

Embedded Analytics and Automotive Security

Aileen Smith
Chief Strategy Officer





Corporate Overview

- VC-funded start-up
 - Recently completed round D (\$6M)
- Founded 2009
- Headquarters in Cambridge UK
- 44 patents
- New Chairman October 2017
 - Alberto Sangiovanni-Vincentelli
- Industry leaders adopting UltraSoC
- Silicon-proven with multiple customers





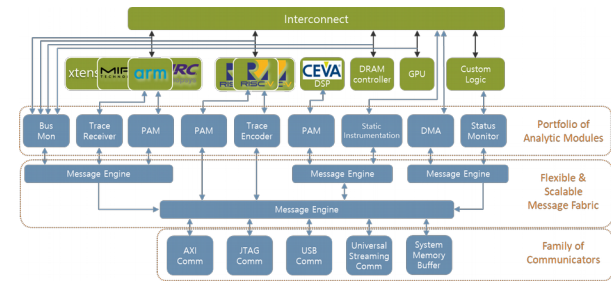
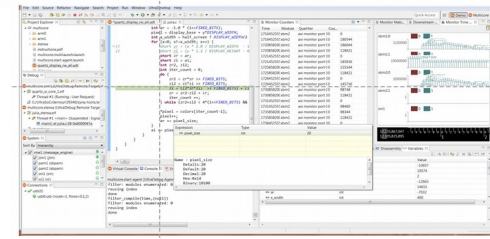
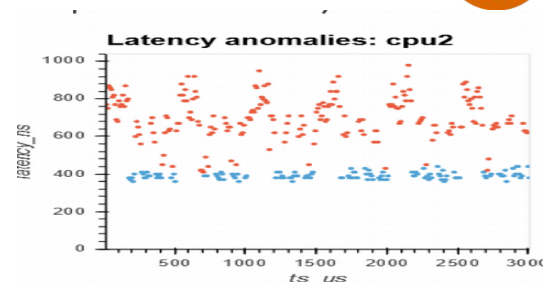
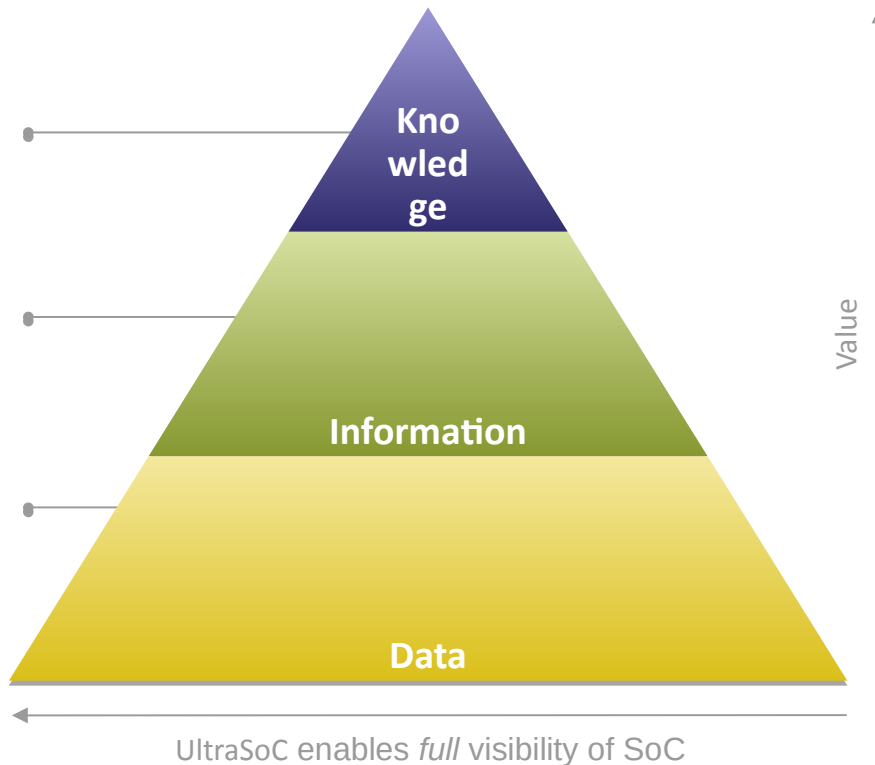
Actionable Insights across the whole SoC



