UCAIug Open-SG Security: Update on Embedded Systems Security Task Force Activities

Rohit Khera Rohit.Khera@sandc.com, Mark Ward mfw5@pge.com

07/20/2011

Agenda

- Organization and Summary
- Deliverables
- Update on Random Number Generation
- Update on Performance Metrics
- Update on Secure MCUs
- Update on Device Resilience & Robustness
- Update on Secure Protocols
- Device Security Management
- Is There Sufficient Granularity in Extant Certification Standards to Address Embedded Security

Organization & Contact Info

Chairs

- Rohit Khera – Rohit.Khera@sandc.com (S&C Electric)
- Mark Ward – mfw5@pge.com (Pacific Gas & Electric)

- Sharepoint

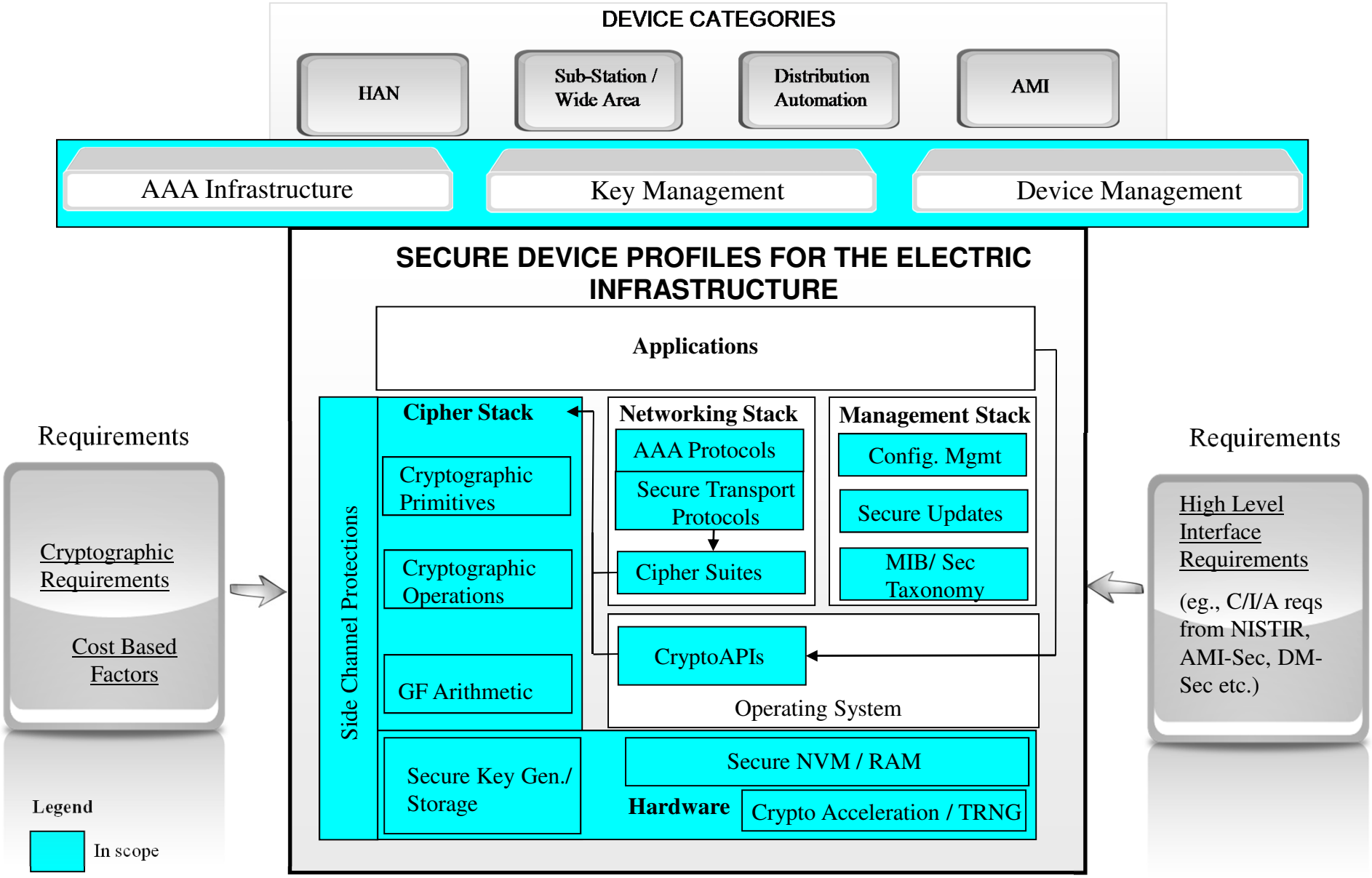
http://osgug.ucaiug.org/utilisec/embedded/default.aspx

