CONFERENCE AND EXHIBITION

EUROPE

MUNICH, GERMANY DECEMBER 6 - 7, 2022

# Fault Injection Analysis for Automotive Safety and Security

Sesha Sai Kumar C V, Ayman Mouallem, Jamil Mazzawi

Optima Design Automation Ltd.

SYST



### Hot from the press...

# Sirius XM flaw could've let hackers remotely unlock and start cars



IS INITIATIVE

In addition to providing a satellite radio subscription, Sirius XM also powers the telematics and infotainment systems used by a number of auto manufacturers, including Acura, BMW, Honda, Infiniti, Jaguar, Land Rover, Lexus, Nissan, Subaru, and Toyota. These systems collect <u>a</u> whole lot of information about your car that's easy to overlook — and could pose potential privacy implications. Last year, a <u>report from Vice</u> called attention to a spy firm, called Ulysses, which collected and planned to sell over 15 billion telematics based car locations to the US government.

Nissan is just one of the auto manufacturer's that use Sirius XM's connected vehicle services.

celleCredits: https://www.theverge.com/2022/12/3/23491259/sirius-xm-hack-remotely-unlock-start-cars



### Agenda

- Introduction: Automotive safety and security
- Relevance of Safety and Security for Automotive Use cases
- Optima Safety Platform
- Functional Safety Verification ISO 26262
- Security Verification





### **Functional Safety**

#### <u>functional safety</u> : absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems



- Average car today uses 300 processors, 50+ complex Electronic Control Units
- ISO 26262 defines automotive safety standards

Functional Safety Standards								
DO 254	IEC 61508							
	ISO 26262	IEC 61511	IEC 62061	IEC 61513	IEC 62404	EN 50128		
				IEC 62138	ISO 13485			
Areospace	Automotive	Industrial	Machine	Nuclear	Medical	Railway		
Defense		Controls	Tooling	Power	Devices	Transport		





### ECUs in the Automobile System



SYSTEMS INITIATIVE



### Risk Assessment for Safety: ASIL



#### Use Case: Head Light Failure while driving Narrow Country Road in the dark





## Head Lamp failure: Safety Perspective

- Driver Requests Head Lamp On/Off
- Head Lamp ECU sends a request via CAN
- Camera Sensor can send Request based on front vehicle Distance.
- Camera ECU sends a request through Gateway ECU
- Safety Consideration
  - ASIL Level for Head Lamp and Camera ECUs based on Exposure X Controllability X Severity
  - Safety Mechanism in MCU, to mitigate loss of Head lamp Switch actuator signal
  - Safety Mechanism in MCU, to mitigate incorrectness of camera sensor signal

Do We need to consider **Security**, in this Use case?







## Head Lamp failure: Security Perspective

- Gateway ECU
  - Bridge between Camera CAN1 and Headlap CAN4
- Attacker compromises the Navigation ECU
  - Through cellular or Blue tooth
- Cellular
  - Sends malicious CAN signal to turn off Head Lamp ECU via Gateway ECU
- Blue Tooth
  - Flood the CAN bus with High priority CAN messages via Gateway ECU to get Lamp on signal ignored
- Security Consideration
  - Fault Injection Attacks, on the hardware (MCU) has become rampant for unauthorized access
  - Each ECU/MCU to be design with Security in mind with countermeasures
  - Embedded Software need to be tested by injecting faults in
    - ECU authentication and Key calculation logics







### Simple Attack to gain Access

- Attacker can directly inject a fault in grant\_access();
- Access is granted irrespective of entered key matches or not
- Counter measure
  - Hardened Firmware code
  - Robust security countermeasures in MCU design

```
int verify key ( ... )
   computed key = get computed key(...);
   if (entered key == computed key)
      grant access ();
      error = NONE;
     else
      error = INVALID KEY;
   return error;
```





## Fault Injection Modelling: Safety And Security

- Safety:
  - Hard Errors: Permanent Faults modelled as S@0 and S@1
  - Soft Errors: Transient Faults modelled as Single Event Upset (SEU)
- Verify Safety Mechanisms by injecting Faults
  - ISO 26262 Recommends Fault Injection simulation to verify
- Security
  - Clock and Voltage Glitches
  - EM and Laser beam Attacks: Multiple SEU faults to model attacks
- Verify Security Vulnerabilities by way of FAS (Fault Attack Simulation)







### Safety and Security Verification: Many tools



### Unique Fault analysis Platform



### Single Platform for Fault Injection Analysis For Both Safety and Security







DECEMBER 6 - 7, 2022

# Functional Safety Verification ISO 26262



### ISO26262 Requirements Simplified

- Semiconductor Chips need to have
  - SM : "Safety Mechanisms"
    - Detect and/or correct faults
    - Within the budgeted time interval (e.g., 0.25ms to 100ms) from the time they happen
  - SM needs to be running continually while the device is operating
- SM diagnostic coverage: Quantitative Analysis
  - The SM needs to be able to cover no less than N% of the possible faults
  - Different ASIL levels have different N values
  - For example: for ASIL-D N>99%

#### ISO 26262-11:2018 4.8.1

For a Safety Concept with Semiconductor Components, Fault Injection is the Known Methodology for various safety lifecycle activities.





### Fault Injection Objectives (ISO 26262-11:2018 4.8)

- Diagnostic Coverage
- Fault Tolerant Time Interval
- Fault Reaction Time Interval
- Architectural Metrics (SPFM, LFM, FIT...)
- Fault Effect and Safety Mechanism Mitigation







### Optima Safety Platform™







### OSP flows for Hard and Soft error analysis



### Optima-SA™ Static Analysis









# Analyze Only Relevant faults

- Static Analysis based on the Failure and Detection Strobes
- COI is established and only relevant faults considered
- For safety critical DUT
  - NO Need to Simulate all f1 to f10 and then decide relevant faults
  - Only f1 and f2 are relevant to analyse further







### Optima-SA<sup>™</sup> Flow



### Safety Setup and Static Analysis

- Safety Setup: Simple way to Capture Safety related information
  - Failure Strobes and Conditional Signals
  - Detection Strobes and Conditional Signals



. . . . . . . . . . . .



