining Automotive Safety Integrity Levels (ASILs)
  - a means to specify safety requirements using ASILs to reach an acceptable residual risk
  - activities for validation and confirmation measures
  - …

The role of fault injection

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

ISO-26262 and Fault Injection

- Explicitly mentioned in the standard for all three levels:
  - System Level
  - Hardware Level
  - Software Level
- Highly recommended for the highest criticality levels of the life cycle
  - Same as saying mandatory

The role of fault injection

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

ISO-26262 and Fault Injection

- System Level

Table 4 — Correctness of implementation of system design specification and technical safety requirements

	Methods	ASIL			
		A	B	C	D
1a	Requirements-based test[a]	++	++	++	++
1b	Fault injection test[b]	+	++	++	++
1c	Back-to-back test[c]	+	+	++	++

[a] A requirements-based test denotes a test against functional and non-functional requirements.

[c] A back-to-back test compares the responses of the test object with the responses of a simulation model to the same stimuli, to detect differences between the behaviour of the model and its implementation.

The role of fault injection

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

ISO-26262 and Fault Injection

- does not provide **a clear guidance** for performing fault injection
- does not mandate **where** the fault campaigns must be performed
- hardware? software? ...
- does not provide guidance on the fault model definition
  - **what** to inject? (SW faults, bit-flip …)

It is the responsibility of the safety engineering team to plan, implement and execute the fault injection campaigns in order to comply with the standard!

The challenges

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

Fault injection in AUTOSAR is challenging:

- no specific fault injection support/interface
- implementations are proprietary
- sparse error-handling mechanisms
- mixed-criticality components involved in the error recovery
- …

Objective: to exercise safety and error handling mechanisms implemented across all the layers of an AUTOSAR system in a minimally-intrusive way

AUTOSAR error handling

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

Error models

- Used in the specification of error handling mechanisms
- Cover the behavioural specification of error manifestation as a consequence of a fault activation

- There are five error categories defined in the specifications:
  1. Data flow errors
  2. Program flow errors
  3. Access errors
  4. Timing errors
  5. Asymmetric errors

AUTOSAR error handling

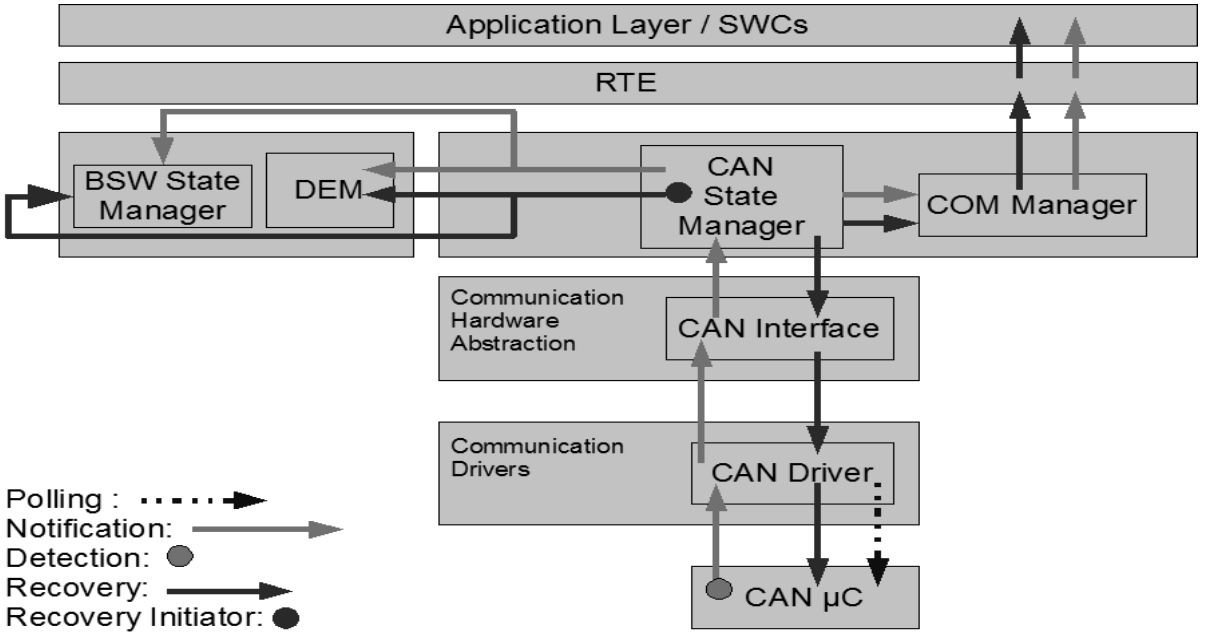
Several, well-established, handling mechanisms are permitted either at the BSW or SWC level. Examples:

