Sun MicroSystems 22nd July 2003

- **32 Bit Smart card Controller**

Never stop thinking

32 Bit Smart card Controller

- - Target Applications.
- - Key Features
- - How this controller addresses future requirements.
- - Architecture of 32 bit controller.
- - Security Concept
- - Performance
- - Road map.
- - Over view of the 32 Bit controller.
- - Functional Blocks of the controller.
- - Platform Support Layer
- - Tools.(SDK and Emulator.)

Infineon technologies
Never stop thinking

SLE88 Family Overview
Target Applications

GSM (SIM Card)

Mobile Communication

UMTS (USIM Card)

m-commerce

Multi-Tasking

Credit Card

Home Banking

Banking

e purse

Security

Identification

PayTV /

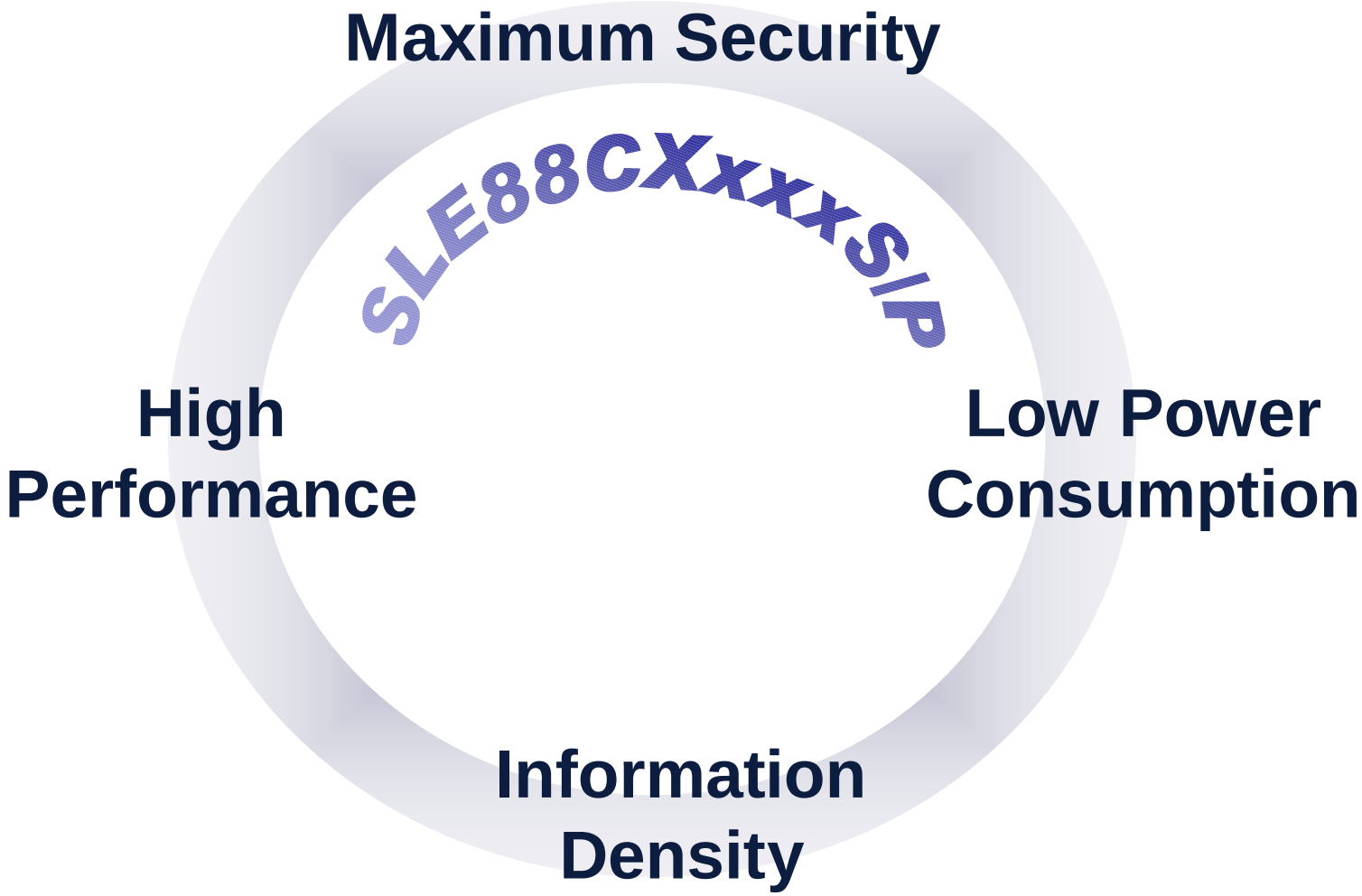
Network Access

Data Encryption

10111

Never stop thinking

Key Features



SLE88
Future requirements .... best addressed by 88 family

Unique proven future platform for real multi-application chip cards

Market requirements

- Increased memory requirements
- Performance headroom
- Fast execution of Java applets
- Secure execution of multi-applications
- Fast and secure Over The Air downloads
- Fast and secure m-commerce transactions
- Easy & flexible SW development
- Fast and incremental migration paths
- Fast time-to-market
- Cost efficiency
- Security, security, security, ...
- „ proven future platform“

Infineon‘s solution

- 32 Bit pipelined CPU with data/instruction caches, 55MHz
- Virtual Memory System with 4 GByte of linear address space
- Virtual Language acceleration (i.e. Java)
- Advanced Crypto Engine
- Platform Support Layer

- 1,8V low power technology
- 0,22 µm technology
- Integral Security Concept

Outstanding level of security and performance

Never stop thinking

SLE88
Today's Market Requirements

Multi-Applications

- 32-Bit Performance
- Large memory sizes
- Fast task switch capability
- Field update capabilities

Virtual Languages
e.g. JavaSC™

Security

- Fast Memory Access
- HW Byte Code Acceleration
- Open Platform Support

- Secure Execution of Multi-Applications
- Highest crypto performance
- Best in class DPA/SPA countermeasures
- To be always ahead of the Hackers

Never stop thinking

Infineon's Answer: The SLE88CX720P

Advanced 32-bit Architecture

- Up to 55 MHz internal frequency
- 4 GB of linear address space
- 240k ROM, 80k E^2, 8k RAM
- HW support for fast application switches

SLE88CX720P

VL Accelerator, PSL

- Data/Instruction Caches
- Dedicated VL Instructions
- Highest CPU performance
- Platform Support Layer (PSL)
  - providing all peripheral drivers
  - enabling fast SW development

Integral Security Concept

- MMU with secure package concept
- RSA signature 2048 bit within 0.17s
- EC DSA signature 160 bit within 20 ms
- Integral Security Concept
  - Sparkling Bus Encryption
  - Dual Rail Precharge Logic
  - Memory Encryption

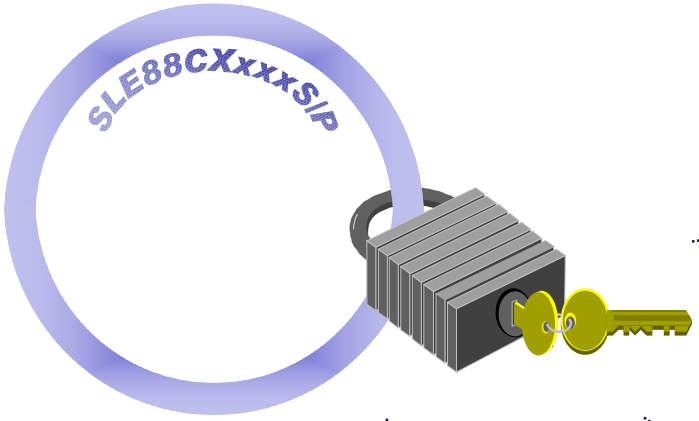
Never stop thinking

SLE88
Feature Overview

- Revolutionary Integral Security Concept
  - Strongest DPA/SPA HW Countermeasures
  - Complete Memory Encryption
  - Sparkling Bus Encryption
- High Performance 32-bit Architecture
  - “Real” Multi-Tasking
  - Four Gigabytes of Virtual Memory per Task
  - High-Performance Advanced Crypto Engine
- Virtual Machine Language Acceleration for
  - Java™
  - MultOS™
  - Windows Powered Smart Cards™
- Flexibility