- Email Reflector – 'OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG'

Bi-Weekly Co-ordination and status calls

Secure Device Profile Components

Create multiple secure profiles to address disparate device resource characteristics and communication infrastructures across multiple device categories – leverage existing standards / SDOs



Deliverables and Assignments

Device Security (Lead Marc Vauclair, NXP)

Topic	Primary Owner/s	Secondary Owner/s	Start Date / Status	Est. Completion
Cryptographic Hardware	Shrinath Eswarahally (Infineon) Shrinath.Eswarahally@INFINEON.COM	Chris Gorog (Deloitte) cgorog@deloitte.com	Underway (first draft submitted)	
Random Number Generation	Sami Nassar (NXP) sami.nassar@NXP.COM Marc Vauclair (NXP) marc.vauclair@NXP.COM	Rohit Khera (S&C Electric) Rohit.Khera@sandc.com		
Device Identity	Sami Nassar (NXP) sami.nassar@NXP.COM Marc Vauclair (NXP) marc.vauclair@NXP.COM Mike Ahmadi (GraniteKey/NXP) mike.ahmadi@GRANITEKEY.COM	Sadu Bajekal (IBM) sbajekal@US.IBM.COM		

Deliverables and Assignments

Device Security (Lead Marc Vauclair, NXP)

Topic	Primary Owner/s	Secondary Owner/s	Start Date / Status	Est. Completion
Secure Protocols	Rohit Khera (Rohit.Khera@sandc.com)	James Blaisdell (JBlaisdell@mocana.com)		
Device Authentication and Access Control	Sami Nassar (NXP) sami.nassar@NXP.COM Marc Vauclair (NXP) marc.vauclair@NXP.COM	Chris Gorog (Deloitte) cgorog@deloitte.com		
Key Management	David Sequino (Green Hills Software) dsequino@GHS.COM Chris Dunn (Safenet) chris.dunn@SAFENET-INC.COM Gib Sorebo (SAIC) sorebog@SAIC.COM	Sami Nassar (NXP) sami.nassar@NXP.COM Marc Vauclair (NXP) marc.vauclair@NXP.COM Chris Gorog (Deloitte) cgorog@deloitte.com		

Deliverables and Assignments

Device Security Management (Lead TDB)