Mechanism	Description	Imp. Level
Plausibility Checks	Predicates defined on a set of variables to determine their validity at runtime	SWC
Execution Sequence Monitoring	Detecting deviations from the correct execution path which could be on the level of individual statements, or block of code.	SWC/BSW
Voting	Consolidate values of redundant units by voting	SWC
Agreement	Components interact/exchange messages in order to reach a decision	SWC
Checksums and Codes	Adding redundant info to data values to increase data consistency, e.g., digital signature or encryption/decryption data	SWC/BSW

AUTOSAR error handling

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

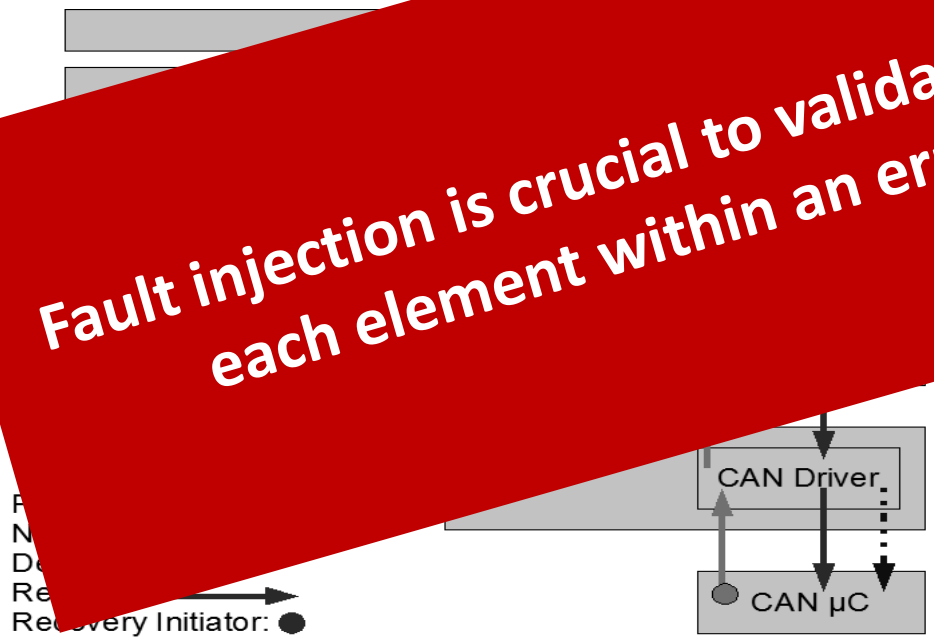
- Concept of **Error Information Path**, defined for each error, specifies information paths for each error that typically point out stages like polling, detection, notification and recovery



AUTOSAR error handling

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

- Concept of **Error Information Path**, defined for each error, specifies information paths for each error that typically point out st s like polling, detection, notification and recovery



Fault injection is crucial to validate the role of each element within an error path!