Never stop thinking

88 Overview Training - Security Concept



MMU

code+ data access protection

hardware attack protection

Sensors

authenticity in applications

chip and data analysis

chip and data manipulation protection

Memory Encryption

Encryption on all ROM RAM, NVM

with mask-, session and chip individual keys

Security Peripherals

Anti Screening Mechanism

Never stop thinking

Security features

- Data Encryption According to DES
- Low and High Voltage/frequency sensors
- Intrernal/external Glitch sensor
- Light sensor
- Active shielding
- Unique Chip ID or each chip
- High security self test software concept.
- Fast , complete erasure of RAM triggered by sensors.
- Scrambling of data bus contents between security devices and core.
- Sparkling encryption and memory encryption.

Infineon technologies
Never stop thinking

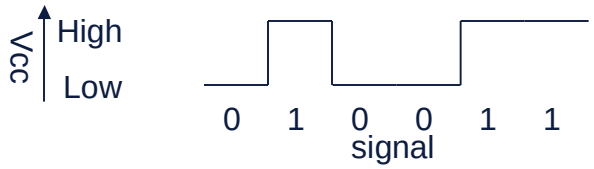
SLE88
Revolutionary Integral Security Concept

- Dual-Rail bus architecture
  - ⇒ Data-independent power profile to prevent known SPA and DPA attacks
- Sparkling Bus Encryption
  - ⇒ Data encryption with continuously changing transport keys
- Automatic Memory Encryption
  - ⇒ Encryption on all ROM, RAM and non-volatile memory areas with mask-, session and chip individual keys
- Memory Management Unit with HW Firewalls
  - ⇒ Provides real and secure multitasking with different levels of access rights
- Active Metal Shield
  - ⇒ Implemented to avoid direct physical attacks

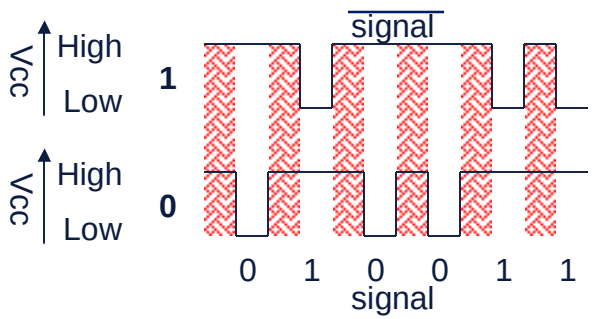
Infineon technologies
Never stop thinking

SLE 88
Dual Rail Precharge Logic

Signal on single rail:



Dual Rail Precharge Logic:



Both data lines are precharged before every bit transmission

Data dependent current profile

- ➔ Strong SPA/DPA countermeasures necessary
- ➔ Increased current consumption due to additional countermeasures in conventional logic

Data independent current profile

- ➔ Target is that no additional SPA/DPA countermeasures are necessary
- ➔ No short circuit currents in precharge logic
- ➔ In total low power consumption

=> Eliminating data dependent power consumption by hardware is the best way to prevent from SPA/DPA

Never stop thinking

SLE88CX720P
The Performance Edge

- Up to 55 MHz internal frequency
- Fast memory access
  - Fast access times
  - Prefetching of Instructions
  - Instruction Cache 1kB, Data Cache 2kB
- Multi-Tasking
  - “Parallel” and independent execution of multiple tasks
  - Fast context switch through optimized call & return processes
  - Parallel use of different peripherals (e.g. UART, ACE, RNG etc.)
- Low power consumption for the complete chip
  - 0,5 mA/MHz 88P
  - Automatic power limitation mode for GSM/UMTS

Infineon technologies
Never stop thinking

SLE88
Virtual Language Support

- Intelligent acceleration of virtual languages
  - Dedicated instructions for acceleration of stack oriented languages like Java™ and MultOS™ and also Windows Powered Smart Cards™
- Flexibility for future enhancements of virtual language specification without HW modifications
- Possibility of secure Over The Air upgrades for applets and even VMs
- SW simulator support for performance estimations

Never stop thinking

SLE88
Flexibility

- Migration path between high-end 88P and cost optimized 88S

- Flexible feature set, e.g.
  - 2048 bit Crypto2000-engine
  - CL-Interface
  - USB...

- Hardware customization by chip-integrated FPGA or Standard Cell building blocks on request

Never stop thinking

SLE88
Virtual Memory System

- Virtual Memory System (VMS) offers 32-Bit linear address space
  - Virtual to physical memory mapping is automatically handled by sophisticated Memory Management Unit (MMU)
  - VMS offers most convenient programming model
    - automatic memory allocation
    - automatic “de-fragmentation”
    - substitution and re-programming mechanism for memory bit errors

Never stop thinking

Coming Next
88 Family of 32-bit Chip Card Controllers: 88P and 88S

88 Family of 32-bit Smart Card Controller
- ***Proven future platform***
- ***Leading edge performance***
- ***Revolutionary Integral Security Concept***
- Built-in Java accelerator
- Compliant to ETSI standard for SIM/USIM

88Plus
- 32-bit solution tailored to meet requirements of future applications
- Largest memories
- Highest performance
- Best in class clock rates up to 55MHz

88S
- Cost optimized 32-bit solution
- GSM dedicated memory configuration
- Optimized performance/cost ratio
- Reduced clock rates up to 33MHz
- Easy and fast migration within 88 family

Infineon technologies
Never stop thinking

Main Differences
88 Family of 32-bit Chip Card Controllers: 88P and 88S

The 88P

- Integral security concept
  - target CC EAL5+
- Highest performance at 55 MHz
  - 2k data and 1k instruction caches
  - RSA signature 2048 bit with CRT 0,17s
- Java acceleration
- Largest memories in the market
  - 80k E^2 /240k ROM/8k RAM
- 3 - 5 V
- Low power consumption (500µA/MHz)

The 88S

- Integral security concept
  - target CC EAL5+
- High performance at 33 MHz
  - 1k data and 0.5k instruction caches
  - RSA signature 2048 bit with CRT 0,27s
- Java acceleration
- GSM optimized memory configuration
  - 72k E^2 /192k ROM/6k RAM
- 1.8 - 5 V
- Lowest power consumption (350µA/MHz)

Infineon technologies
Never stop thinking

SLE88CX4000
Feature Highlights (1)

- C11FL: 0.13 µm
- Higher Internal Frequency: 66MHz
- Larger memories:
  - 80kByte “hidden” ROM for PSL
  - 400kByte EEPROM (“Flash”)
  - 16kByte RAM
- “Flash”:
  - Reduced programming time: 2ms
  - Increased page size: 128 bytes
  - Configurable in code/data memory spaces with 4Kbytes granularity

Never stop thinking

SLE88CX4000P
Feature Highlights (2)

- Reduced Power Consumption: 350 µA/MHz
- Supply voltage range: 1.62 V to 5.5 V
- Crypto@1408Bit:
  - Larger register length: 1408 bits
  - SPA/DPA HW countermeasures
  - At least four times faster than ACE:
    - RSA1024 signature with CRT within 36 ms
    - RSA2048 signature within 4 ms
  - Support of ECC GF(p) and GF(2m)