UltraSoC delivers actionable *insights*

With system-wide *understanding*

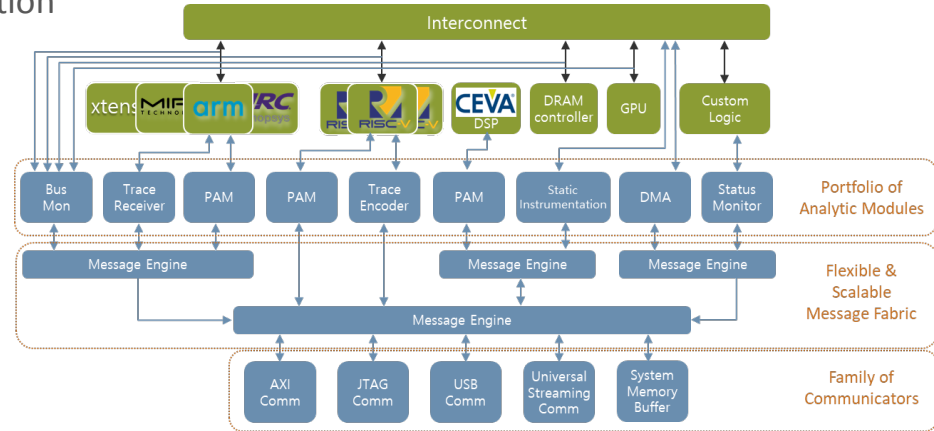
From rich *data* across the whole SoC





A coherent architecture to debug, develop, optimize & secure

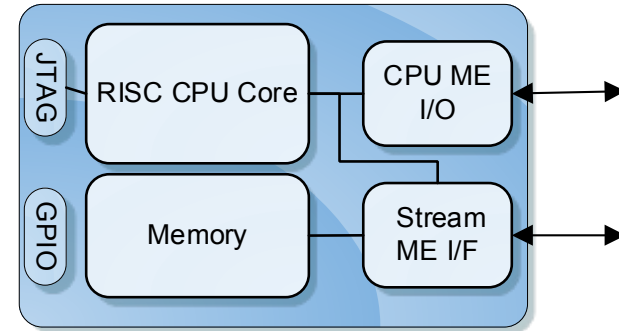
- Full SoC visibility, HW & SW
- Support all architectures: Freedom of IP selection
- Real-time & non-intrusive
- Advanced analytics & forensics
- “in life” analytics & SLA compliance
- Supports Functional Safety
- Supports Bare Metal Security™



UltraSoC Embedded Analytics

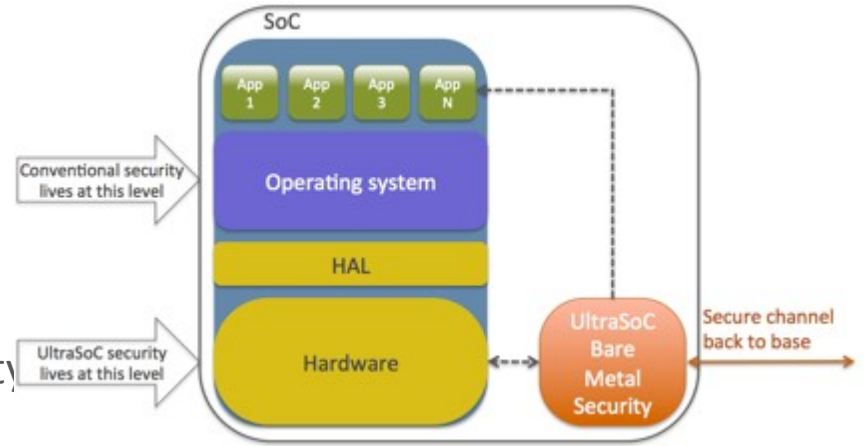


- Analytics subsystem running continuously, analysing, monitoring for safety and security, reconfiguring H/W parameters as required
 - AI/ML algorithms define “normal” SoC behaviour and identify deviations from the norm
- Hardware resources are configurable at runtime
 - Allows reuse of hardware resources for different scenarios and different algorithms
- Security and safety of systems
- Hardware provides data so CPU load is small
- Fastest speed of detection