Fault injection requirements

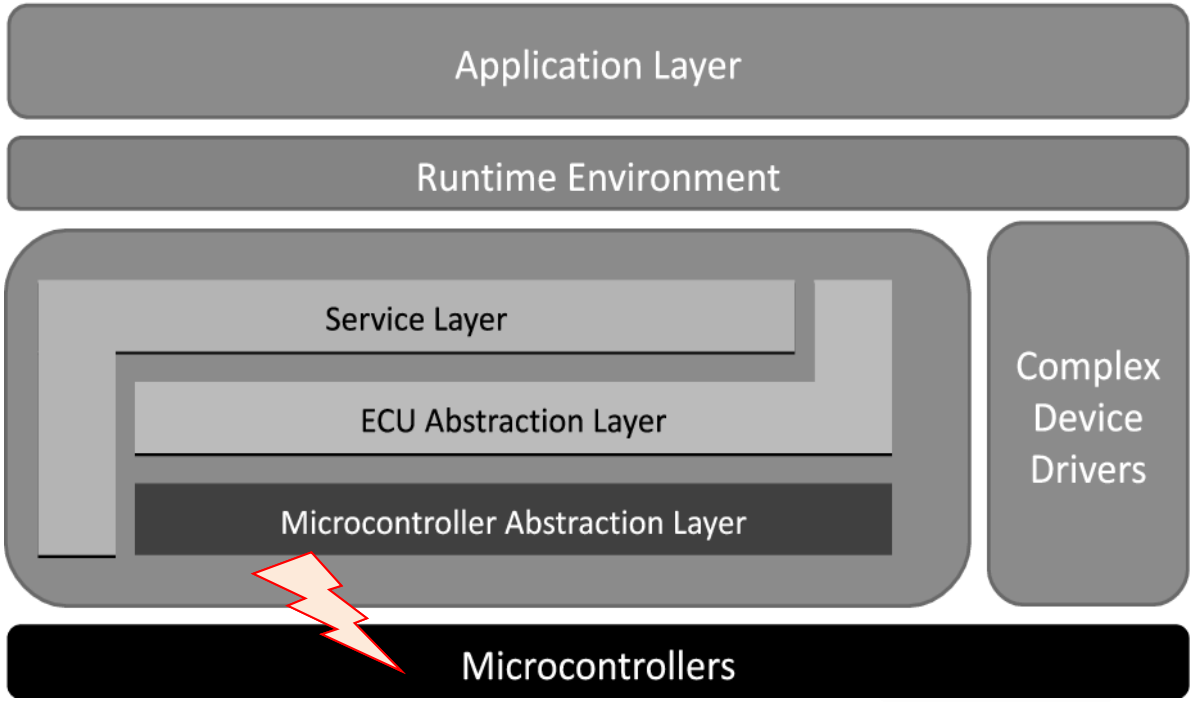
CRITIWARE s.r.l.
Innovating Critical Systems Engineering

- Should not assume availability of APIs or hooks.
- Should exercise system-wide features.
- Should be minimal intrusive.
- Should trigger error information paths.

A possible solution

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

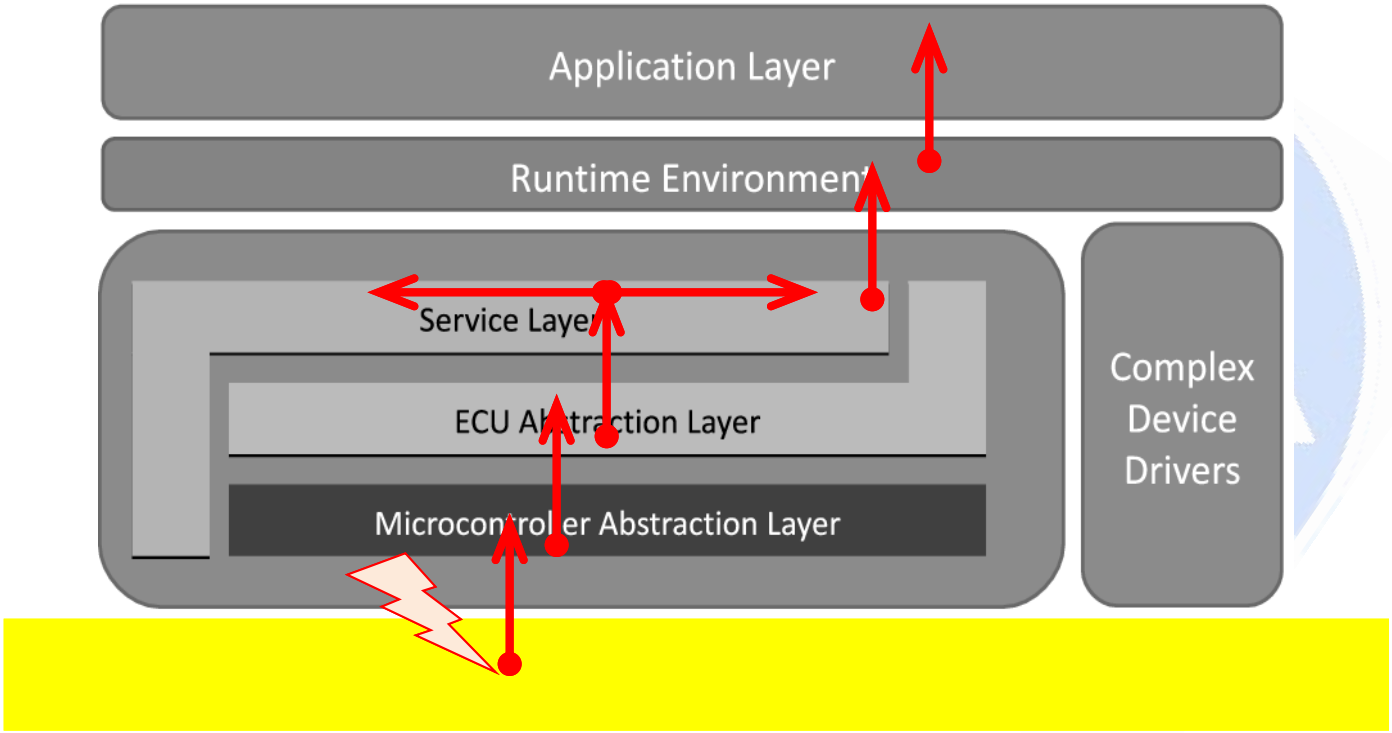
Injection performed at microcontrollers level: it aims to trigger error-handling mechanisms across different AUTOSAR layers