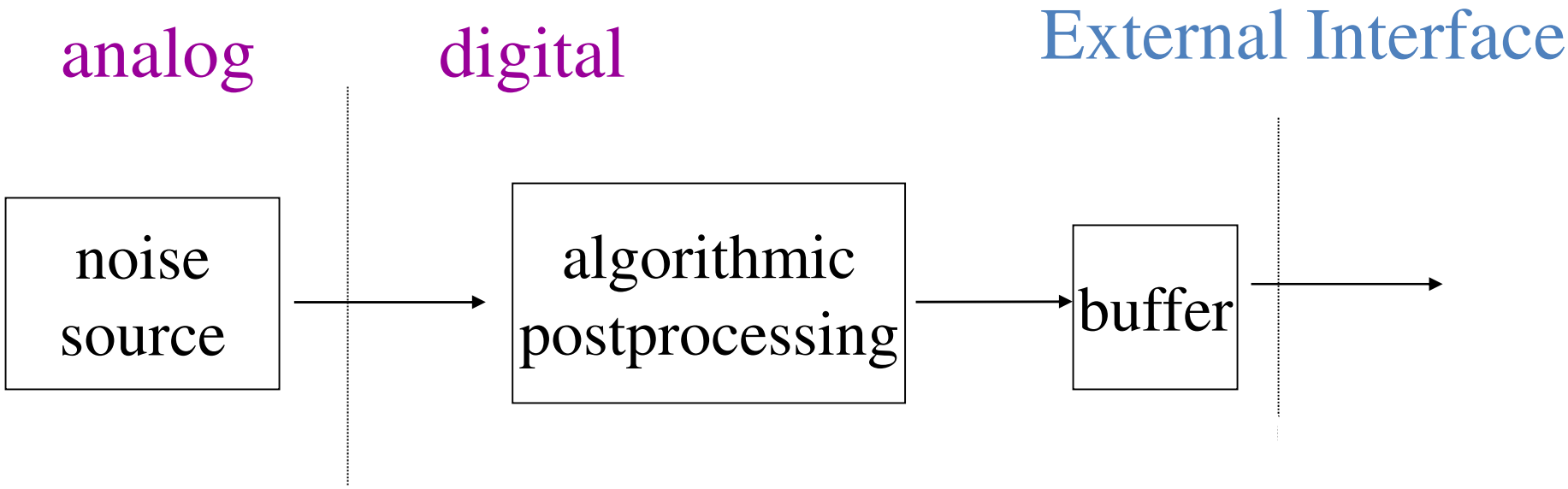
Topic	Primary Owner/s	Secondary Owner/s	Start Date / Status	Est. Completion
Device Mgmt	None	Sami Nassar (NXP) sami.nassar@NXP.COM Marc Vauclair (NXP) marc.vauclair@NXP.COM Steve Dougherty (IBM) sdougherty@US.IBM.COM Sadu Bajekal (IBM) sbajekal@US.IBM.COM		

Deliverables and Assignments

Misc.

Topic	Primary Owner/s	Secondary Owner/s	Start Date / Status	Est. Completion
Ciphers (refer to NISTIR 7628 Crypto Section)	Rohit Khera (S&CElectric Rohit.Khera@sandc.com	Daniel Thanos (GE) Daniel.Thanos@GE.COM	Underway	
Device Robustness & Resilience	Bora Akyol (PNNL) bora@PNL.GOV Daniel Thanos (GE) Daniel.Thanos@GE.COM	Chris Gorog (Deloitte) cgorog@deloitte.com		

True Random Number Generation – Schematic View



Ref: Werner Schindler[1], Wolfgang Killmann[2]
Evaluation Criteria for
True (Physical) Random Number Generators
Used in Cryptographic Applications

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI) Bonn, Germany

[2] T-Systems ISS GmbH Bonn, Germany

Random Number Generation

- Proposal to use German Federal Office for Information Security(BSI) functionality Classes for physical random number generators (AIS 31)

  CLASS P1 Applications (Less sensitive)

  1) Challenge Response Protocols
  2) Initialization Vectors
  3) Seeds for Deterministic Random Number Generators

  CLASS P2 Applications (Highly sensitive)

  1) Signing Key Pairs
  2) DSS Signature Generation
  3) Random Padding Bits

- FIPS 140 -2 , NIST SP 800-90 for deterministic random number generation

TRNG Testing

tot-test	shall detect a total breakdown of the noise source
startup test	shall ensure the functionality of the TRNG on startup
online test	shall detect deterioration of the quality of random numbers

Desirable to detect catastrophic failures in DAS randoms, viz., when entropy/bit = 0, need to model underlying statistical distribution of variable

