Securing the connected world

cryptographic offloading and acceleration for data centers

SILEX Inside

Silex Inside

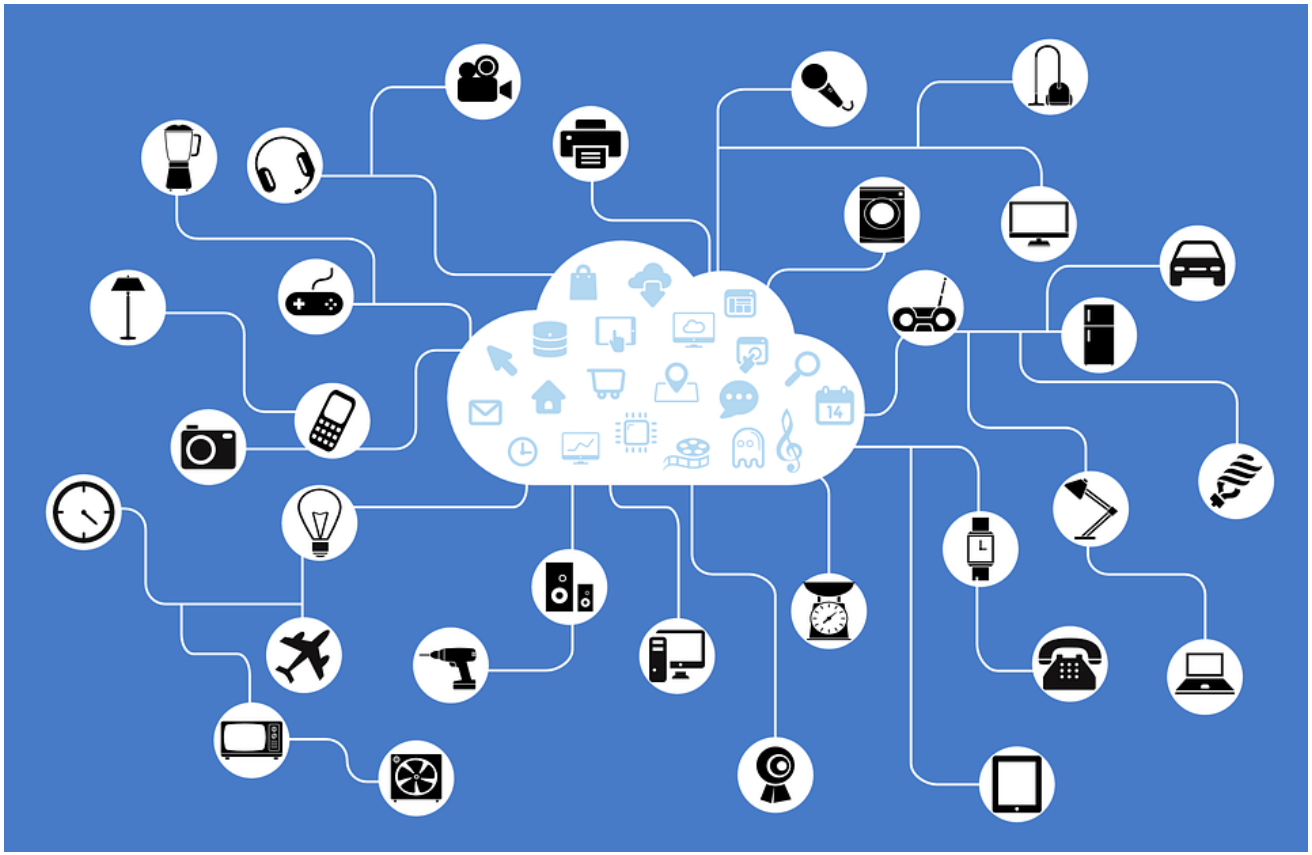
Barco Silex becomes

SILEX
Inside

SILEX
Inside

Connected world

- From end-point to data center



SILEX Inside

Connected world

- Data center challenges
  - High throughput secure data processing
  - High performance secure connection engine
  - Requires HW offloading
    - Reduce power consumption
    - Increase performance
    - Offload processor

SILEX Inside

A secure connected world

- Data transfer:
  - Source authentication
  - Data integrity
  - Confidentiality