A possible solution

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

Injection performed at microcontrollers level: it aims to trigger error handling mechanisms across different AUTOSAR layers

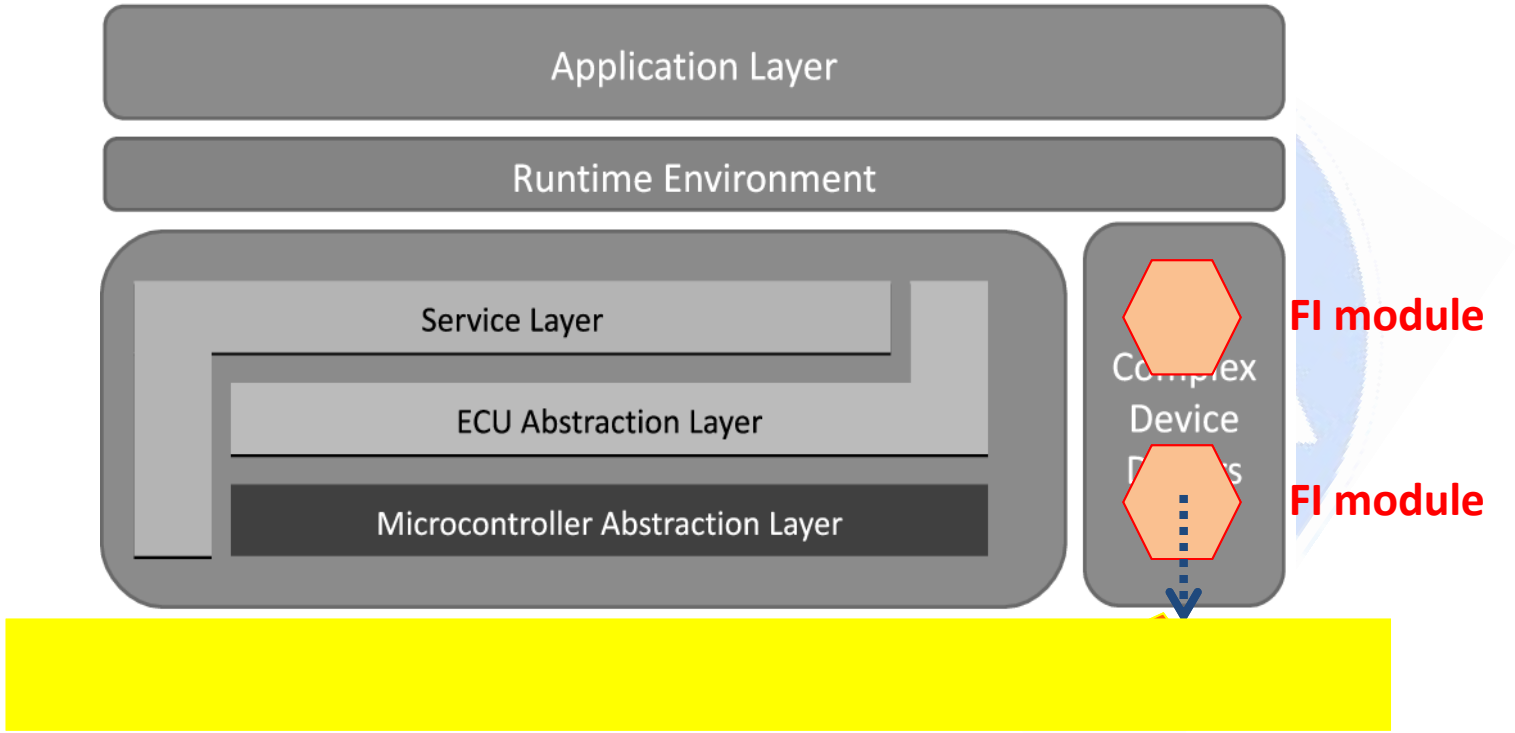


A possible solution