➔ Bare Metal Security: a different layer

- Re-use the logic for debug
 - *“Is the system operating as expected?”*
- Hardware-based, under the OS
- Completely independent monitoring system
- Invisible to main system
- Very hard to detect or subvert
- Consistent and integrated with functional safety
- Supports requirements of SAE 3061 cybersecurity for automotive
- Complements other security architectures
 - *“intruder alarm” versus “lock”*






SAE J3061 Cyber Security for Automotive



• SAE J3061 and ISO/SAE 21434 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

- Tailors a cybersecurity process framework from the ISO 26262 process framework
- Cybersecurity and functional safety share parallel processes
 - Threat analysis and risk assessment vs hazard analysis
 - Attack tree analysis vs fault tree analysis
- Cybersecurity countermeasures should be consistent with safety measures and safety mechanisms
- The cybersecurity and functional safety teams need to interact
- Implies need for hardware elements for cybersecurity

• UltraSoC monitors can support both safety and cybersecurity

 SURFACE VEHICLE RECOMMENDED PRACTICE	J3061™	JAN2016
	Issued	2016-01
Cybersecurity Guidebook for Cyber-Physical Vehicle Systems		

RATIONALE

To provide a cybersecurity process framework and guidance to help organizations identify and assess cybersecurity threats and design cybersecurity for cyber-physical vehicle systems throughout the entire development lifecycle process.

- Defines a complete lifecycle process framework that can be tailored and utilized within each organization's development processes to incorporate cybersecurity into cyber-physical vehicle systems from concept phase through production, service, and decommissioning.
- Provides high-level guiding principles.
- Provides information on existing tools and methods.
- Provides the foundation for further standards development.

TABLE OF CONTENTS

1.	SCOPE	5
1.1	Purpose	5
1.2	When to Apply to Cybersecurity Process	6
2.	REFERENCES	6
3.	DEFINITIONS AND ACRONYMS	8
4.	RELATIONSHIP BETWEEN SYSTEM SAFETY AND SYSTEM CYBERSECURITY	17
4.1	Analogies between System Safety and System Cybersecurity Engineering	18
4.2	Unique Aspects of System Safety and System Cybersecurity	18
5.	GUIDING PRINCIPLES ON CYBERSECURITY FOR CYBER-PHYSICAL VEHICLE SYSTEMS (COPV)	20
5.1	Know Your System's Cybersecurity Potential	20
5.2	Understand Key Cybersecurity Principles	22
5.3	Consider the Vehicle Owner's Use of the System	21
5.4	Implement Cybersecurity in Concept and Design Phases	21
5.5	Implement Cybersecurity in Development & Validation	21
5.6	Implement Cybersecurity in Incident Response	22
5.7	Cybersecurity Considerations When the Vehicle Owner Changes	22

SAE Technical Standards Board Rules provide that: "This report is submitted to SAE as advisory material and engineering information. The use of this report is entirely voluntary and its application and use is at the discretion of the user. It is not intended to be a standard. It is not intended to be used for certification purposes." This report is a SAE document and may be used for any purpose, but it is not intended to be a standard. It is not intended to be used for certification purposes.





Resilience

i) the ability to maintain a core purpose or

ii) the ability to restore core purpose in the face of a disruption

- Partner with ResilTech (Italy) who are leaders in this space and consult on ISO 26262
- Partner with Moortec (on-chip PVT sensors) for resilience checking e.g. load balancing based on temperature