Never stop thinking

SLE88
“Flash” Technology

- C11FL: 0.13µm
- Configurable in code/data memory spaces with 4Kbytes granularity
- Page size: 128 Bytes
- Byte wise addressable
- Erase cycle time 1ms
- Write cycle time 1 ms
- 500,000 write/erase cycles
- Data retention: min. 10 years @ 25°C

Never stop thinking

SLE88
“Flash” Personalization

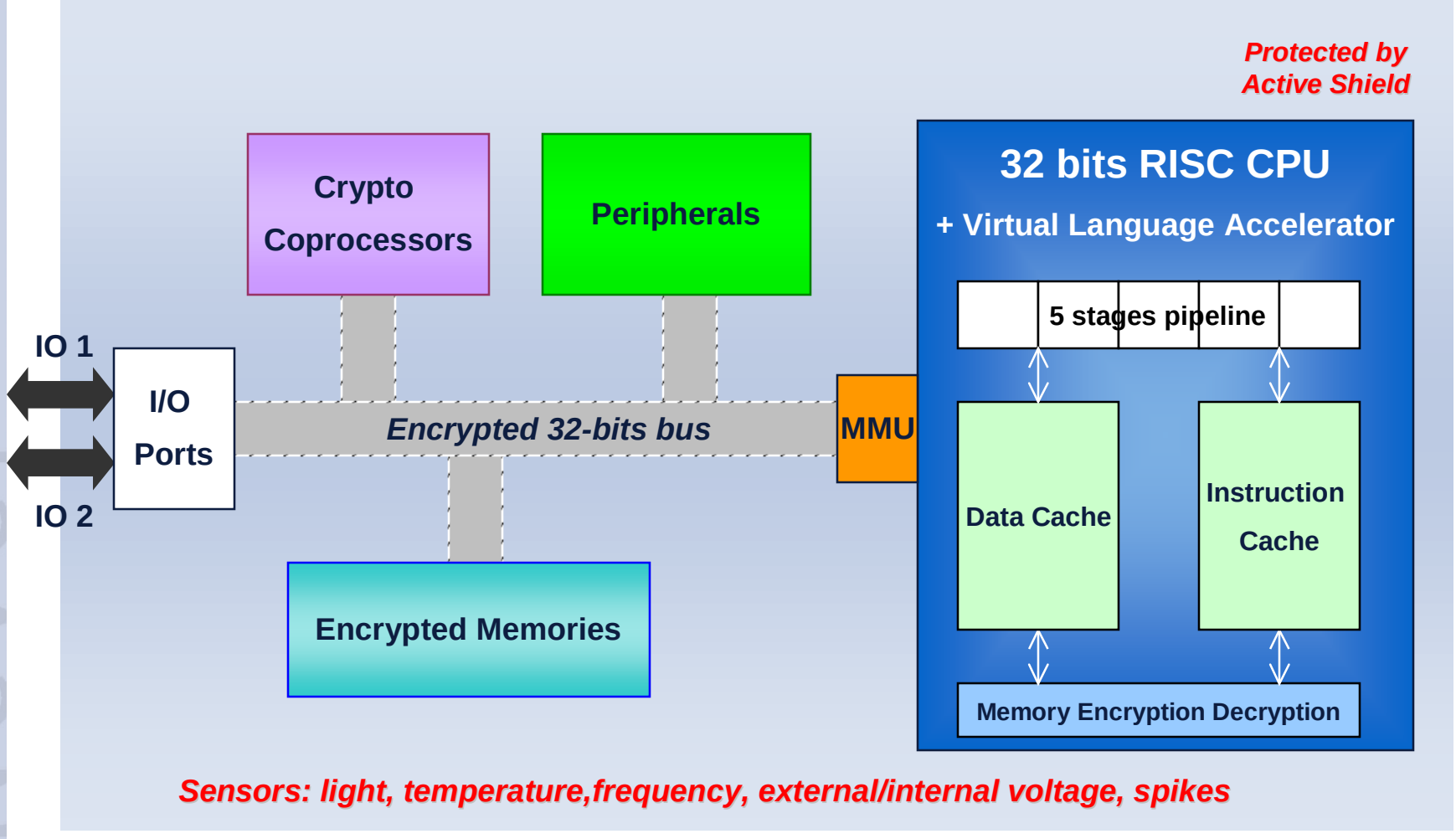
- 240kBytes NVM
- 10 MHz External Frequency
- Division Factor 16
- 32-fold programming