## Static Analysis: Fault Statuses

### • SI → SAFE INVISIBLE

- SAFE: NOT Observed at Failure Strobe
- INVISIBLE: NOT Observed at Detection Strobe
- SV → SAFE VISIBLE
  - SAFE: NOT Observed at Failure Strobe
  - INVISIBLE: Observed at Detection Strobe

### Only Relevant faults to be Analysed

### UI 🗲 UNSAFE INVISIBLE <mark>No Safety Mechanism (SPF)</mark>

- UNSAFE: Observed at Failure Strobe
- INVISIBLE: NOT Observed at Detection Strobe

### UV 🗲 UNSAFE VISIBLE <mark>Possible Detects (Diagnostic Coverage)</mark>

- UNSAFE: Observed at Failure Strobe
- INVISIBLE: Observed at Detection Strobe





### Mapping Static Analysis to ISO2626 Metrics



### Multiple Failure modes: safety Setup



#### Optima-SA<sup>™</sup> Analyzes Faults, Single, Multiple and Merged Failure Modes







SYSTEMS INITIATIVE



### Optima-HE<sup>™</sup> Flow







### Faults for Optima-HE<sup>™</sup>



Relevant Faults

- Faults after Collapsing
- Faults Pruned by Optima-SA<sup>™</sup> UV
- Fault List Optimization by Optima-CA<sup>™</sup> Constant Analysis
- Faults analyzed by CA will not be considered
  - Marked BLOCKED/MASKED or SAFE







- Max time 1: F1 is EOT\_TO
  - no propagation or detection
  - Stops at Max time 1
- Max time 3: F1 is Detected\_Propagated
  - Propagated First
  - Simulation continues as set sim\_time\_after\_initial decision
  - Detected Before Detection Interval
  - Stops at Max time 3

- Max time 2: F1 is Propagated
  - Propagated First
  - Simulation continues as set\_sim\_time\_after\_initial\_decision
  - Stops at max time 2
- Max time 4: F1 is Detected\_late\_and\_Propagated
  - Propagated First
  - Simulation continues as set sim\_time\_after\_initial decision
  - Detected After Detection Interval, late detection
  - Stops at Max time 4