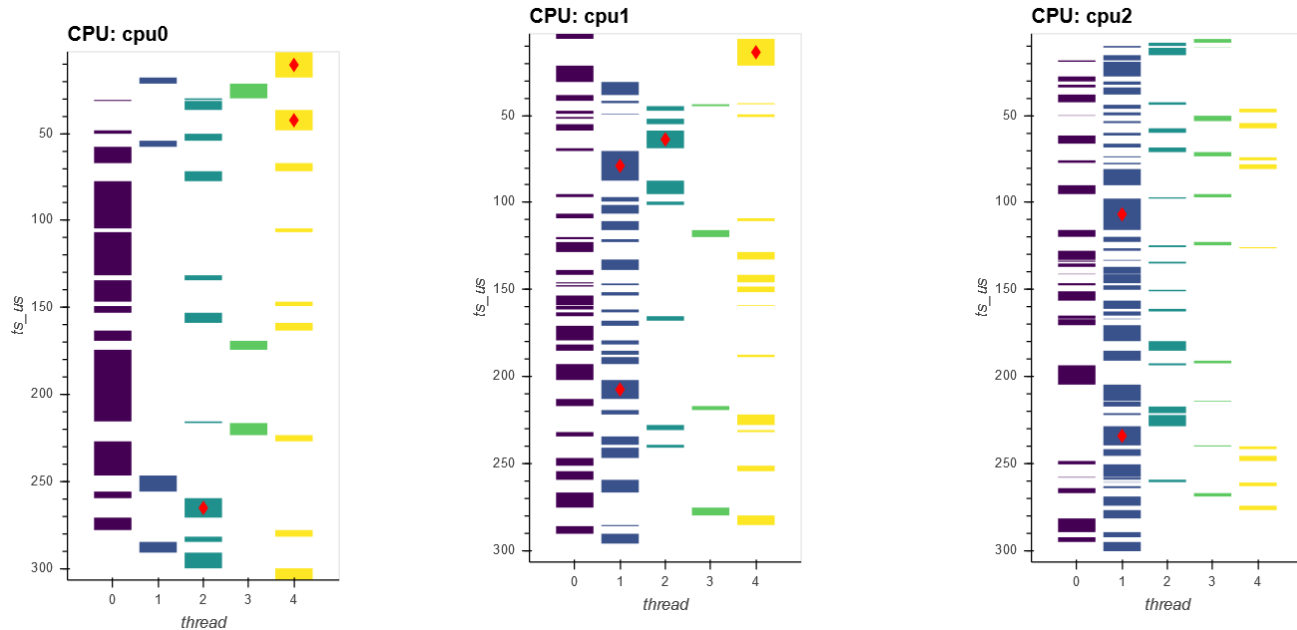
Security – Real-time monitoring

- Challenge Response
- Authentication
- Alarm Function (hacking, intrusion)
- UltraSoC provides Bare Metal security as well as message encryption
- Interaction between software and existing hardware (post silicon).
- Ensure software updates do not have a negative effect on system integrity

Safety – Real-time monitoring

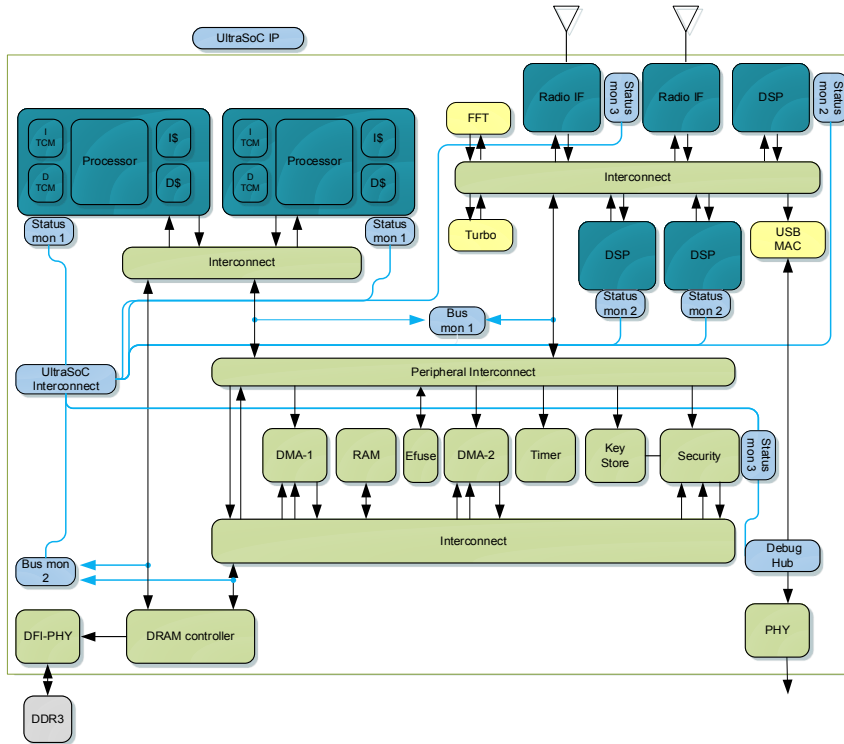
- Hardware monitoring that system is working within limits
- Hardware monitoring to warn that system is working outside limits
- UltraSoC can be used to monitor Data Corruption or implement Lock-Step