- 25 s total programming time
- 0.78 s / chip
- 0.42 ms / page / chip

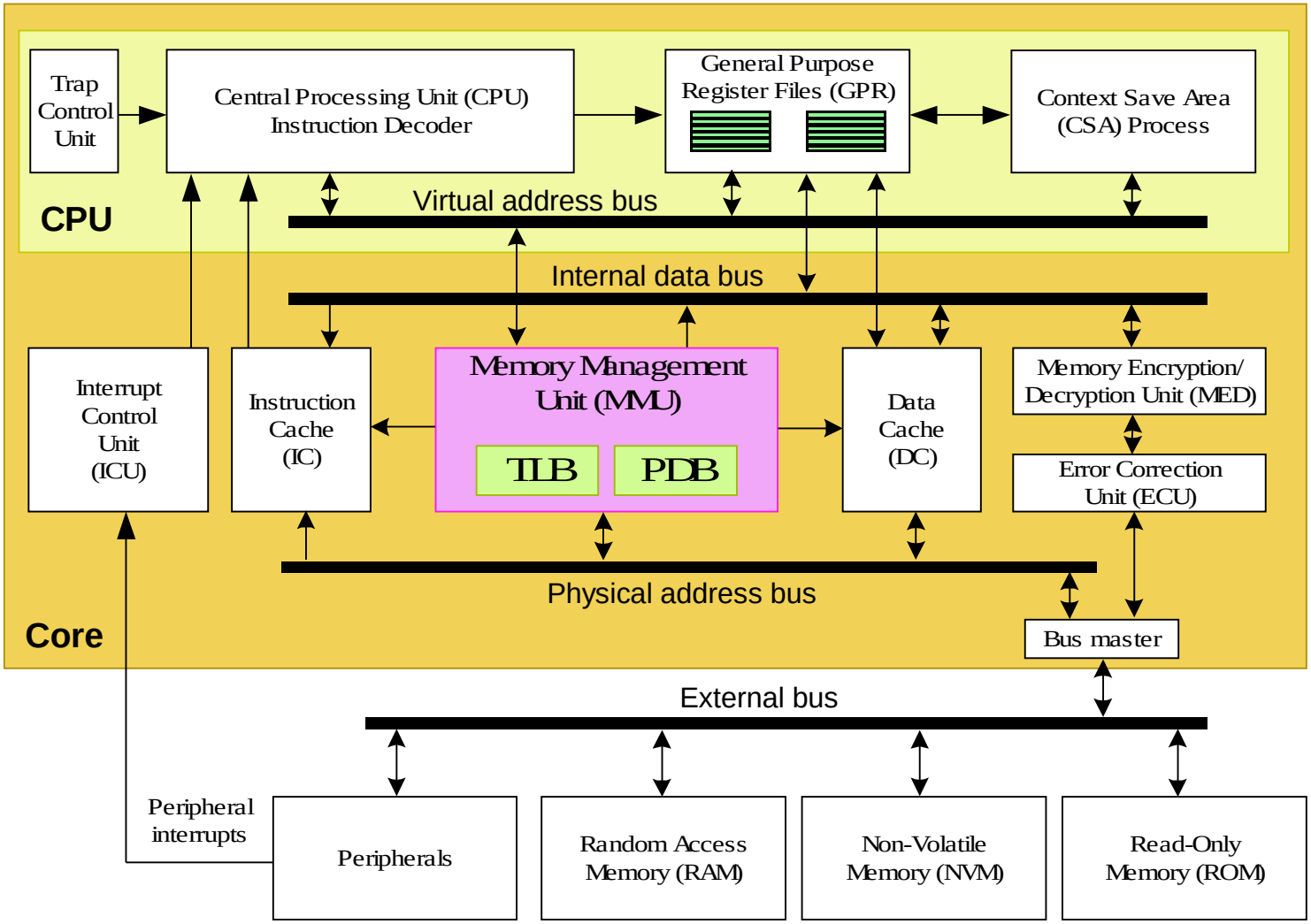
Never stop thinking

88 Overview - Architecture

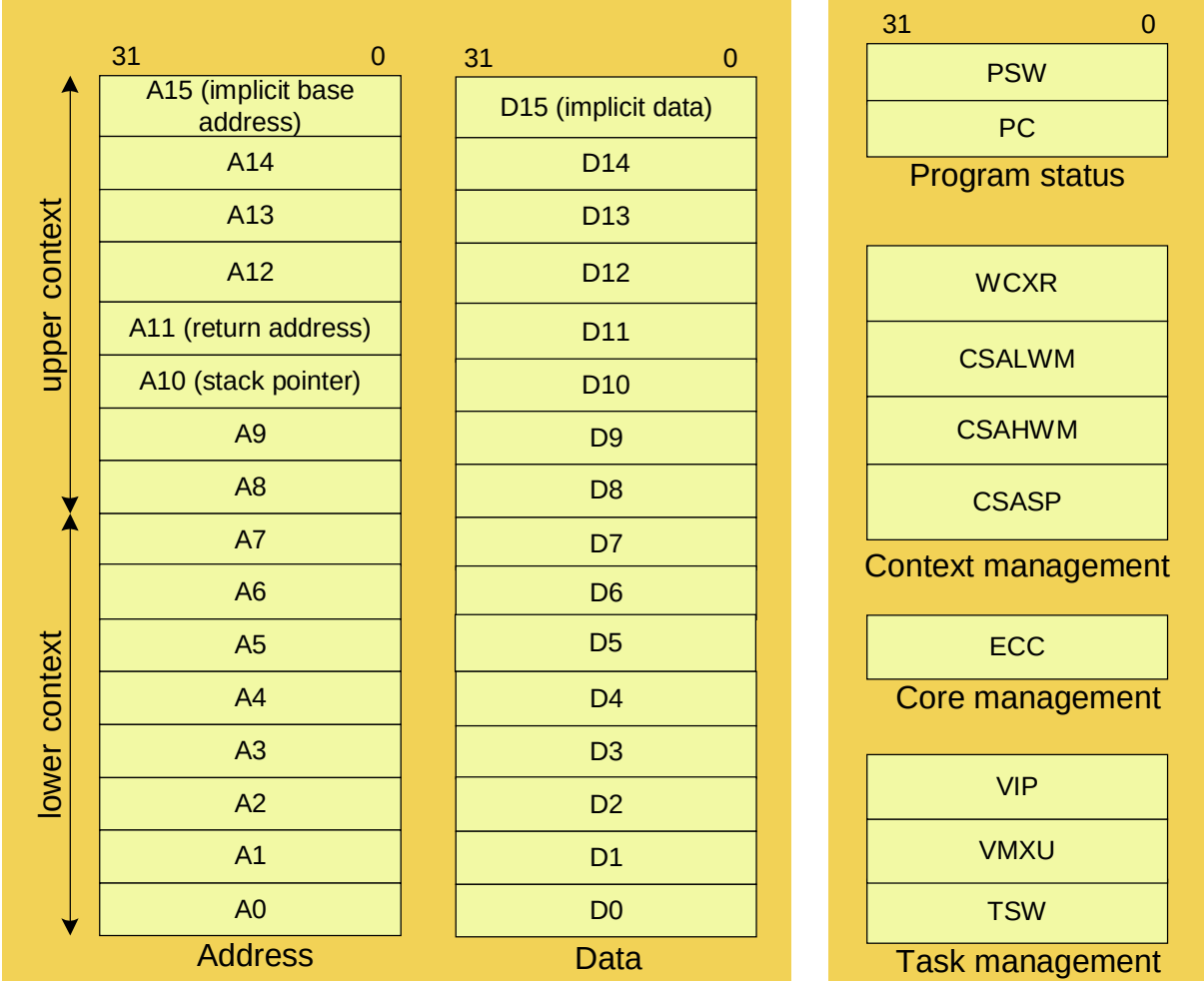
Overview



SLE88
Architecture



SLE88
General Purpose Registers

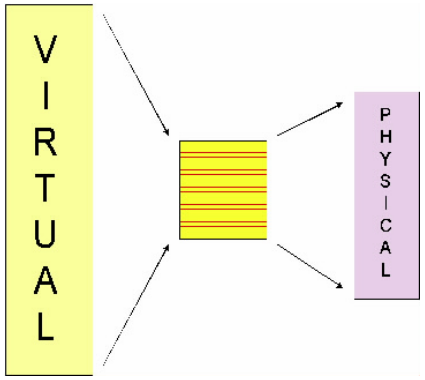


Memory Management Unit

large address range (32 bits)

one can address: 2^32 items = 4 GB

That is the virtual Memory !



Physically <<<<< 4 GB

(4GB = hard disk of a PC)

MMU contains mechanism to protect applications against each other

=> Secure download of application/patches in the field

=> Firewalls protect application against each other (GSM, Banking)

Access to Core Special Function Registers

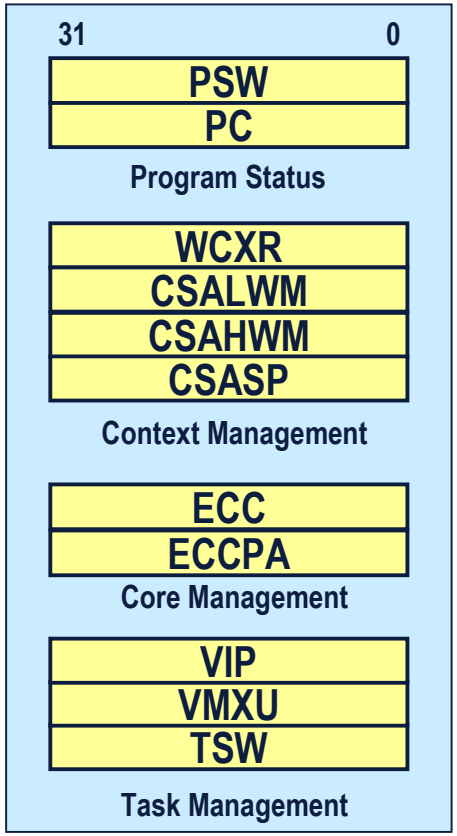
FROM

```
mfcr.w  d3, psw
mfcr.a  a3, csasp
```

