CryptoSoC

Cryptographic System On a Chip

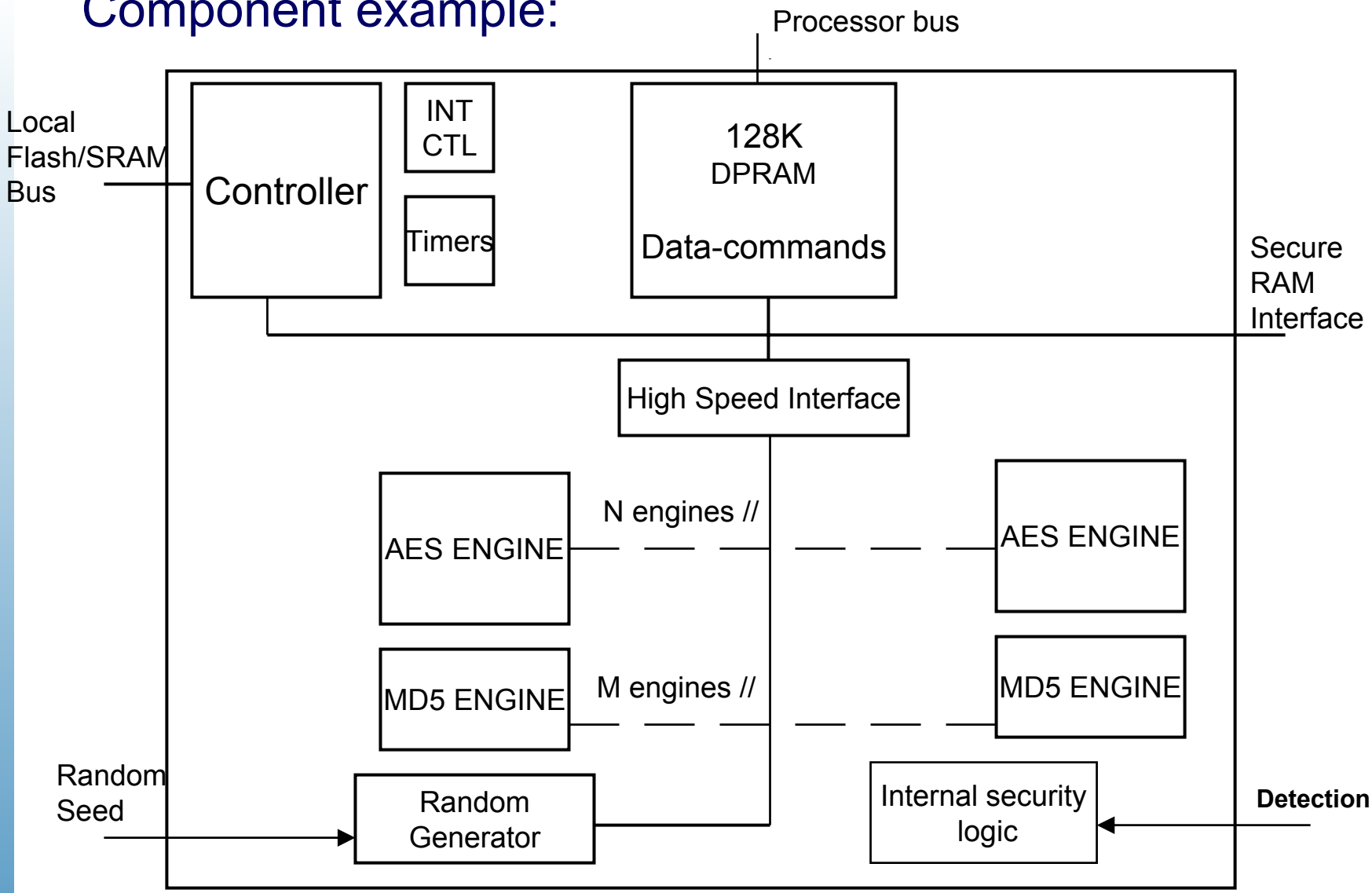
« European Components for a Trusted Protection of our Critical Infrastructures »

CryptoSoC

- **Goals : specification and development of a « cryptographic » SoC starting from re-usable IP blocks.**
  - Definition of all the IP blocks required (cryptograpy, secure memories, self-protection, keys, ...).
  - Compliances to standards and compatibility with the Internet applications (RFC 's, FIPS, …).
  - Possibility to derive differents cryptographic components suitable for different application (networking equipments, servers, mobile platforms, …).
  - Focus:
    - High performances
    - High security

CryptoSoC

Component example:



- **Partners**
  - Industries:
    - STMicroelectronics (I)
    - Bull (FR)
    - SAGEM (FR)
  - University and research partners R&D
    - Politecnico di Torino (I)
    - Politecnico di Milano (I)
    - CEA-LIST (F)
  - SME :
    - AMTEC (I)
    - I2E (FR)

- **Timeframe**
  - Start : 1Q2002
  - End : 4Q2004

- **Deliverables / Millestones**
  - WP1 : Functional specification: 3Q2002
  - WP2 : Architectural specification: 2Q2003
  - WP3 : IP blocks : 1Q2003 -> 1Q2004
  - WP4 : CryptoSoC FPGA prototypes: 1Q2004
    Demostrators : 4Q2004

Achievements H3-2002

- Analysis of the Internet applications requiring security infrastructure in terms of market size and security requirements (I.e. e-commerce, m-commerce, content distribution, outsourcing services).
- Analysis of the cryptographic specific requirements of the most used secure protocols (IPSEC, SSL/TLS, SMIME, …)
- Analysis of the existing components and platform and architectural solutions of the most popular secure devices suppliers.
- The results of this work is available in the form of reports.