Fastest time to detection





Example 2 – Hardware layer security



Check accesses to E-Fuse and Key Store

Use Bus mon 1' to capture accesses to the E-Fuse and Key Store entities

```

if <Address> >= MemAddressL && <Address> <
MemAddressH
&& NOT (<Id> >= IdL && <Id> <= IdH)
then if Count > 0
    CaptureTrace()
    SendEventMessage()
else
    IncrementCount()
fi

```

Where:

- <> are Interconnect fields being observed by the bus monitor.
- CaptureTrace() puts the transaction into the trace buffer
- SendEventMessage() is an instruction to the monitor to send an event out on UltraSoC's message bus
- IncrementCount increments the counter by 1 (allows for BootRom access)

NB This is pseudo-code actual filtering is in hardware and not software
 5 April 2018

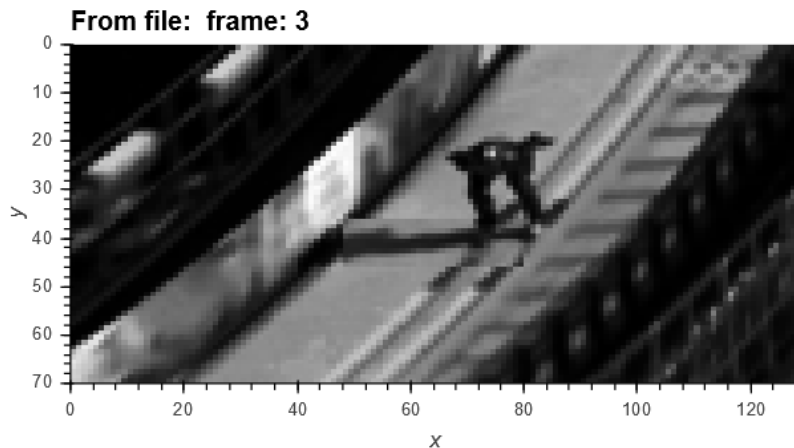


Example 3 – Non-intrusive “stuck pixel” detection

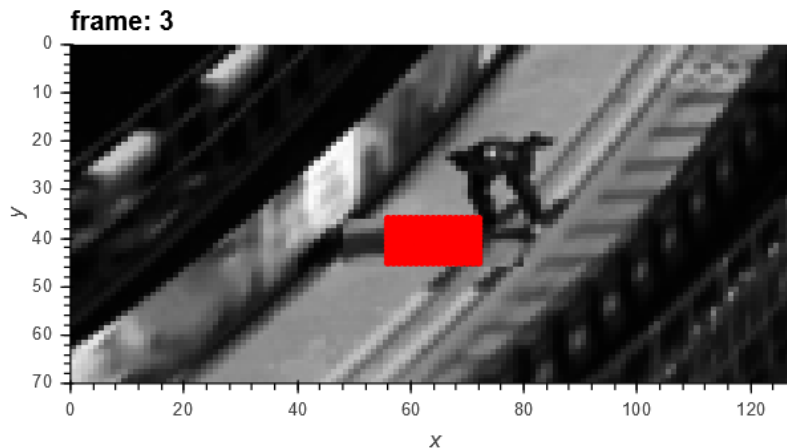


Fastest time to detection

Incoming image



Detected stuck pixels



UltraSoC Security & Embedded Analytics

- The only commercial heterogeneous solution
- Non-intrusive, wire-speed monitors
- Integration Simplicity

- Enables in-life monitoring and fastest detection
 - Reliability, Compliance & Bare-Metal Security™



Contact details:

Aileen Smith

aileen.smith@ultrasoc.com

www.ultrasoc.com

 @UltraSoC