TO

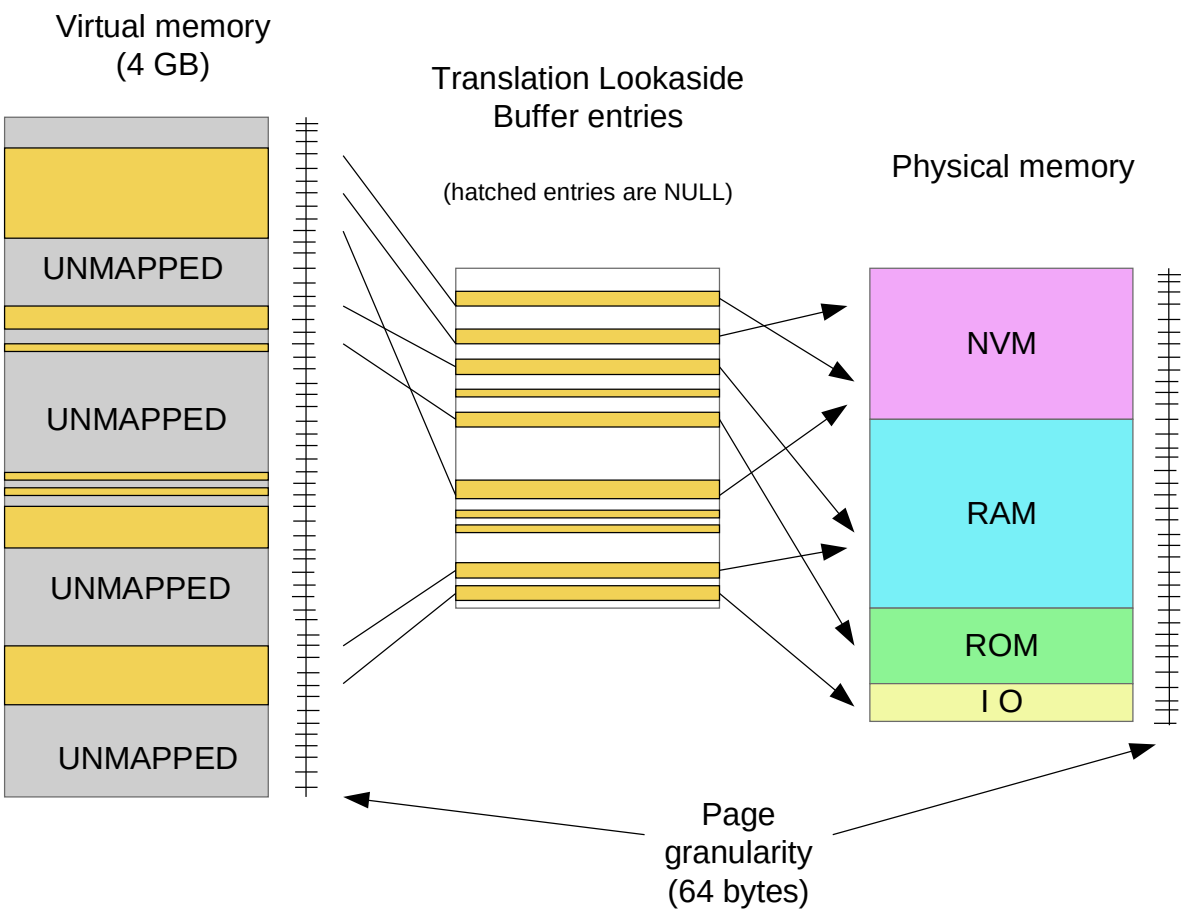
```
mtcr.w  psw, d3
mtcr.a  csasp, a3
```