Ref: Werner Schindler[1], Wolfgang Killmann[2]
Evaluation Criteria for
True (Physical) Random Number Generators
Used in Cryptographic Applications

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI) Bonn, Germany

[2] T-Systems ISS GmbH Bonn, Germany

Software Performance on Common Application MCUs

Performance numbers are a mix of mode averages. Your actual performance numbers will be different (e.g. signing and sign verification dramatically different operations). We are happy to provide a more detailed and complete report under NDA. To request our detailed, broken out performance metrics, please visit http://mocana.com/nanocrypto-performance-metrics/.

	Operational Environments			
Subset of Algorithms	Cell Processor	ARM (IXP 425; 133MHz)	PowerPC 1.5GHz	64-bit x86
AES-CBC (Average keysize 128-256); message size = 1024B; results in KB/sec	41242.60	837.26	35560.73	83764.53
AES-CTR-128 (Average of message size = 16, 64, 256, 1024, 8192); results in KB/sec	47848.58	988.77	39603.14	102490.18
SHA256 (average of message size = 16, 64, 256, 1024, 8192); results in KB/sec	30397.99	1393.36	36241.02	56519.16
SHA512 (average of message size = 16, 64, 256, 1024, 8192); results in KB/sec	11142.95	339.29	11781.44	1005822.80
AES-GCM 64KB lookup (average of message size = 16, 64, 256, 1024, 8192); results in KB/sec	30634.14	700.93	29415.38	73732.22
AES-GCM 4KB lookup (average of message size = 16, 64, 256, 1024, 8192); results in KB/sec	35738.24	734.36	30006.16	61944.12
AES-GCM 256B lookup (average of message size = 16, 64, 256, 1024, 8192); results in KB/sec	29214.74	592.51	24688.70	46144.64
DH group 2: Average of less optimized algorithm and highly optimized algorithm and full and half DH calculations; number calculations per second	172.60	13.17	170.01	910.65
ECDSA average signing w/ blind and sign verification and less otimized and highly optimized algorithms for p-192; calculations per second	933.54	43.66	910.92	3961.32
RSA average decryption, signing w/ blind and verification less optimized and highly optimized algorithm; calculations per second; keysize 2048	519.74	18.92	449.92	2433.20

More Cryptographic Performance Metrics

From ref(1) on Intel Core 2 1.83 GHz processor under Windows Vista in 32-bit mode Milliseconds/Operation

RSA 2048 Signature	6.05ms
RSA 2048 Verification	0.16ms
ECDSA over GF(p) 256 Signature	2.88ms
ECDSA over GF(p) 256 Verification	8.53ms
ECDHC over GF(p) 256 Key-Pair Generation	2.87ms

Secure MCUs
33MHz

RSA 2K signatures – 42 ms (generation) 1ms (verification)
ECC 224 signatures – 4.6 ms (generation) 9.2 (verification)

References

- 1) Crypto++ 5.6.0 Benchmarks, http://www.cryptopp.com/benchmarks.html (on Intel Core 2 1.83 GHz processor under Windows Vista in 32-bit mode)

Draft Requirements – Secure MCUs

- Onboard Co-processors
- Fully Encrypted CPU core and cache.
- Onboard True Random Number generator: capable in accordance with FIPS 140-2
- Strong Block cipher Encrypted memories and their buses.
- Encrypted Bus and registers for peripherals access.
- Built in error detection capability
- Memory Bus and peripheral Bus are not exposed outside the IC Package. Limited 2-3 signals for communication.
- CRC generator
- Dynamic Power management modes.
- Open Standard Communication interface and protocol.
- Asymmetric crypto processor : To support key length for RSA upto 4096 and ECC 512.
- Symmetric crypto coprocessor for AES/3DES (?) : High speed engine to run AES 256 Encryption/Decryption. Capable of running 3DES (?) algorithm.