### Intuitive Fault Classification: Map to ISO26262



### Optima Safety Platform: GUI

	File Edit Tools Window Help	Optima Safety Platform ** /ho	me/cvseshu/SCR1_RIS	CV/scr1-master_clone/FDTI_I	DCM/demoFi	DTI.tcl <@optperf1.i	nt.optima-da.com	n>			© © &	
	😤 😤 Hi 🛼 💽 🖾 🛗 🔡 !		5earch in Com	mands			a 10					
Instruct         Note 0         Law 1         Yes           1	Hierarchy Dashboard	8 ×	Safety Visualizer Da	shboard							e x	
Control Lysing (A)         1	Instance	► Node ID V Name Type -										
1         2         4         1         2         4         1	e scrl_top_ahb	1 scr1 top a → Extern	XG									
<ul> <li> <ul> <li></li></ul></li></ul>	i pwrup_rstn_reset_sync		Cafety setup IF	Nama Activa	r		Total	51 SV	1 10			
<ul> <li> <sup>1</sup> (c) (c) (c) (c) (c) (c) (c) (c) (c) (c)</li></ul>	i_cpu_rstn_reset_sync		salety setup it	Name Active		To ball faculture	Incan	31 37	0	76760	- 7	
	i_tapc_rstn_and2_cell	3 scr1_top_a → Extern	0 Opt	ImaDe Irue	-	lotal faults	156322	2544 /112	8 589	0 76760		
<sup>1</sup> (a) mininging onerk, failing onerk <sup>1</sup> (a) strl.top.a	i_redcpu_oneclk_delay_in	4 scr1_top_a → Extern				Collapsed faults	156322	2544 7112	8 589	0 76760		
• (a) - (b) -	i_maincpu_oneclk_delay_out	5 scr1_top_a → Extern				Faults [%]	100.00	1.63 45.5	0 3.7	7 49.10		
Image: http://www.image: http://wwww.image: http://www.image: http://www.image: http://www.image	i core top red	6 scr1 top a  Fxtern			ľ	Gates	143992	2524 6520	4 525	6 71008		
Image: 1 proving the product of the	🖷 📕 i_tcm				-	Elene	12222	12 502	4 624	5750		
Interf         Interf<	I timer	7 scr1_top_a → Extern	il in the second se		-	riops	12322	12 592-	+ 034	+ 5752		
Destination         Detromatic service         Detromatic service <thdetromatic service<="" th="">         Detromatic serv</thdetromatic>	⊕ 📕 i dmem router	✓ Total Rows: 57937			]	Latches	8	8 0	0	0		1
■         =         =         ■         ■         =         =         ■         ■         =	ommands Dashboard		Active safety setup	is : OptimaDefaultSafetySetu	0qu							
Bit Numer:         Sci Log. Jubil, comp. (polic). (p	Session 1	-1 +1 =1	Selected hierarchy i	s:scri_top_and	-		-	1	1	1-1		
Principus 1         Principus 1         O         O         DESTRICT         Des	Fault name: scr1_top_ahb/i_core_top/i_pipe_to	op/i_pipe_ifu/ifu2imem_addr_o[9]_SA0	DET_LATE	DET_LATE_AND_PROP	DET_TIM	IE DET_PROP	EOT_SAFE	EOT_UNSAFE	EOT_TO	HE_RES	PROP_DUE	1
File       0       1       123542       0       0       0       Detected (a, max = 0, max	Fan out size: 1		o	0	125478	1 1	0	0	0	DET_PROP	N	
milet change in black is comparedides error ut 255442, in the comparedides error ut 2554442, in the comparedides error ut 255444444444, in the comparedides error ut 25544444444444444444444444444444444444	HE decision: DETECTED_LATE_AND_PROPAGA		<u>۲</u> 0	1	125564	2 0	0	0	0	DETECTED_LATE_AND	N	
grad to be abbility dets: compare/dets: err out 125552; str. top, abb/, dets: compare/dets, err out 125572; str. top, abb/, dets: compare/dets, err out 125582; str. top, abb/, dets: compare/dets, err out 125682; str. top, abb/, dets: compare/dets,	detection strobes : {scr1 top ahb/i dcls com	pare/dcls err out 1255642 .	a 0	0	125445	2 1	0	0	0	DET PROP	N	
125762, scr1 (op, ahb/), dcls, compare/dcls, err, out 125772, scr1, top, ahb/i, dcls, compare/dcls, err, out 125862, scr1, top, ahb/i, dcls, compare/dcls, err, out 125602, scr1, top, ahb/i, dcls, compare/dcls, err, out 125602, scr1, top, ahb/i, dcls, comp	scr1_top_ahb/i_dcls_compare/dcls_err_out 12	55652 , scr1_top_ahb/i_dcls_compare/dcls_err_out	Tab	0				0	0			
12/25792, sc1 tog abb/ (ds: compare/ds: err out 1225902, model compare/ds: err out 1225902, sc1 tog abb/ (ds: compare/ds: err out 1225902, sc1 tog abb/) (ds: compare/ds: err out 125902, sc1 tog abb/) (ds: compare/ds: err out 125002, sc1 tog abb/) (ds: compare	1255762 , scr1_top_ahb/i_dcls_compare/dcls_ scr1_top_abb/i_dcls_compare/dcls_err_out_12	err_out 1255772 , 55782 scr1 top abb/i dcls compare/dcls err out		0		U	L	0	U	EUT_SAFE	N	1
gr (2) tog. ahb/i / dls. compare/dls. err. out 1255812, scr1, tog. ahb/i, dds. compare/dls. err. out 125582, scr1, tog. ahb/i, dds. compare/dls. err. out 125592, scr1, tog. ahb/i, dds. compare/dls. err. o	1255792 , scr1_top_ahb/i_dcls_compare/dcls_	err_out 1255802 ,	<u> </u>	0	125445	0	0	0	0	DETECTED	N	1
12322/2.501_00_allor/045_compare/dds_err_001       125322.       101_00_allor/045_compare/dds_err_001       125322.       102_01_001_045_compare/dds_err_001       125362.       102_01_001_045_compare/dds_err_001       125362.       102_01_001_045_compare/dds_err_001       100       0       EOT_SAFE       N         1225392.scr1.top_alb/l_dds_compare/dds_err_01125592.cr1.top_alb/l_dds_compare/dds_err_01125592.scr1.top_alb/l_dds_compare/dds_err_011255902.scr1.top_alb/l_dds_compare/dds_err_01125592.scr1.top_alb/l_dd	scr1_top_ahb/i_dcls_compare/dcls_err_out 12:	55812 , scr1_top_ahb/i_dcls_compare/dcls_err_out	<u>u</u> 0	0	125446	1 1	0	0		DET_PROP	N	1
1255852, scr1 cop_ahb/, dcls_compare/dcls_err out 1255862, scr1 top_ahb/, dcls_compare/dcls_err out 1255892, scr1 top_ahb/, dcls_compare/dcls_err out 1255992, scr1 top_ahb/, dcls_compare/dcls_err out 1255992, scr1 top_ahb/, dcls_compare/dcls_err out 125592, scr1 top_ahb/, dcls_compare/dcls_err out 125692, scr1 top_abb/, dcls_compare/dcls_err out 1	E scr1 top ahb/i dcls compare/dcls_compare/dcls_	55842, scr1 top ahb/i dcls compare/dcls err out	da lab	0	125445	2 1	0	0	0	T PROP	N	1