System Register

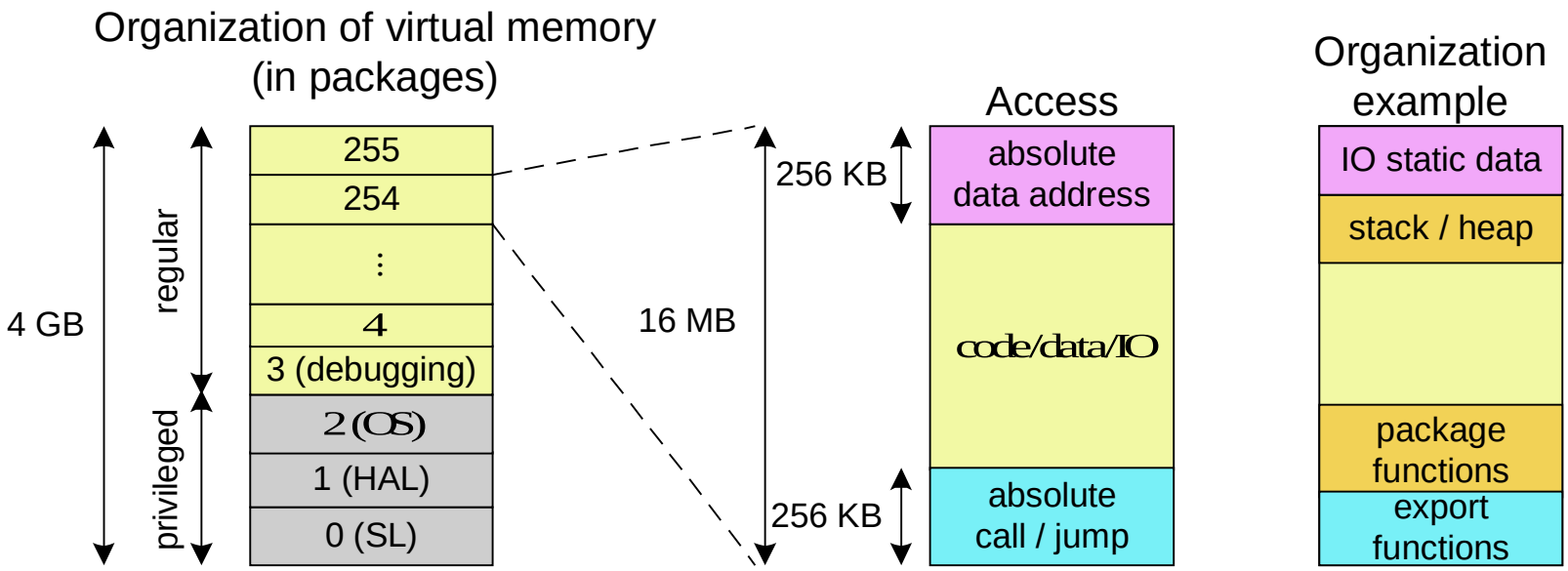


Never stop thinking

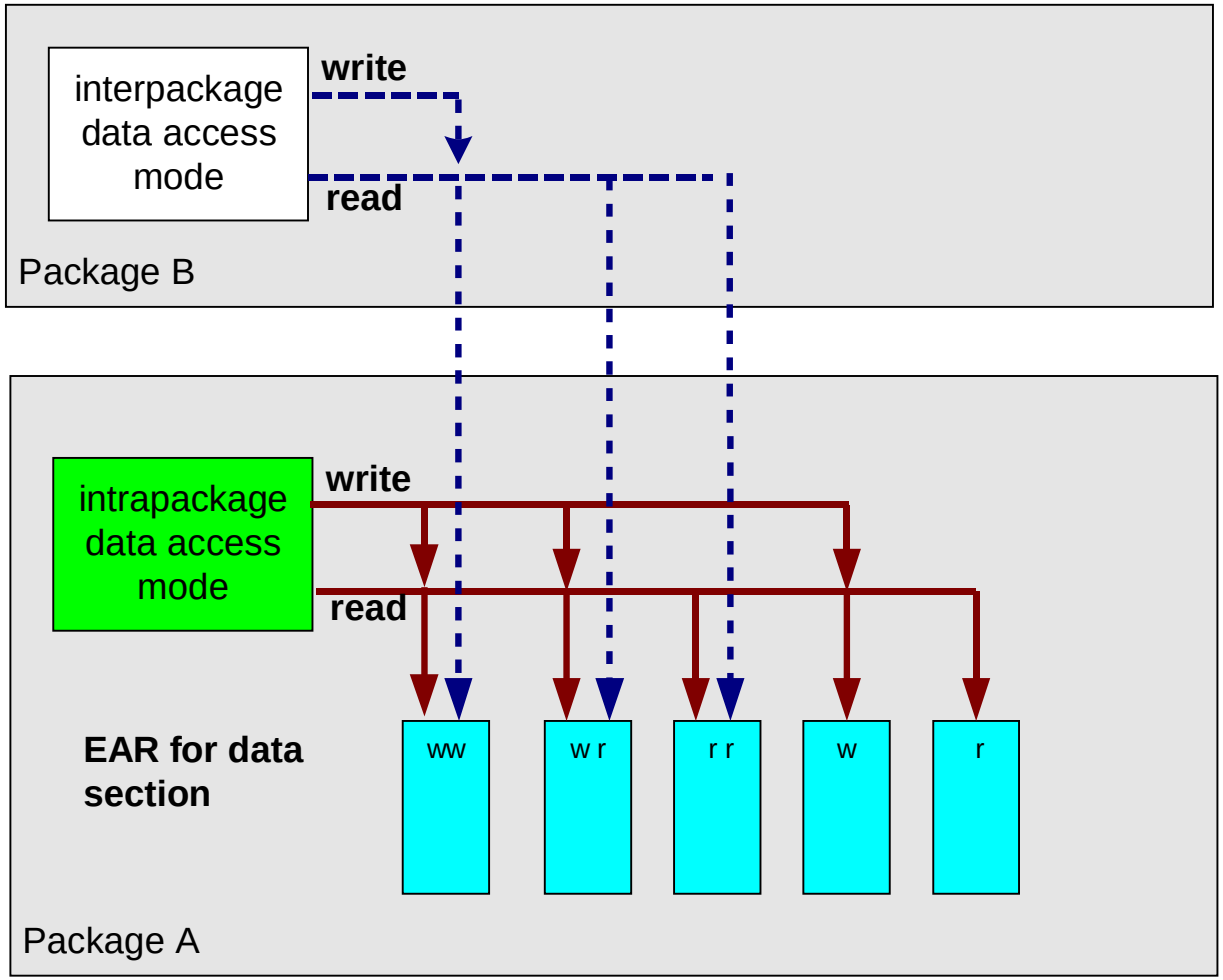
SLE88
Page Translation in VMS



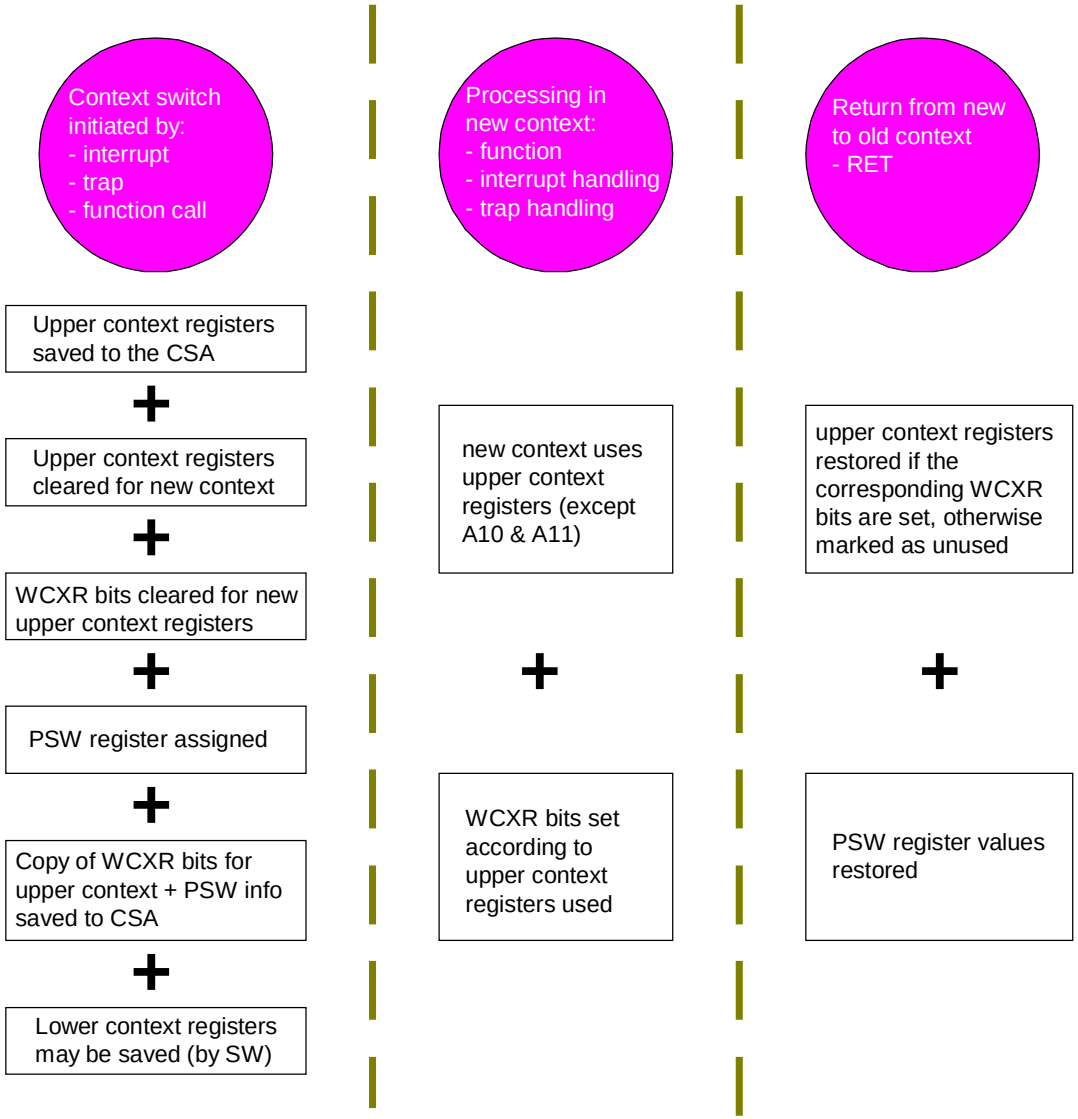
SLE88
Memory Model



SLE88
Data Access Types

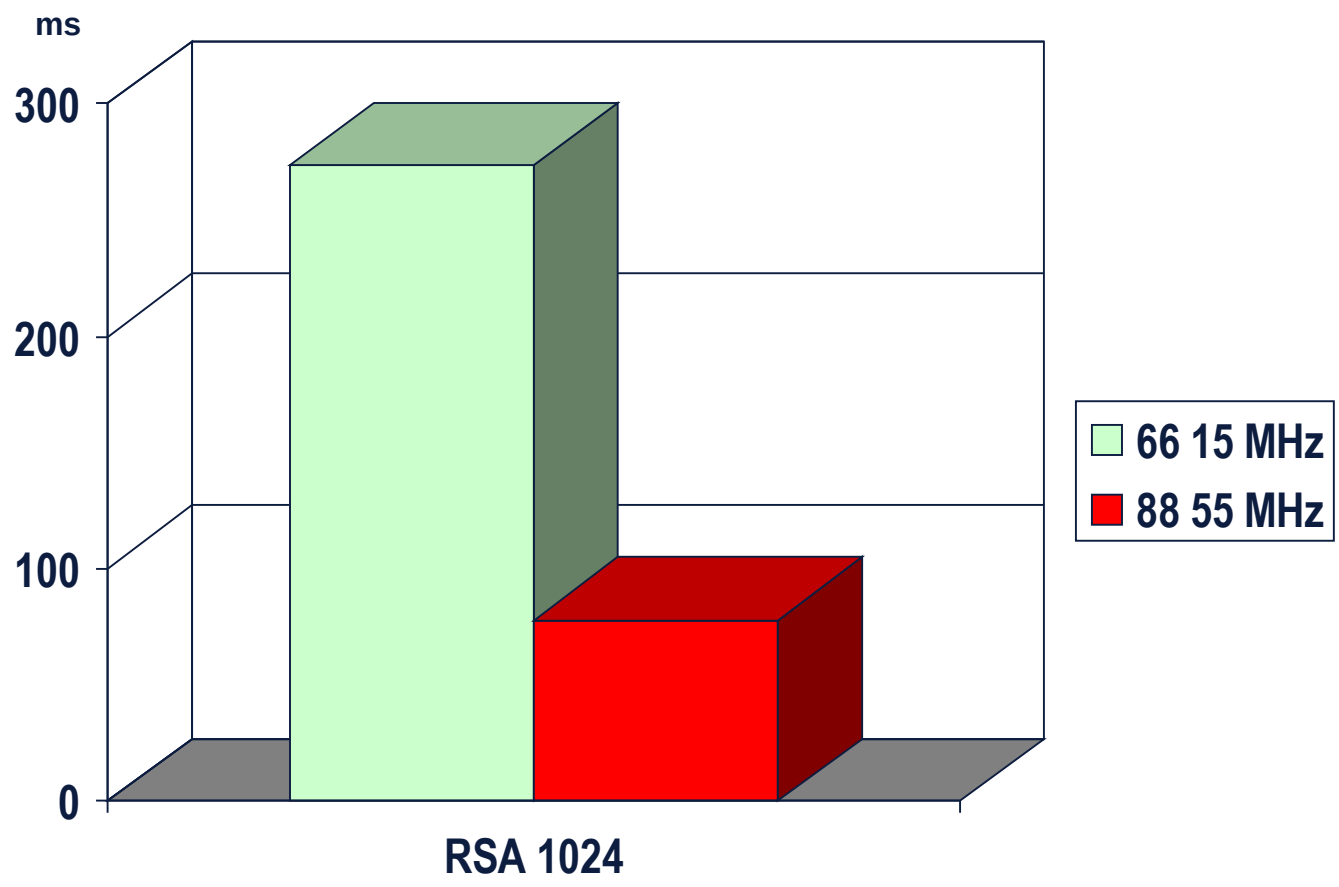


SLE88
Principle of Context Switch



Coprocessors for Cryptography

ACE



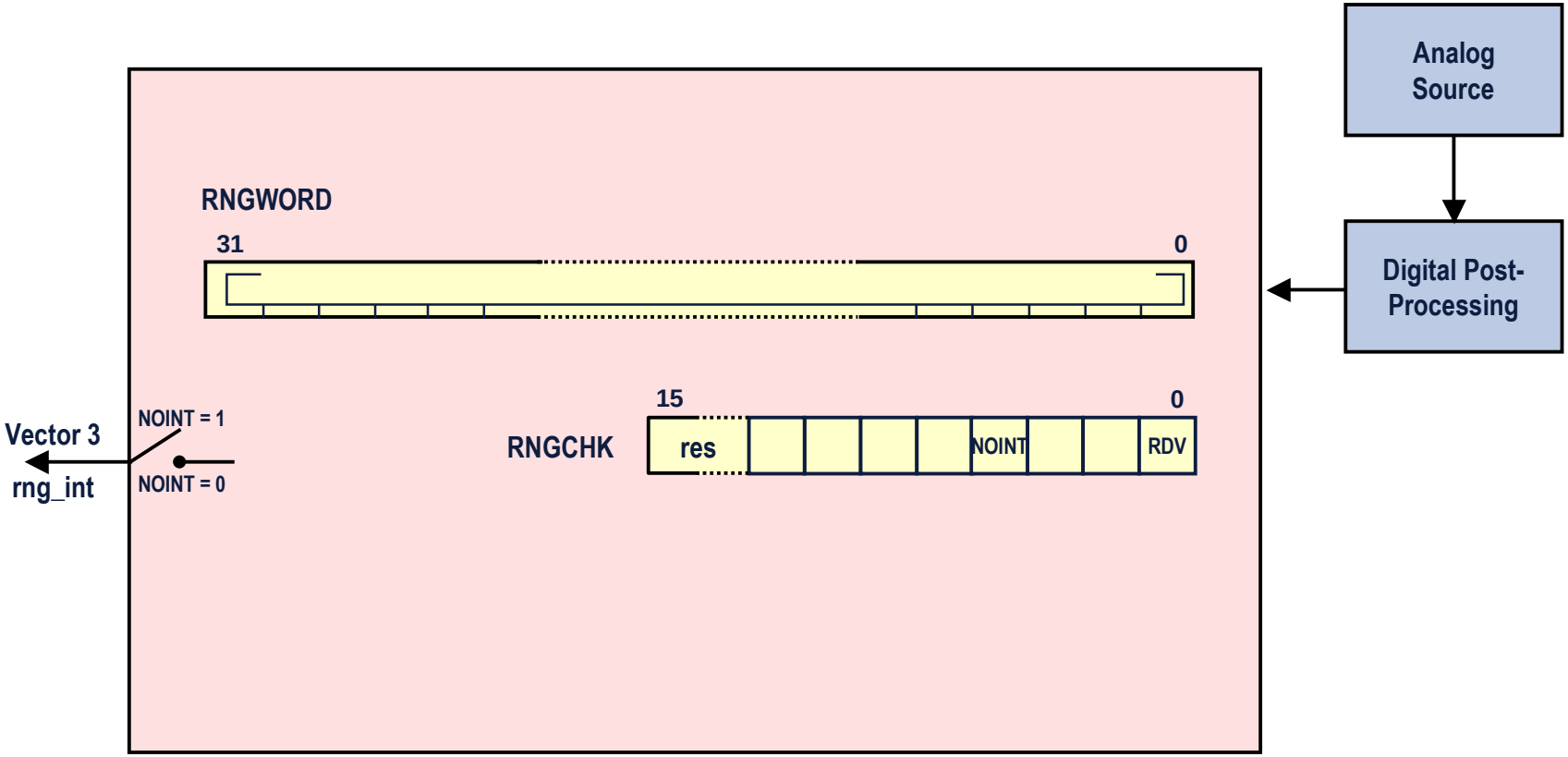
Never stop thinking

Crypto Performance Comparison

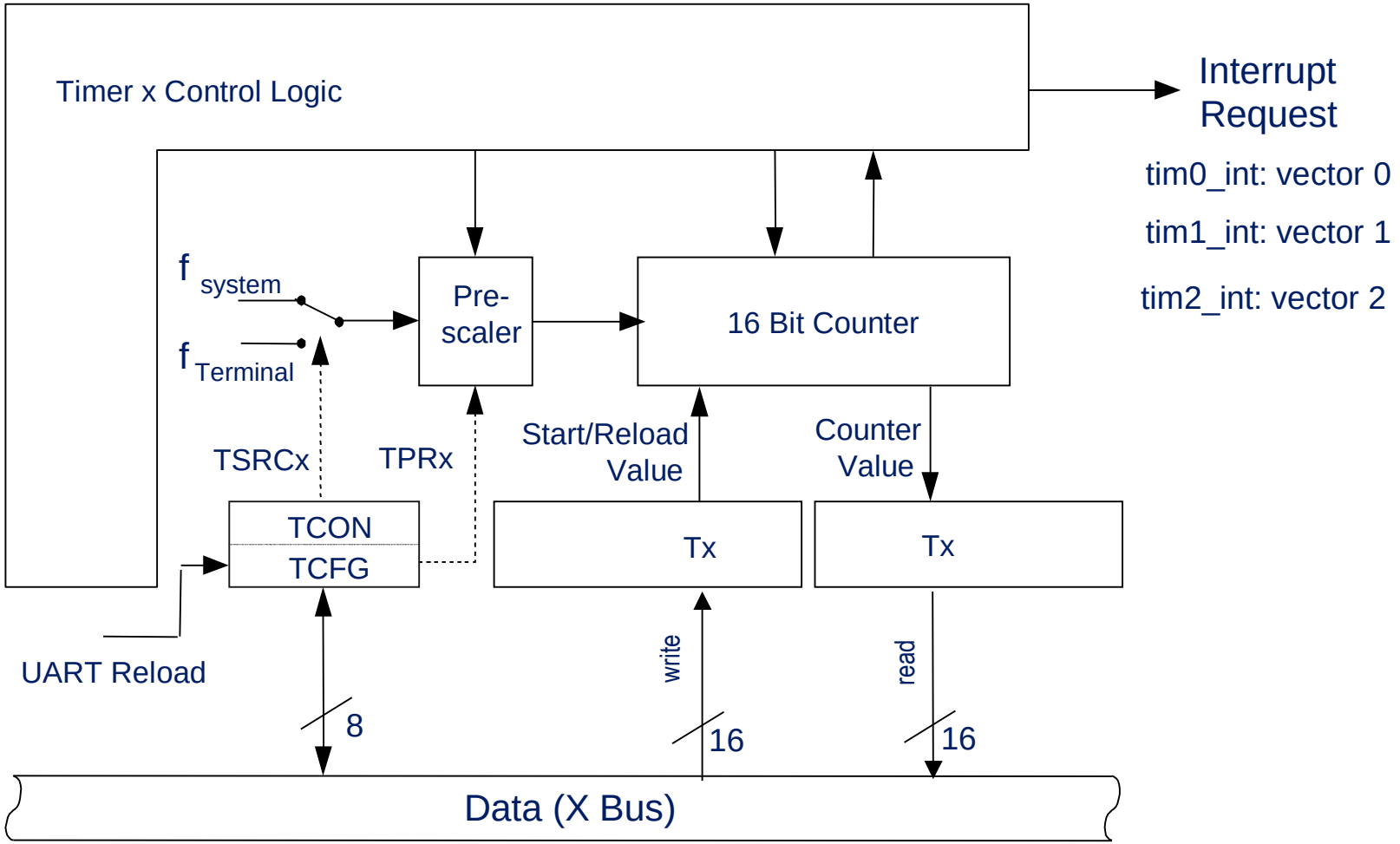
Operation	Modulus	Exponent	ACE Perf. at 5MHz [ms]	ACE Perf. at 55MHz [ms]	Crypto@1408Bit Perf. at 5MHz [ms]	Crypto@1408Bit Perf. at 66MHz [ms]