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

How to inject? CDD-based solution: access to microcontrollers layer and RTE

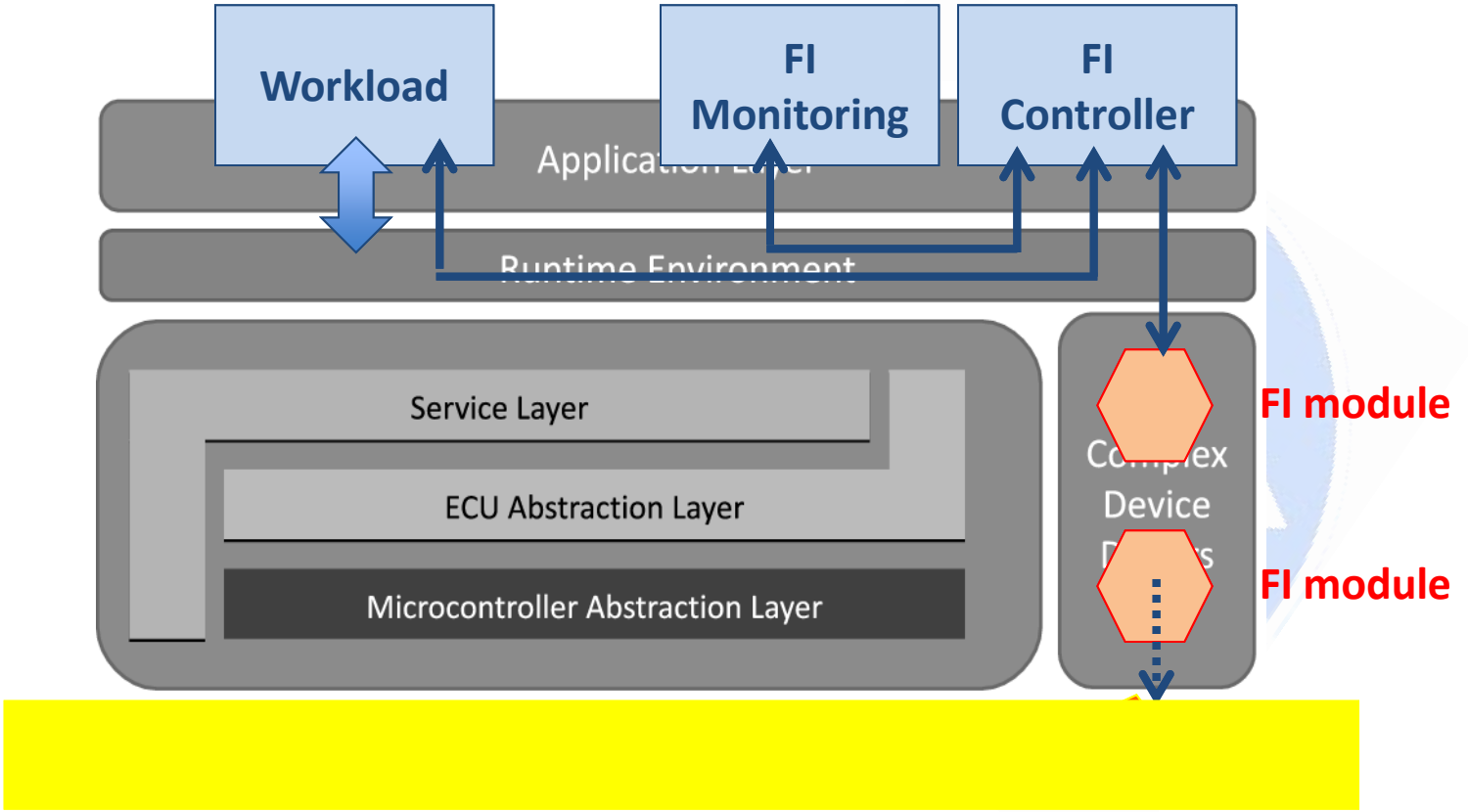
- corruption of the status, behaviour, or content of the µCs through the CDD (communication-related, WatchDog Timer, or NVRAM-related).