gr cr1 top. ahb/i dcls_compare/dcls_err_out       1255892, scr1 top. ahb/i dcls_compare/dcls_err_out       0       0       1       0       0       EOT_SAFE       N         0       0       0       125482, scr1 top. ahb/i dcls_compare/dcls_err_out       0       0       0       DET_PROP       N         0       0       0       1254462       1       0       0       DET_PROP       N         0       0       1254462       1       0       0       DET_PROP       N         125592, scr1 top. ahb/i dcls_compare/dcls_err_out       125592, scr1 top. ahb/i dcls_compare/dcls_err_out       0       0       0       DET_PROP       N         125592, scr1 top. ahb/i dcls_compare/dcls_err_out       125592, scr1 top. ahb/i dcls_compare/dcls_err_out       0       0       0       DET_PROP       N         125602, scr1 top. ahb/i dcls_compare/dcls_err_out       125602, scr1 top. ahb/i dcls_compare/dcls_err_out       125602, scr1 top. ahb/i dcls_compare/dcls_err_out       0       0       DET_PROP       N         125602, scr1 top. ahb/i dcls_compare/dcls_err_out       125602, scr1 top. ahb/i dcls_compare/dcls_err_out       0       0       0       DET_PROP       N       N       N       N       N       N       N       N       N       N       N       N<	N 1255852 , scr1_top_ahb/i_dcls_compare/dcls_	err_out 1255862 ,	U	0				-	0	FOT		1
crl top abb/_dcls_compare/dcls_err_out 1255992, scrl top_abb/_dcls_compare/dcls_err_out         0       0       0       1254462       1       0       0       DET_PROP       N         0       0       0       1254462       1       0       0       DET_PROP       N         0       0       0       1254462       1       0       0       DET_PROP       N         0       0       0       1254462       1       0       0       DET_PROP       N         1255972, scrl_top_abb/_dcls_compare/dcls_err_out 1255982, scrl_top_abb/_dcls_compare/dcls_err_out 1255982, scrl_top_abb/_dcls_compare/dcls_err_out 1255982, scrl_top_abb/_dcls_compare/dcls_err_out 125692, scrl_top_abb/_dcls_compare/dcls_err_out 1256022, scrl_top_abb/_dcls_compare/dcls_err_out 1256022, scrl_top_abb/_dcls_compare/dcls_err_out 1256022, scrl_top_abb/_dcls_compare/dcls_err_out 1256032, scrl_top_abb/_dcls_compare/dcls_err_out 1256032, scrl_top_abb/_dcls_compare/dcls_err_out 1256032, scrl_top_abb/_dcls_compare/dcls_err_out 1256032, scrl_top_abb/_dcls_compare/dcls_err_out 1256032, scrl_top_abb/_dcls_compare/dcls_err_out 1256042, scrl_top_abb/_dcls	Scr1_top_ahb/i_dcls_compare/dcls_err_out 12: 1255882 scr1_top_abb/i_dcls_compare/dcls	55872 , scr1_top_ahb/i_dcls_compare/dcls_err_out err_out 1255892		U		U	1	U	0	EOI_SA	N	
<sup>1</sup> <sup>1</sup> <sup>255912</sup> , scr1.top.ahb/, dcls_compare/dcls_err_out 1255932, scr1.top.ahb/, dcls_compare/dcls_err_out 1256042, scr1.top.ahb/, dcls_co	scr1_top_ahb/i_dcls_compare/dcls_err_out 12	55902 , scr1_top_ahb/i_dcls_compare/dcls_err_out	0	0		0	1	0	0	EOT_SAFE	N	1
Set 1: dog_anhol/ dots_compare/dots_err_out 1255922, scr1_tog_ahhol/_dots_compare/dots_err_out       255922, scr1_tog_ahhol/_dots_compare/dots_err_out       0       0       1       0       0       ECT_SAFE       N         scr1_tog_ahhol/_dots_compare/dots_err_out       1255922, scr1_tog_ahhol/_dots_compare/dots_err_out       1255922, scr1_tog_ahhol/_dots_compare/dots_err_out       0       0       0       0       DET_PROP       N         scr1_tog_ahhol/_dots_compare/dots_err_out       1255922, scr1_tog_ahhol/_dots_compare/dots_err_out       1255922, scr1_tog_ahhol/_dots_compare/dots_err_out       0       0       0       DET_PROP       N         scr1_tog_ahhol/_dots_compare/dots_err_out       1256022, scr1_tog_ahhol/_dots_compare/dots_err_out       1256022, scr1_tog_ahhol/_dots_compare/dots_err_out       0       0       1254462       1       0       0       DET_PROP       N         scr1_tog_ahhol/_dots_compare/dots_err_out       1256022, scr1_tog_ahhol/_dots_compare/dots_err_out       1256022, scr1_tog_ahhol/_dots_compare/dots_err_out       0       0       0       0       DET_PROP       N         scr1_tog_ahhol/_dots_compare/dots_err_out       1256022, scr1_tog_ahhol/_dots_compare/dots_err_out       1256022, scr1_tog_ahhol/_dots_compare/dots_err_out       0       0       0       DET_PROP       N       N       Det_Top       N       Det_Top       Det_Top       Det_Top       <	1255912, scr1_top_ahb/i_dcls_compare/dcls_	err_out 1255922 ,	0	0	125446	1 1	0	0	0	DET_PROP	IV.	
scr1 top ahb/i_dcls_compare/dcls_err out 1255962, scr1 top ahb/i_dcls_compare/dcls_err out 1255962, scr1 top ahb/i_dcls_compare/dcls_err out 1255962, scr1 top ahb/i_dcls_compare/dcls_err out 125592, scr1 top ahb/i_dcls_compare/dcls_err out 1256012, scr1 top ahb/i_dcls_compare/dcls_err out 1256012, scr1 top ahb/i_dcls_compare/dcls_err out 125602, scr1 top ahb/i_dcls_compare/dcls_err out 1256002, scr1 top ahb/i_dcls_compare/dcls_err out 125602,	1255942, scr1 top ahb/i dcls compare/dcls	err out 1255952 ,	0	0		0	1	0	0	EOT SAFE	N	
1253972, scr1_top_ahb/_idcls_compare/dcls_err_out 125592, scr1_top_ahb/i_dcls_compare/dcls_err_out 125502, scr1_top_ahb/i_dcls_compare/dcls_err_out 1256012, scr1_top_ahb/i_dcls_compare/dcls_err_out 125602, scr1_top_ahb/i_dcls_compare/dcls_err_out 125602, scr1_top_ahb/i_dcls_compare/dcls_err_out 125602, scr1_top_ahb/i_dcls_compare/dcls_err_out 125602, scr1_top_ahb/i_dcls_compare/dcls_err_out 1256072, scr1_top_ahb	scr1_top_ahb/i_dcls_compare/dcls_err_out 12	55962 , scr1_top_ahb/i_dcls_compare/dcls_err_out		0	125446	2 1	0	0	0		N	
