2023 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE 10 YEAR ANNIVERSARY

Fault-injection-Enhanced Virtual Prototypes Enable Early SW Development for Automotive Applications

Mohammad Badawi, Javier Castillo,
Andreas Mauderer, Jan-Hendrik Oetjens

BOSCH

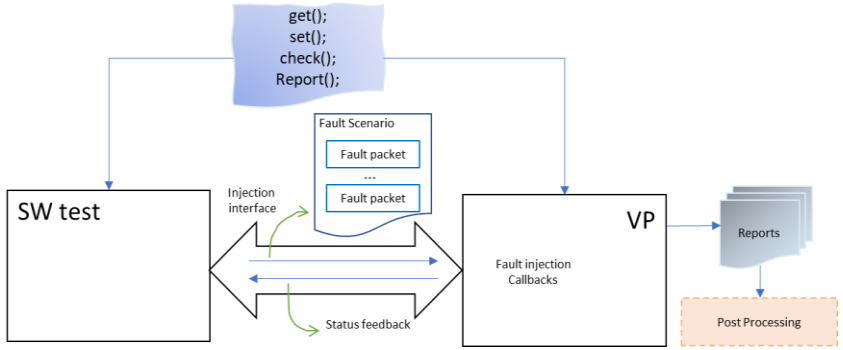
accellera SYSTEMS INITIATIVE

VPs Enable Early SW-Safety Development

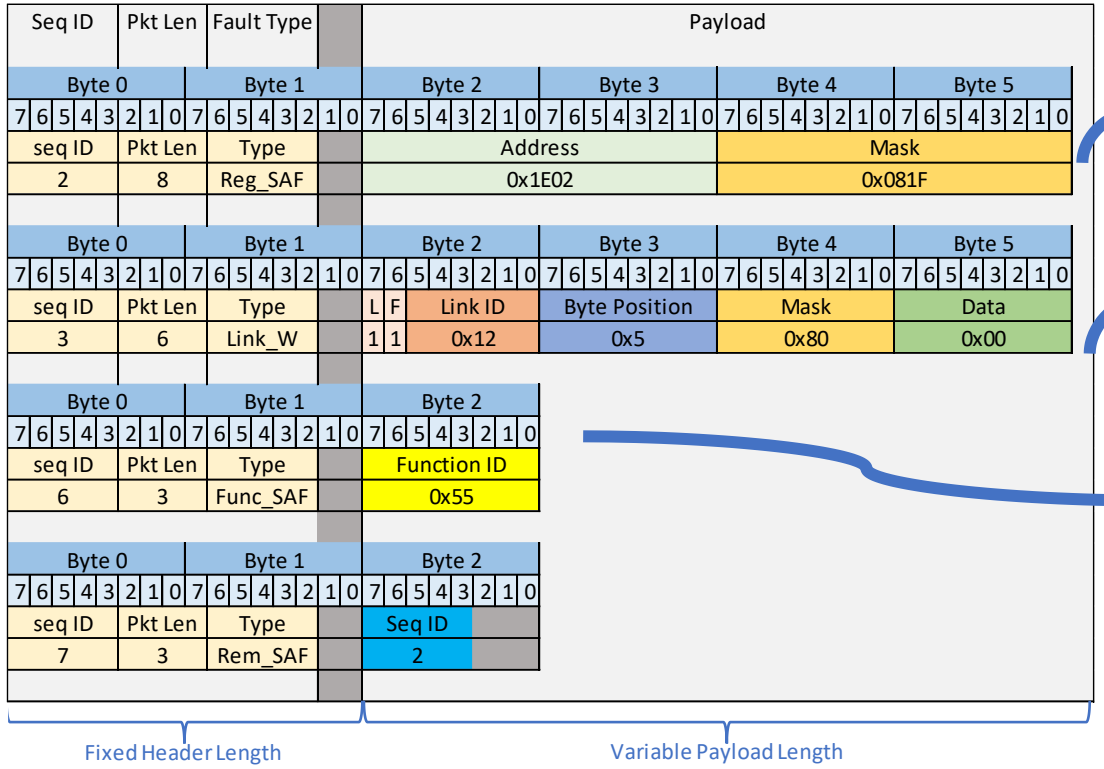
- Effort to comply to safety standards increases as SoC's complexity increase.
- System dependability (HW + SW) → evaluate SW before HW is available.
- SW-based FDM & FRM to enhance overall system dependability, but:
  - Increase SW complexity.
  - Further SW quality assurance is needed → more effort and time.
  - More reason for SW to start earlier.
- Using VPs to enable SW development very early, but need to
  - Provide high degree of flexibility to ease integration with SW.
  - Raise abstraction level → correct functionality can be viewed from SW perspective.

Fault Injection Framework

- Generalize fault injection and reporting to provide the needed flexibility.
- Models faults in registers, communication and computation:
  - Transient faults (SEU and MEU).
  - Permanent faults.
- Use of Fault Scenarios
  - Ease traceability.
  - Enable creating a set of related faults.
  - Scenario identifier, Number of packets involved, Reference to first packet.
  - Envelope for faulty use cases.