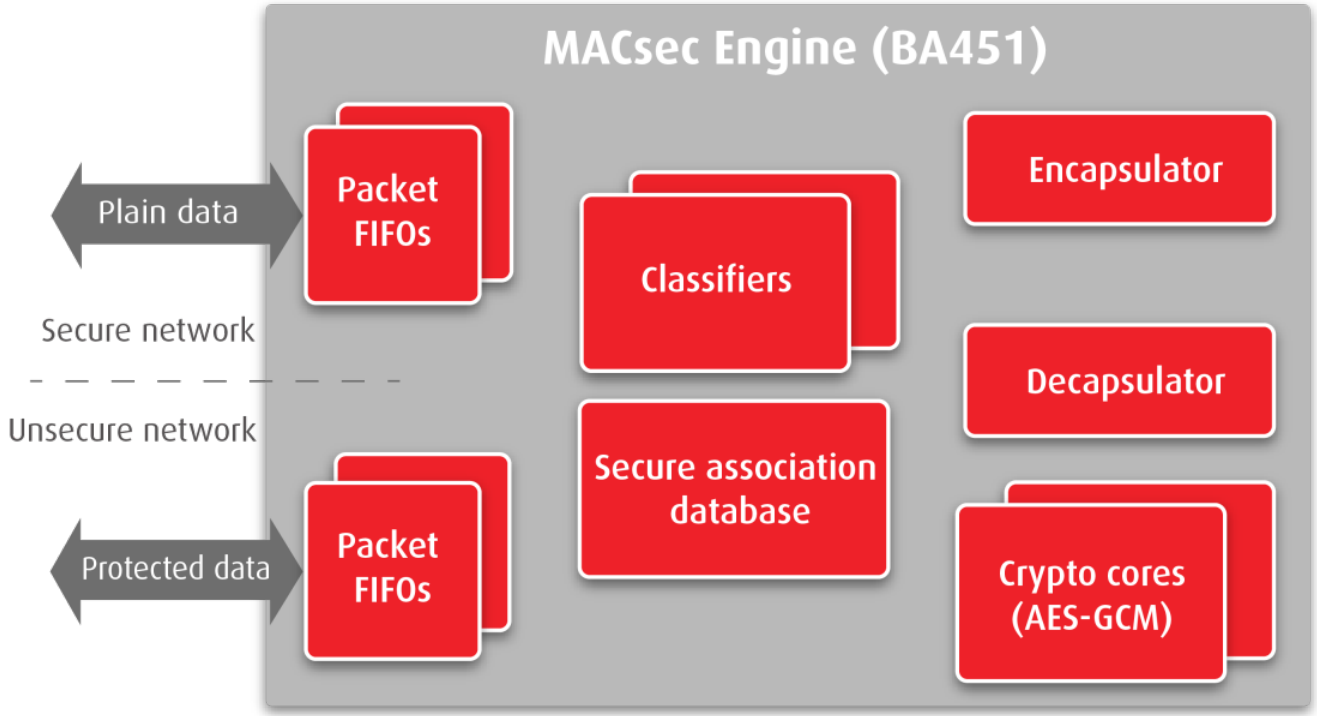
  → MACsec is the transport security protocol of choice
  - Software implementations not well suited
    - timing-critical
    - high-throughput applications
    - HW offloading required

CPU Offloading

- Secure data transfer
  - High throughout MACsec engine
  - BA451
    - IEEE 802.1AE, IEEE 802.1AEbn, IEEE 802.1Aebw compliancy
    - Support for all cipher suites (GCM-AES-128/256, GCM-AES-XPN-128/256).
    - Highly scalable: best trade-off between performance, area and latency
    - 128, 512 or 1024-bits data width
    - Throughput from 10 to 800 Gbps with low latency
    - SecTAG insertion/removal and ICV insertion/checking

CPU Offloading

- BA451



SILEX Inside

A secure connected world

- Secure connections
  - TLS/SSL connections
  - Requires compute intensive asymmetric cryptography
  - Software implementations not well suited
    - high number of connections/sec (PK operations)
    - HW offloading required