1256002, scr1_top_ahb/i_dcls_compare/dcls_err_out 1256012,       0       0       0       0       EOT_SAFE       N         scr1_top_ahb/i_dcls_compare/dcls_err_out 1256022, scr1_top_ahb/i_dcls_compare/dcls_err_out       0       0       0       0       0       DET_PROP       N         scr1_top_ahb/i_dcls_compare/dcls_err_out 1256042, scr1_top_ahb/i_dcls_compare/dcls_err_out       1256042, scr1_top_ahb/i_dcls_compare/dcls_err_out       0       0       0       0       DET_PROP       N         scr1_top_ahb/i_dcls_compare/dcls_err_out       1256042, scr1_top_ahb/i_dcls_compare/dcls_err_out       0       0       0       0       0       DET_PROP       N         scr1_top_ahb/i_dcls_compare/dcls_err_out       1256042, scr1_top_ahb/i_dcls_compare/dcls_err_out       0       0       0       0       0       DET_PROP       N       N         scr1_top_ahb/i_dcls_compare/dcls_err_out       1256042, scr1_top_ahb/i_dcls_compare/dcls_err_out       0       0       0       1       0       0       DET_SAFE       N       N         1256042, scr1_top_ahb/i_dcls_compare/dcls_err_out       1256042, scr1_top_ahb/i_dcls_compare/dcls_err_out       0       0       1254462       1       0       0       DET_PROP       N       N       2022       1       0       0       DET_PROP       N       2022 </td <td>scr1 top ahb/i dcls compare/dcls err out 12</td> <td>err_out 1255982 , 55992 . scr1 top ahb/i dcls compare/dcls err out</td> <td></td> <td>U</td> <td>125440</td> <td>1</td> <td>0</td> <td>U</td> <td>0</td> <td>DET_PROP</td> <td></td> <td>Fault lable</td>	scr1 top ahb/i dcls compare/dcls err out 12	err_out 1255982 , 55992 . scr1 top ahb/i dcls compare/dcls err out		U	125440	1	0	U	0	DET_PROP		Fault lable
scr1_top_ahb/i_dcls_compare/dcls_err_out 1256022, scr1_top_ahb/i_dcls_compare/dcls_err_out       0       0       1254462       1       0       0       DET_PROP       N         1256032, scr1_top_ahb/i_dcls_compare/dcls_err_out       1256032, scr1_top_ahb/i_dcls_compare/dcls_err_out       1256032, scr1_top_ahb/i_dcls_compare/dcls_err_out       0       0       0       DET_PROP       N         scr1_top_ahb/i_dcls_compare/dcls_err_out       1256032, scr1_top_ahb/i_dcls_compare/dcls_err_out       1256032, scr1_top_ahb/i_dcls_compare/dcls_err_out       0       0       1       0       0       EOT_SAFE       N         1256032, scr1_top_ahb/i_dcls_compare/dcls_err_out       1256032, scr1_top_ahb/i_dcls_compare/dcls_err_out       0       0       1       0       0       EOT_SAFE       N         1256032, scr1_top_ahb/i_dcls_compare/dcls_err_out       1256032, scr1_top_ahb/i_dcls_compare/dcls_err_out       0       0       1       0       0       EOT_SAFE       N         1256032, scr1_top_ahb/i_dcls_compare/dcls_err_out       1256102, scr1_top_ahb/i_dcls_compare/dcls_err_out       0       0       1254462       1       0       0       DET_PROP       N       V       2022       1       0       0       DET_PROP       N       2022       ESIGN AND VERIEICATION       ESIGN AND VERIEICATION	1256002, scr1_top_ahb/i_dcls_compare/dcls_	err_out 1256012 ,	0	0		0	1	0	0	EOT_SAFE	N	Ontima-SA™
1250032, jahl/jdcls_compare/dcls_err_out       256052, scr1_top_ahb/j.dcls_compare/dcls_err_out       0       0       0       1       0       0       EOT_SAFE       N         scr1_top_ahb/j.dcls_compare/dcls_err_out       1256062, scr1_top_ahb/j.dcls_compare/dcls_err_out       0       0       1       0       0       EOT_SAFE       N         scr1_top_ahb/j.dcls_compare/dcls_err_out       1256082, scr1_top_ahb/j.dcls_compare/dcls_err_out       0       0       1       0       0       EOT_SAFE       N         1256092, scr1_top_ahb/j.dcls_compare/dcls_err_out       1256092, scr1_top_ahb/j.dcls_compare/dcls_err_out       0       0       1       0       0       EOT_SAFE       N         1256092, scr1_top_ahb/j.dcls_compare/dcls_err_out       1256092, scr1_top_ahb/j.dcls_compare/dcls_err_out       0       0       1       0       0       EOT_SAFE       N         1256092, scr1_top_ahb/j.dcls_compare/dcls_err_out       1256102, scr1_top_ahb/j.dcls_compare/dcls_err_out       0       0       1254462       1       0       0       DET_PROP       N       2022         [scr1_top_ahb/j.dcls_compare/dcls_err_out       125632, scr1_top_ahb/j.dcls_compare/dcls_err_out       0       0       1254792       1       0       0       DET_PROP       N       ESIGN AND VERIEICATION	scr1_top_ahb/i_dcls_compare/dcls_err_out 12:	56022 , scr1_top_ahb/i_dcls_compare/dcls_err_out	0	0	125446	52 1	0	0	0	DET_PROP	N	i With all releva
1256062, scr1_top_ahb/i_dcls_compare/dcls_err_out 1256072,         scr1_top_ahb/i_dcls_compare/dcls_err_out 1256082, scr1_top_ahb/i_dcls_compare/dcls_err_out         1256092, scr1_top_ahb/i_dcls_compare/dcls_err_out 1256082, scr1_top_ahb/i_dcls_compare/dcls_err_out         1256092, scr1_top_ahb/i_dcls_compare/dcls_err_out 1256102,         scr1_top_ahb/i_dcls_compare/dcls_err_out 1256112, scr1_top_ahb/i_dcls_compare/dcls_err_out         1256092, scr1_top_ahb/i_dcls_compare/dcls_err_out 1256112, scr1_top_ahb/i_dcls_compare/dcls_err_out         0       0       1254462       1       0       0       DET_PROP       N         1256122, scr1_top_ahb/i_dcls_compare/dcls_err_out 1256132}, propagation strobes :       0       0       1254792       1       0       0       DET_PROP       N       DESIGN AND VERIEICATION **	scr1_top_ahb/i_dcls_compare/dcls_err_out 12	56052 , scr1_top_ahb/i_dcls_compare/dcls_err_out	0	0		0	1	0	0	EOT_SAFE	N	Faults COL
Scr1_top_anb/i_dcls_compare/dcls_err_out 1256102, scr1_top_anb/i_dcls_compare/dcls_err_out 1256112, scr1_top_anb/i_dcls_compare/dcls_err_out 1256132, scr1_top_anb/i_	1256062, scr1_top_ahb/i_dcls_compare/dcls_	err_out 1256072 ,	0	0		0	1	0	0	FOT SAFE	N	Information
scr1 top ahb/i dcls compare/dcls err out 1256112, scr1 top ahb/i dcls compare/dcls err out 1256132, scr1 top ahb/i dcls compare/dcls err out 12561	1256092, scr1 top ahb/i dcls compare/dcls	err out 1256102 ,	-					0				
1256122, scr1_top_ahb/i_dcis_compare/dcis_err_out 1256132}, propagation strobes : 0 0 0 1254792 1 0 0 0 DET_PROP N COLLAR STREET OF AND VERIFICATION ************************************	scr1_top_ahb/i_dcls_compare/dcls_err_out 12	56112 , scr1_top_ahb/i_dcls_compare/dcls_err_out	0	0	125446	1	0	0	0	DET_PROP	N	(2022)
	1256122, scr1_top_ahb/i_dcls_compare/dcls_ {scr1_top_ahb/i_tcm/i_dp_memory/addra[9]1	err_out 1256132}, propagation strobes : 255632, scr1 top abb/i tcm/i do memory/addra[9]	0	0	125479	1	0	0	0	DET_PROP	N 🚽	
	1255642 , scr1_top_ahb/i_tcm/i_dp_memory/a	addra[9] 1255752 ,	total rows: 7022	6 (1 selected)							<u></u>	DVCON
	leert ton abbli temli da momonuladdra[0] 17	155767 cert tan abbii temii da mamanuladdra[0] 🗕	11 1000110003. 7022	o (1 selecteu)								