Draft Requirements – Secure MCUs

Accessible Memory

Utility accessible memory shall be secure (factory lockable and Utility lockable), programmable and non-volatile during the production processes.

IC Security

Hardware and software (logical) tamper-resistance.

Security/exception sensors such as voltage, frequency, and temperature.

A design to prevent unauthorized access via hardware and software security features.

Auto detection if tamper attempt is made.

Attack Security

DFA = Differential Fault Analysis

SPA = Simple Power Analysis

DPA = Differential Power Analysis

DEMA = Differential Electro-Magnetic radiation Analysis

Common Criteria, Protection Profiles, Vulnerability Assessment Activities, Side Channel Attacks

Electro Static Discharge (ESD) protection

Security policy complies with the Common Criteria EAL4+ (ISO/IEC objectives and requirements in a document specified by ISO/IEC 27002.

The IC Memory Management shall have:

Secure EEPROM/Flash on the same IC

Durability (data retention): At least 15-20 years

Anti-tearing reading/writing mechanisms

The memory shall support a minimum of 500K read/write cycles without failure or performance degradation.

UNIQUE IC SERIAL NUMBER

Unique IC shall be obtainable by reading the Chip UID

Unique serial number shall be stored internally in the IC and not printed on the surface of the IC or IC package

Approaches for Integrating Secure Hardware

- ***Monolithic / Single Die***

  Example – Smart Cards (Cryptographic / Security boundary encompasses the entire system)

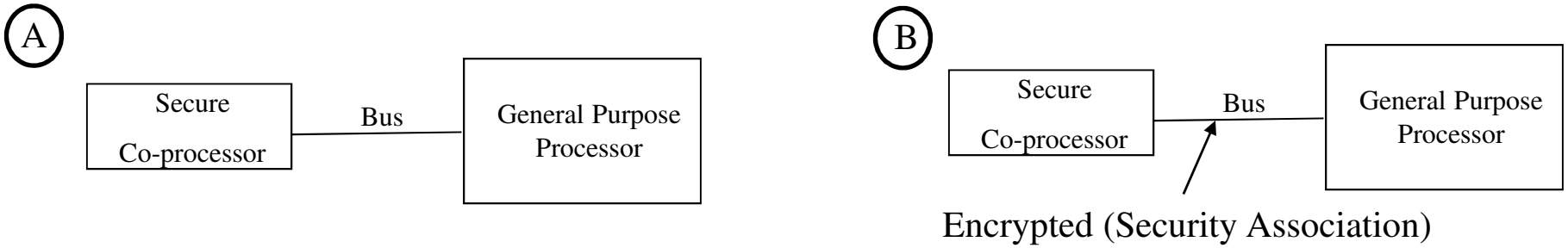
  Advantages – Entire system contained within boundary

  Dis-Advantages – Low word size (typically 16 bit) and clock rating

- ***Co - Processor***

  Advantages – Augment security functions, secure key storage, acceleration, side channel protections etc.

  Dis-Advantages – Cleartext traverses bus to general purpose MCU?