A possible solution

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

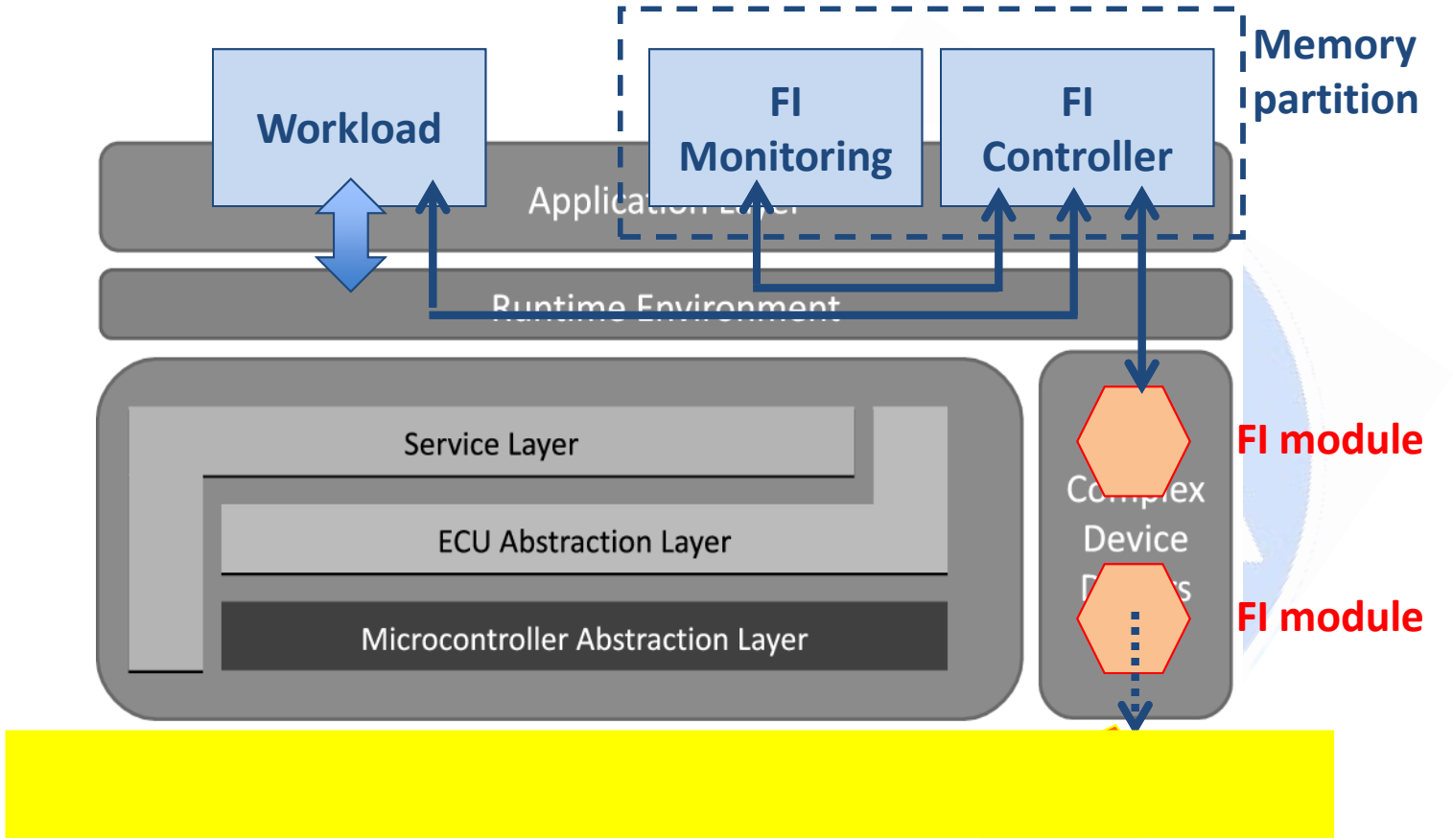
Fault-injection control & monitoring



A possible solution

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