MUNICH, GERMANY DECEMBER 6 - 7, 2022



SA

Static

Analysis

Config

Safety

Setup

Load

design

SYSTEMS INITIATIVE

HE-FS

Hard Error

fault

simulation

SE-FS

Soft Error

fault

simulation

HE-CM

HE-CA

Constant

Analysis

SE-CA

Constant

Analysis





### Soft Error Analysis Flow







## Calculating AVF

- Multiple SE fault-simulations are performed for each flop
  - Each SE is injected at different time/cycle in the simulation
  - Optima recommends 50 to 100 faults-per flop
- Each fault-simulation can end with

AVF

- **Propagated** The fault propagated to a "safety-critical" node/output
- Detected The fault has ended at Detection Strobe
- Dissipated The fault dissipated or disappeared
- EOT End Of Trace: the fault-sim has reached the end of simulation without any of the results above.
- Optima marks EOT as SAFE or UNSAFE based on a WIDTH parameter.

Number of propagated faults

#### Total fault simulations executed





### Optima-SE<sup>™</sup> Advantage

- Optimal and simple Safety Setup using
  - Find Failure and Detection strobes with Extensive Safety Setup analysis
- User can specify Number of Faults to be injected on a flop
- Fault Placement Times
  - Equal time windows
    - Total stimulus time / number of faults
  - Random Placement Times
    - · Stimulus time divided in to equal windows and in each window random time
  - User specified Times
    - User can specify the particular time stamp fault to be placed on the target flop
- Fault Type
  - Flip fault: The value at the target flop output flipped at the placement timestamp
  - · Constant: A stuck at fault is placed at the target flop for the specified window
- Fastest Simulation Engine for AVF calculations





### FiT Rate with AVF

<u>Without knowing</u> the AVF of each flip-flop

FIT\_chip =
 n \* fit\_unhard

Every Flop Contributes To FIT\_Chip <u>Knowing</u> the AVF of each flop <u>Without hardening</u>  $FIT_chip = \sum_{k=0}^{n} (AVF(k) * fit_unhard)$ 

Lower AVF flops are safe, Hence FIT\_chip is reduced











DECEMBER 6 - 7, 2022

# Security Verification with FAS Fault Attack Simulation



### Fault Attacks

- Fault Injection Attacks are mainstream for hackers
- Differential Fault Analysis (DFA) is very well established
- Hackers use DFA to extract the Information and Secret Assets
- Common fault-injection attacks:
  - Laser fault injection
  - EM fault injection
  - Power fault injection
  - Frequency fault injection
  - Spoofing and changing data on a bus or communication channel
  - Changing password-in to try many combinations
  - Etc.

# FAS Verifies the attack Countermeasures using fault-simulation, on RTL or Gate Level Designs





### FAS: Fault Attack Simulation

• FAS is part of the integrated Solution in Optima-SEC<sup>™</sup>



- FAS gets information from Security Information Flow Analysis
  - Vulnerable portions of the Design
  - Suspicious Trojan insertion point





### Defining FAS

- Complex Attack can be simulated, by defining
  - Target Gate/Node/Flop
  - Type of Fault (SEU, Stuck-at, bridging, etc.)
  - Simulation Time at which attack happens
  - Time span of the attack





# Generating FAS Faults

- Auto Generated
  - Millions of Faults Automatically by using fas\_faults -generate command f with various params
- Manual
  - Targeted on specific flops/gates by using command fas\_faults -add specifying location, fault type and length.

### // Directed random attacks generated by the tool:

```
fas_faults -generate
   -total_attacks 100,000
   -each_attack_hits {5 10}
   -hits_window {50,000 51,000}
   -instance_list {aes_128/r7}
   -group round7
```

```
fas_faults -generate
   -total_attacks 1,000,000
   -each_attack_hits {5 10}
   -hits_window {150,000 160,000}
   -instance_list {aes_128/r8}
   -group round8
```

#### // User specified attacks:

```
fas_faults -add
{ (SEUF,aes_128_dcls/aes_main/s0[127],0,0)
  (SEUF,aes_128_dcls/aes_red/s0[124],50000,0)
  (SEUF,aes_128_dcls/aes_red/s0[126],100000,0)
  (SEUF,aes_128_dcls/aes_red/s0[123],150000,0)
  (SEUF,aes_128_dcls/aes_main/s0[120],200000,0)
}
```

-group manual · · ·





### FAS Campaign and Results snapshot



SYSTEMS INITIATIVE

. . . . . . . . . . . . .