Typical Secure MCU Layout

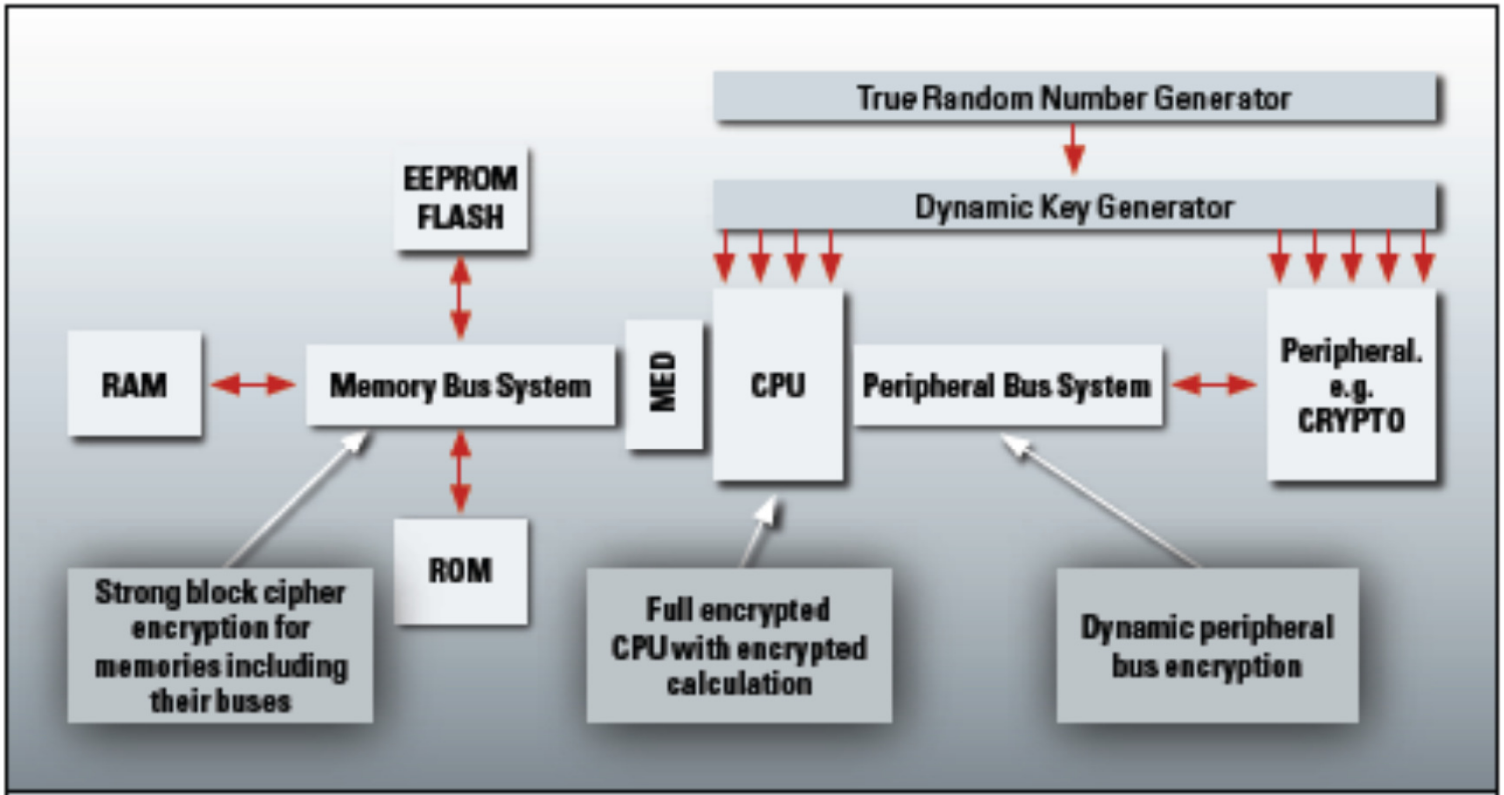


Fig. 5: Full Encryption throughout the chip

Device Robustness & Resilience (Select Outline & Topics)

Architectural principles for both hardware and software components; protection and detection of physical device boundaries; defense against denial of service attacks; operational continuity and protocol implementation guidelines

- **Hardware Principles**

  watchdog timers, interrupt coalescing, virtual memory/memory protection support, thread priorities

- **Network Communication Interfaces**

  Timing, voltage, temperature,

  Network interface robustness against:

  - DoS conditions (e.g. network flooding)
  - Well-known packet vulnerabilities (e.g. LAND ATTACK)

  Malformed/Fuzzed Packets from L1 to L7.