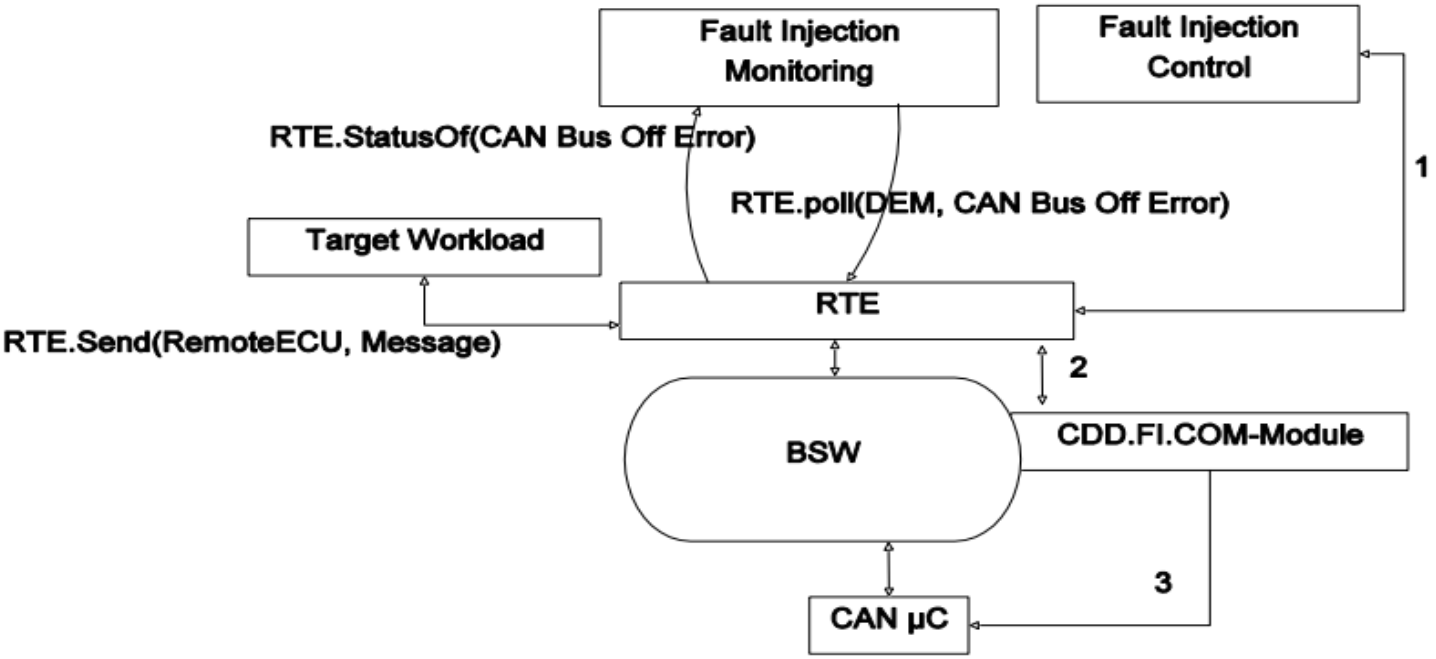
Leveraging the memory partition feature



Example: CAN Bus OFF

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

A CAN Bus Off error is emulated when there is a CAN communication channel loss.