### FAS Attack timing on Block Cypher (AES-128)

From: 0 sec Marker: 145000 ps | Cursor: 400 ps To: 350 ns Signals Waves 1000**0**0 p 200000 ps Time state\_in[127:0] =AA8F5F0361 AA8F+ 4915+ C6E4+ 66E0+ DAEAEA997556EF51585DC3155ADA244B 486C+ FA63+ 282D+ 7E41+ 6878404844DD58F8897317E47887DBAA state out[127:0] =282DF3C46A \*\*\*\*\*\* 282DF3C46AF386254A4E90A70890E546 } Round 3 Round 4 { EE06DA7B876A1581759E42B27E91EE28 The most common target key[127:0] = EE06DA7B87 \*\*\*\*\*\* A7B876A1581759E42B27E91EE2B state in[127:0] =282DF3C46A \*\*\*\*\*\*\*\* 282DF3C46AF386254A4E90A70890E546 D5BFB897317E47887DBAA state out[127:0]=ABD2CDFE37 ABD2CDFE375AB54950A0AFC 14477088311726E71F03F140926C27A3 \* for Attack is: Round 4 Round 5 { kev[127:0] =7F2E2B88F8 7F2E2B88F8443E0980 3CAA+ 7F2E+ 702F+ 7F2E2B88F8443E098DDA7CBBF34B9290 \* <sup>53AG</sup>7<sup>th</sup>-round to final-round 7989+ 14477088311726E71F03F140926C27A3 state\_in[127:0] =ABD2CDFE37 ABD2CDFE375AB54950A0AFC state\_out[127:0] =D46F4F6C55 \* D46F4F6C55B 46F+ A0F7+ 30DD66D8E8FE567F23DDE9D268549304 datapath in AES-128 } Round 5 Round 6 { EC614B851425758C9 key[127:0] =EC614B8514 EC61+ 4258+ EC614B851425758C99FF09376AB49BA7 state in[127:0] =D46F4F6C55 D46F4F6C55B896337E05BB3D7979DE23 \*\*\*\*\*\* F100+ C816+ D46F+ A0F7+ 30DD66D8E8FE567F23DDE9D268549304 state out[127:0]=04F2CA9707 Fault attack on 7<sup>th</sup> round before it is 04F2CA9707782845E22F019649C5D710 62F+ 04F2+ A81B+ DED8C5D3DC392FE5541E04F1BC15A269 260E+ } Round 6 Round 7 { 217517873550620BACAF6B3CC61BF09B key[127:0]=217517873 4E54+ 14F9+ 2175+ 87D3+ 217517873550620BACAF6B3CC61BF09B state in[127:0] =04F2CA9707 260E+ C62F+ 04F2+ A81B+ DED8C5D3DC392FE5541E04F18C15A269 state\_out[127:0]=B7AAE4C51D 37AAE4C51D252D4F6C920F8194E58150 5A41+ D187+ B7AA+ 8951+ 2688F7A9E81A481E7815350A1B222619 for DFA Bound 7 Round 8 { 0EF903333BA9613897060A04511DFA9F EAD2+ 4743+ 0EF9+ CBA2+ 0EF903333BA9613897060A04511DFA+ key[127:0] =xxxxxxxxxxx \*\*\*\*\*\* state in[127:0] =B7AAE4C51D B7AAE4C51D252D4F6C920F8194E58150 5A41+ D187+ B7AA+ 8951+ 26B8F7A9E81A481E7815350A1B222619 \* state out[127:0] =xxxxxxxxxx 23E78C3C132163DBAAC0C6572E03CB95 EA83+ FDE3+ 23E7+ 4C39+ 442406B6D951389D404D63C4+ } Round 8 Round 9 { key[127:0] =xxxxxxxxxxx B1D4D8E28A7DB9DA1D7BB3DE4C664941 AC77+ 5499+ B1D4+ 6973+ B1D4D8E28A7DB9DA1D+ \*\*\*\*\*\*\* 23E78C3C132163DBAAC0C6572E03CB95 EA83+ FDE3+ 23E7+ 4C39+ 442406B6D951389D404D63C4+ state\_in[127:0] =xxxxxxxxxx state out[127:0] =xxxxxxxxxx \* 7FFE0E9551A566350E347C472929ECCB EB40+ BD6E+ 7FFE+ DD9D+ 83F75DD088F38-} Round 9 Final Round { key in[127:0] =xxxxxxxxxx \*\*\*\*\*\* B4EF5BCB3E92E21123E951CF6F8F188E D014+ 1311+ B4EF+ C477+ B4EF5BC+ EB40+ BD6E+ 7FFE+ DD9D+ 83F75DD088F384 state in[127:0] =xxxxxxxxxx 7FFE0E9551A566350E347C472929ECCB 66E94BD4EF8A2C3B884CFA59CA342B2E 3925+ 69C4+ 66E9+ 0545+ 5+ state\_out[127:0] =xxxxxxxxxx \*\*\*\*\*\*\* } Final Round Cipher Text { out[127:0] =xxxxxxxxxx 66E94BD4EF8A2C3B884CFA59CA342B2E 3925+ 69C4+ 66E9+ 0545+ 5+ \* Cipher Text

SYSTEMS INITIATIVE

# DFA for Block Cypher attacks

- Attack Location
  - AES Data path
  - AES Key Schedule
  - Single Byte
  - Multiple Byte
- Attacks are based on
  - DFA algorithms
  - Brute Force
- Attacks Discussed in this presentation
  - Attack 1: First round single bit
  - Attack 2: Single bit at 9<sup>th</sup> round input
  - Attack 3: On Time Redundancy Counter Measure
  - Attack 4: On Parity Bit Counter Measure





## Attack 1: Single Bit at 9<sup>th</sup> round input

- First round attacks are not practical, so attack the 9<sup>th</sup> round
- Single bit arbitrary fault at input of 9<sup>th</sup> round
- As demonstrated by Piret et al\*, The fault propagates through rounds as below



\* Piret, G., Quisquater, J.-J.: A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD.
In: Walter, C.D., Ko,c, C, .K., Paar, C. (eds.) CHES 2003. LNCS, vol. 2779, pp. 77–88. Springer, Heidelberg (2003)

"Shift





### Attack 1: modelling

• fas\_faults -add {
 (SEUF,
 aes\_128/r8/state\_out[127],
 265000,
 0)
 }
 -group r9\_in\_bit

0	4	8	12
127120	9588	6356	3124
1	5	9	13
119112	8780	5548	2316
2	6	10	14
111104	7972	4740	158
3	7	11	15
10396	7164	3932	70





# Attack 1: Faults at Final Output

fas\_faults -add {(SEUF,aes\_128/r8/state\_out[127],265000,0)} -group r9\_in\_bit

- FAS result: information leaked
- Decision time: 305,000

#### FAS result:

Information leaked (16)times (strobe\_name,
observation\_time):

(aes 128/out[18],	305000)	(aes 128/out[46],	305000)
(aes_128/out[19],	305000)	(aes_128/out[21],	305000)
(aes_128/out[42],	305000)	(aes_128/out[44],	305000)
(aes_128/out[43],	305000)	(aes_128/out[67],	305000)
(aes_128/out[66],	305000)	(aes_128/out[17],	305000)
(aes_128/out[16],	305000)	(aes_128/out[23],	305000)
(aes_128/out[45],	305000)	(aes_128/out[127],	305000)
(aes_128/out[126],	, 305000)	(aes_128/out[122]	, 305000)



### These results match 100% expected behavior according to proposed



attack by Piret et al.