- **CPU Resource Conservation**

  All mission critical devices require conservative CPU and memory resource margins in order to remain resilient against many types of faults and resource exhausting attack

- **Memory and Storage Conservation**
- **Battery and Power Conservation**
- **Continuing to Operate Under Adverse Conditions**

Device Management

- Current discussions center around understanding the device landscape
  - What types of devices are out there?
  - How are they currently managed?
  - What are the constraints of these devices?
  - What protocols are used?
- Management of firmware updates, device settings, data storage and management, etc.
- Considering the re-purposing of device management from other industries (e.g. mobile devices)
- Challenged by the legacy device vs. “Green Field” dilemma
  - Re-purposing device management methods from other industries potentially works as we work toward building newer devices
  - Many legacy devices are not “broken” , so why fix them?

Secure Protocols

Provide guidance around Performance Characterization, Implementation Guidelines (Some overlap w/ Device Robustness Resilience), PKI/Key Mgmt. Integration

- **IP Based**

  D/TLS , IPSec, SSH

Authentication

Radius/Diameter, EAP/PANA, LDAP, Kerberos**,** Multicast (GDOI?)

- **Non IP Based**

  DNP Secure Authentication, AGA-12, IEEE P1711, EAP, WPA2

- **Othe**r

  XMPP

Is There Sufficient Granularity in Certification Standards to Address Embedded Security ?

Select Security Validation & Certification Requirements (Taken from Proposed Certification Standard IEC 62443-2-4).

Process Area	Certification Requirements
Vendor Organizational Processes	1) Vendor should have policies & procedures to support a utility's security incident response team 2) Vendor should create security policies & standards related to internal processes & enforce these within its organization & subcontractors 3) Vendor should conduct background checks on personnel involved with security development 4) Vendor shall designate a security point of contact for utility customers 5) Vendor shall participate in at least one industry security standards group
Vendor Control System Capabilities	1) Vendor should document security requirements around OS hardening, data flows of sensitive information and data retention capabilities 2) Vendor shall document security testing procedures for integrated third party software 3) Vendor shall conduct & document 3rd party security & architecture reviews 4) Vendor shall document protections undertaken to secure communication protocols 5) Vendor system shall support commercial anti-virus or alternative mitigations 6) Vendor shall provide evidence that its systems are checked to be free of malicious code prior to shipping to the customer 7) Vendor should define and document a software patching policy 8) Vendor should provide access to all software patches and service packs relevant to its systems 9) Vendor shall provide tools to audit the security patch status of its systems 10) Vendor shall provide password management functions for its systems 11) Vendor shall provide functions to rotate, protect & encrypt passwords 12) Vendor's systems shall provide role based access and support for centralized access and policy management 13) Vendor shall be able to generate logs of individual account access activity for a minimum of 90 days 14) Vendor systems shall support utility backup and restore functions

Is There Sufficient Granularity in Certification Standards to Address Embedded Security ?

Select Security Validation & Certification Requirements (Taken from Proposed Certification Standard IEC 62443-2-4).

Process Area	Certification Requirements
Vendor Control System Capabilities (cont'd)	1) Vendor shall provide security monitoring capabilities on its systems 2) The vendor shall support a management information base on its systems 3) The vendor system shall log all state changes 4) The vendor system shall report all security events through a standard utility interface 5) The vendor shall notify the utility of changes to subcontractors & consultants who have access to the deployed system 6) The vendor system shall acknowledge all operator set point changes 7) The vendor shall used wireless technologies that comply with approved international wireless communication standards 8) The use of proprietary / non standard wireless protocols shall not be used without permission of the utility 9) The vendor shall have periodic system risk assessments conducted on its systems 10) The vendor shall provide secure means to update firmware to its systems 11) The vendor shall implement wireless security tunnels over IPSec / SSL or WPA2 12) The vendor systems shall support FIPS 140-2 and ANSI X509 digital certificates 13) The vendor shall provide a central console for key management 14) The vendor shall automate key exchange processes between its systems