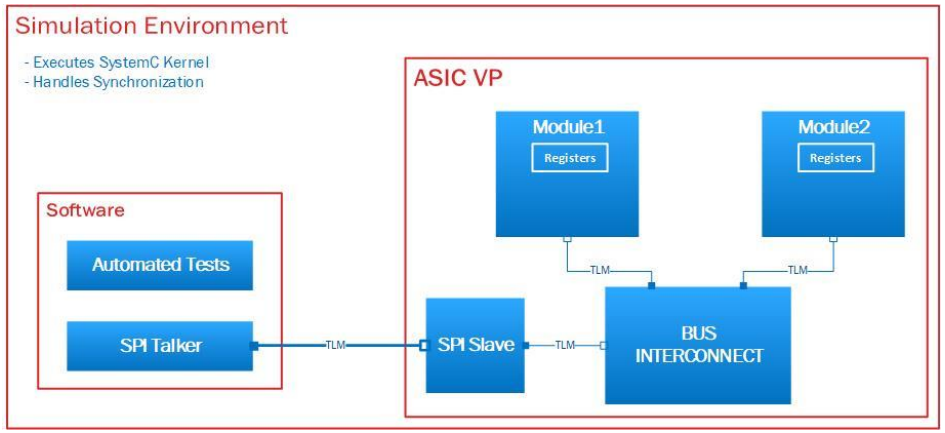
Fault Payload Packets



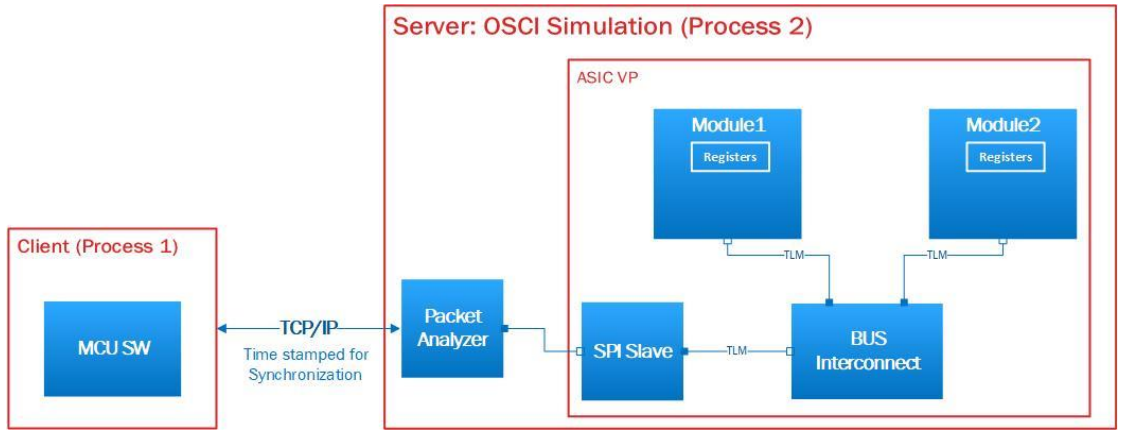
- Register Access Callback
  - Inject fault in a register.
- TLM Socket Callback
  - Communication fault at interconnect, interface or register port.
- Function Corruption Callback
  - Hook customized functions to targeted data processing functions in the VP.

Case Studies: Integration

- Simulation Based FMUs



- Multi-Process Simulation



Case Studies: Results

- Fault injection reports
- Fault injection overhead
- Overhead caused to applications

Sequence ID	Time Received [ms]	Time Injected [ms]	Fault Type	Payload Byte	Address	Resulting Data
1	1	1	REG_SAF		0x1004	0xFFFF00C4
2	2	2	REG_W		0x1000	0xFFFF0002
3	2	2	REG_W_M		0x1004	0xFFFF00A0
4	3	3	LINK_W	0x0A	0x0064	0x58
4	3	3	LINK_W	0x20	0x0064	0xAA
4	3	3	LINK_W	0x50	0x0064	0xB9
5	5	5	REG_W		0x1004	0xFFFF0002

Fault Type	Num Faults	Overhead [ms]	Overhead Per Fault [ms]
Reg_W	50	0.518	0.010
Reg_W	500	4.103	0.008
Reg_W	1000	8.370	0.008
Reg_W	2000	17.776	0.009
Reg_W_M	50	0.699	0.014
Reg_W_M	500	7.288	0.015
Reg_W_M	1000	14.761	0.015
Reg_W_M	2000	27.705	0.014
Link_W	10	0.003	0.0003
Link_SAF	10	0.006	0.0006

Summary and Future Work

- SW-based EDM and ECM start early before RTL and GL available.
- Simulating complex real-life fault scenarios becomes possible using VP.
- Flexibility to address different integration with SW.
- Traceability and observation; fault scenarios and comprehensive reposting.
- Minor overhead.
- Further issues to address:
  - Tracing fault propagation.
  - Fault dependency analysis and better understanding of masked faults.
  - Improved and standardized fault reporting.

Questions

accellera
SYSTEMS INITIATIVE