### Attack 2: on Time Redundancy Counter Measure

- Some attacks beat Hardware redundancy
- Same fault in main AES as well as redundant AES
- Generate FAS attacks to target
  - Flops both in aes\_main and aes\_red

#### Modelling

```
fas_faults -generate
-total_attacks 1000000
-each_attack_hits 2
-hits_window {105000 305000}
-instance_list {aes_128_dcls/aes_main
aes_128_dcls/aes_red} -group_oneM_2flops
```





### Attack 3: on Parity-bit Countermeasure

- Two faults hit the same byte in the state
- Hit cycles separated by 8 rounds distance
  - E.g. 1<sup>st</sup> round 127-bit and 8<sup>th</sup> round 127-bit
- FAS attack model

```
fas_faults -add {
 (SEUF,aes_128/r1/t0/t0/s4/S_/out[0],115000,0) //1<sup>st</sup> round input
 (SEUF,aes_128/r7/state_out[127],245000,0) //8<sup>th</sup> round input
 }
-group r1 r8 parity attack
```

Information is leaked from Ineffective Faults







### Laser Attack FAS modelling

- Attack Origin: Location of the Attack
- Radius of the attack: Laser focus radius
- PAG: Potentially attacked Gates
  - No Of Gates Under the Laser spot
  - Changes with technology node, more gates in lesser technology node
  - At 22nm assumed to be 100 gates
- Laser Intensity
  - More power more gates influenced
  - Depends on radius, more radius less intensity
- Duration of the Attack: How long IC is irradiated
  - This influences the logic value duration to be modelled
- Each attack done in one pulse
  - In multiple laser pulses, after first pulse, the attack is detected and cleared, so need to model only one pulse at a time





### PAG: Potentially Attackable Gates

- R7\_logic
  - Laser focused on R7
  - Larger radius
- R8\_logic
  - Laser focused on R8
  - Medium radius
- R9\_logic
  - Laser focused on R9
  - Smaller radius







### Laser FAS attack: PAG8, PAG4, PAG2

- Design Used: AES-128 without protection
- Generated 10,000 FAS's for each attack (laser location)
- R7\_logic
  - \$PAG\_r7\_logic is the list of gates affected by Laser on R7 logic
    - fas\_faults -generate
    - -total\_attacks 10000
    - -each\_attack\_hits 8
    - -timing\_window {225000 235000}
    - -flops\_list {\$PAG\_R7\_logic}

#### Info Leak FAS attacks 7276 out of 10,000 PAG8

• R8\_logic

IS INITIATIVE

- \$PAG\_r8\_logic is the list of gates affected by Laser on R7 logic
  - fas\_faults -generate
  - -total\_attacks 10000
  - -each\_attack\_hits 4
  - -timing\_window {245000 255000}
  - flops\_list {\$PAG\_R8\_logic}

#### Info Leak FAS attacks 7522 out of 10,000 PAG4



- \$PAG\_r8\_logic is the list of gates affected by Laser on R7 logic
  - fas\_faults -generate
  - -total\_attacks 10000
  - -each\_attack\_hits 2
  - -timing\_window {265000 275000}
  - -flops\_list {aes\_128/r9/state\_out[127:0]}

#### Info Leak FAS attacks 7523 out of 10,000 PAG2



# Performance

- AES-128 is injected with 10 Million FAS
- R7\_logic chosen
  - All adjacent 4-bits are injected with faults at random times
  - \$PAG\_R7\_logic → aes\_128/r7/state\_out[127:0]
- Attack modelling
  - fas\_faults -generate
  - -all\_combinations
  - -each\_attack\_hits 4
  - -timing\_window {225000 235000}
  - -flops\_list {\$PAG\_R7\_logic}
  - -group 10M
- Single Thread
  - 10,668,000 faults run in 14,850 sec. (4Hrs 7min.) → 0.00139 sec per FAS attack
- 20 Threads (10times Faster)
  - 10,668,000 FAS's with 1,504 sec. (25 min) → 0.000141 sec per FAS attack

### Over 10 million FAS's in 25 min! (Single machine)





### Hardware fault Injection: CAPEC-624

- CWE-1247: Improper Protection Against Voltage and Clock Glitches
  - A device needs to guard against fault attacks such as voltage glitches and clock glitches that an attacker may employ in an attempt to compromise the system.
- CWE-1248: Semiconductor Defects in Hardware Logic with Security-Sensitive Implications
  - These defects manifest as faults on chip-internal signals or registers, have the effect of inputs, outputs, or intermediate signals being always 0 or always 1, and do not switch as expected.
- CWE-1332: Improper Handling of Faults that Lead to Instruction Skips
  - Attackers can use fault injection techniques to alter the operating conditions of hardware so that security-critical instructions are skipped more frequently or more reliably than they would in a "natural" setting.





### Hardware fault Injection: CAPEC-624 Contd...

- CWE-1256: Improper Restriction of Software Interfaces to Hardware Features
  - Software-controllable mechanisms to dynamically scale device voltage and frequency and monitor power consumption are common features in today's chipsets, but they also enable attackers to mount fault injection and side-channel attacks without having physical access to the device.
- CWE-1261: Improper Handling of Single Event Upsets
  - The hardware logic does not effectively handle when single-event upsets (SEUs) occur.
- CWE-1319: Improper Protection against Electromagnetic Fault Injection (EM-FI)
  - The device is susceptible to electromagnetic fault injection attacks, causing device internal information to be compromised or security mechanisms to be bypassed.
- CWE-1334: Unauthorized Error Injection Can Degrade Hardware Redundancy
  - An unauthorized agent can inject errors into a redundant block to deprive the system of redundancy or put the system in a degraded operating mode.





### Blackbox Reverse Engineering CAPEC-189

- CWE-1255: Comparison Logic is Vulnerable to Power Side-Channel Attacks
  - The power consumed by a device may be instrumented and monitored in real time. Attacker can inject faults to alter the power profile and get the information





2022 DESIGN AND VERIFICATION TH DVCDN CONFERENCE AND EXHIBITION

> MUNICH, GERMANY DECEMBER 6 - 7, 2022

Thank you!