1- RTE.Call(CDD.FI-COM-Module, activate(CAN.BUS.OFF))

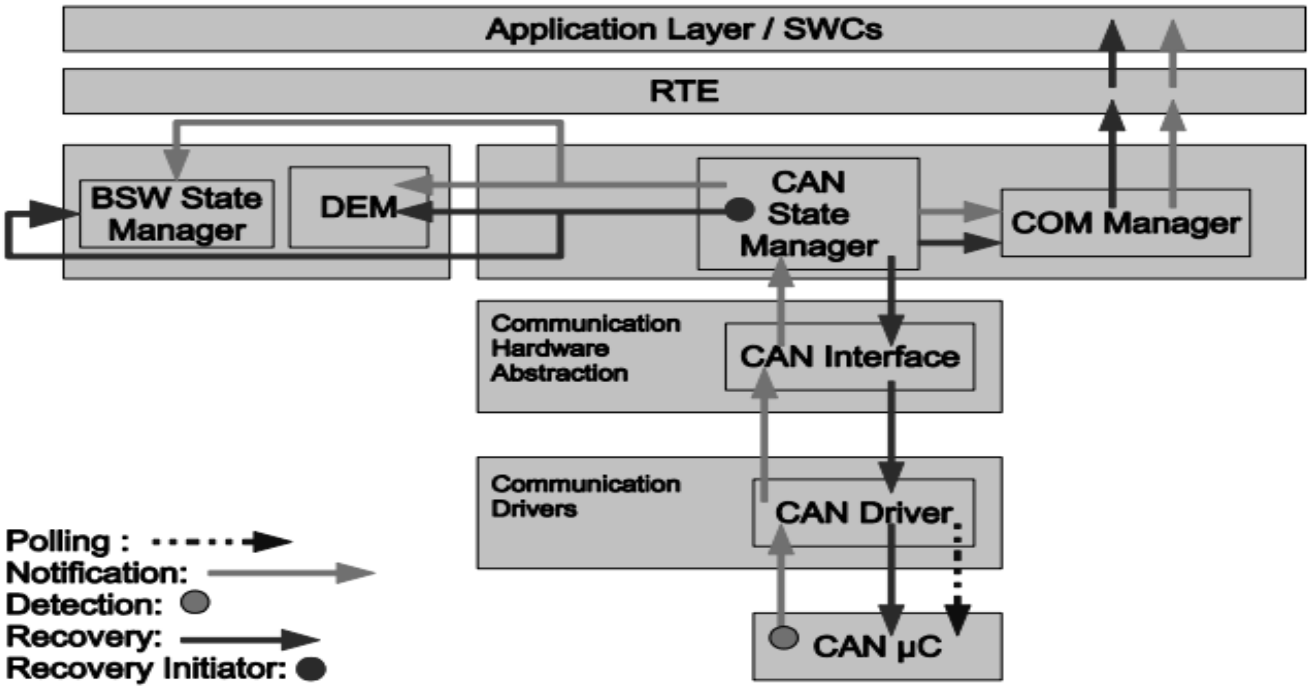
2- CDD.FI-COM-Module.activate(CAN.BUS.OFF)

3- BUS_OFF = True

Example: CAN Bus OFF

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

Despite injection is conducted at HW level, error handling is spread across different components and AUTOSAR layers.



Conclusion

CRITIWARE s.r.l.
Innovating Critical Systems Engineering

- There is a need for a flexible fault injection approach for AUTOSAR with the ability to assess the spread error-handling mechanisms
- A minimally-intrusive, (i.e., no change in the BSW) CDD-based fault injection framework for AUTOSAR that also benefits from memory partitioning was presented and it is believed to be promising
- **Open issues:**
  - fault-model;
  - cost-effectiveness;
  - temporal intrusiveness;

Related publications

A. Salkham, A. Pecchia, N. Silva *Assessing AUTOSAR Systems Using Fault Injection.* Proc. of the 23rd IEEE International Symposium on Software Reliability Engineering Workshops (**ISSREW**), Nov 2012, Dallas, USA

A. Salkham, A. Pecchia, N. Silva *Design of a CDD-based Fault-injection Framework for AUTOSAR Systems*. Proc. of the Next Generation of System Assurance Approaches for Safety-Critical Systems (**SASSUR**), Sept 2013, Toulouse, FRANCE

Ackonwledgments

CRITICAL Software Technology for an Evolutionary Partnership (CRITICAL-STEP), Marie Curie Industry-Academia Partnerships and Pathways (IAPP) number 230672, within the context of the EU Seventh Framework Programme (FP7).

http://www.critical-step.eu