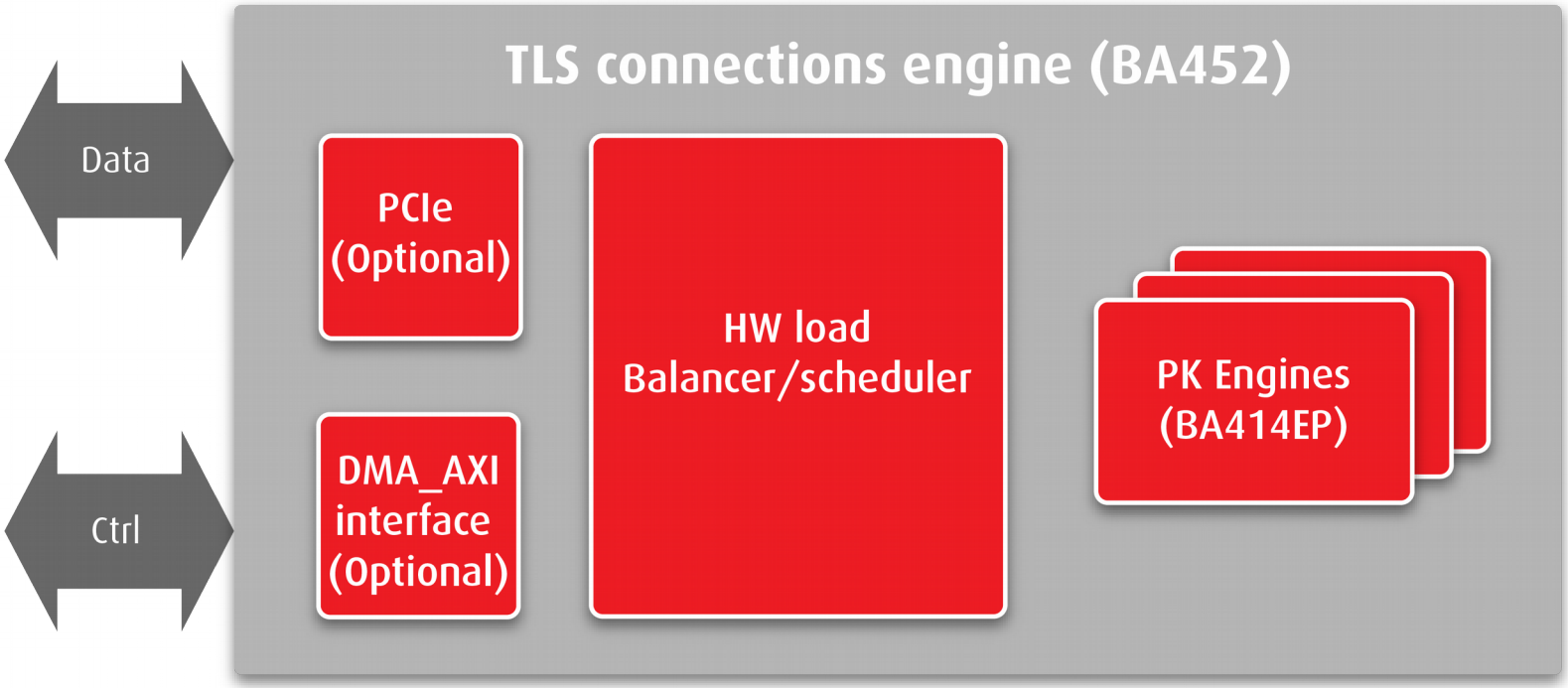
CPU Offloading

- Secure connections
  - TLS/SSLconnections
  - High performance Asymmetric PKE engine
  - BA452
    - Supports TLS 1.3: all cipher suites
      - RSA/DHE
      - ECDHE/ECDSA (all curves)
        - NIST/Brainpool curves
        - X.25519/X.448, Ed25519/Ed448
    - Can be implemented in FPGA and ASIC
    - several 10k's TLS/SSL connections per second
      - several hundred thousand ECC P-256 operation per second
    - Above 1Ghz on latest ASIC technology, and 600/700 MHz on latest FPGA
    - HW load balancer schedules optimal use of high performance PK engines

SILEX Inside

CPU Offloading

- BA452
  - HW load balancer schedules optimal use of high performance PK engines



SILEX Inside

Needs and benefits

- HW MACsec engine
  - Very high throughput (800Gbps with one engine)
  - Host CPU is free for other critical tasks
  - Improved security
- HW TLS/SSL connection engine
  - Several 10K operations/sec (sign and verify)
  - FPGA availability in data centers allows for cheap but very efficient implmentation
  - Host CPU is free for other critical tasks