RSA signature (without CRT)	512 bit	512 bit	110	10,2	53	4
RSA signature (without CRT)	1024 bit	1024 bit	860	78	238	18
RSA signature (without CRT)	2048 bit	2048 bit	113.000	10.000	25.000	1.900
RSA signature (with CRT)	1024 bit	1024 bit	230	25,2	53	4
RSA signature (with CRT)	2048 bit	2048 bit	1.800	170	475	36
RSA verification	1024 bit	32 bit	30	2,8	7	0,5
RSA verification	2048 bit	F_4	628	57	146	11
RSA Key Generation (n=5)	1024 bit		22.440	2.040	4.356	330
RSA Key Generation (n=5)	2048 bit		137.280	12.480	35.640	2.700
EC DSA over GF(p) signature	160 bit	160 bit	260	24	99	7,5
EC DSA over GF(p) verification	160 bit	160 bit	550	50,4	198	15
EC DSA over GF(2^n) signature	160 bit	160 bit	---	---	158	12
EC DSA over GF(2^n) verification	160 bit	160 bit	---	---	317	24
			available on 66P and 88	available on 88	in development	in development

Infineon technologies
Never stop thinking

Random Number Generator, RNG



Timer 0,1,2

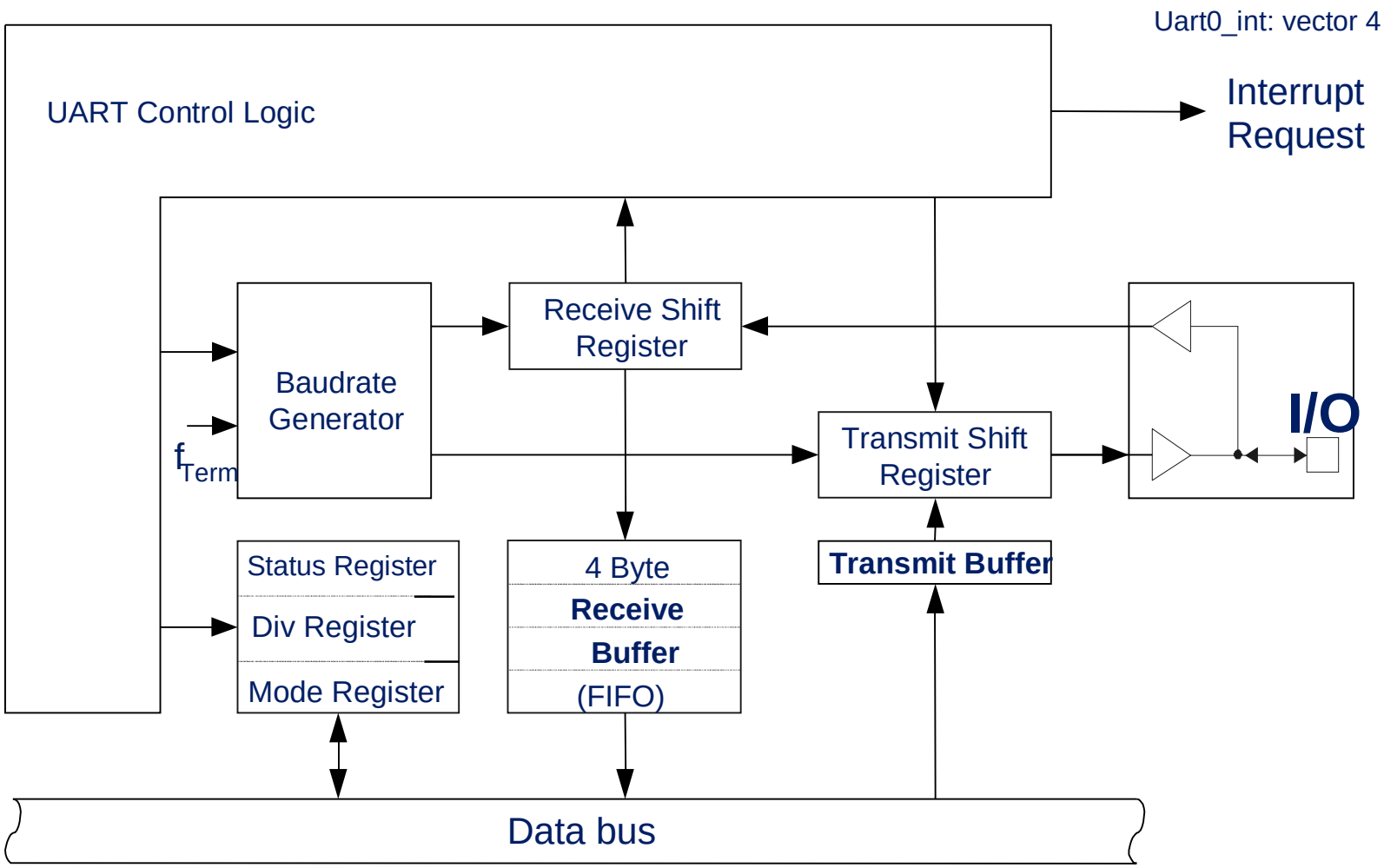

Timer x Control Logic
Interrupt Request
tim0_int: vector 0
tim1_int: vector 1
tim2_int: vector 2
f system
f Terminal
Pre-scaler
16 Bit Counter
TSRCx
TPRx
Start/Reload Value
Counter Value
TCON
TCFG
Tx
Tx
UART Reload
write
read
8
16
16
Data (X Bus)

Timer SFR and Interrupt Mapping

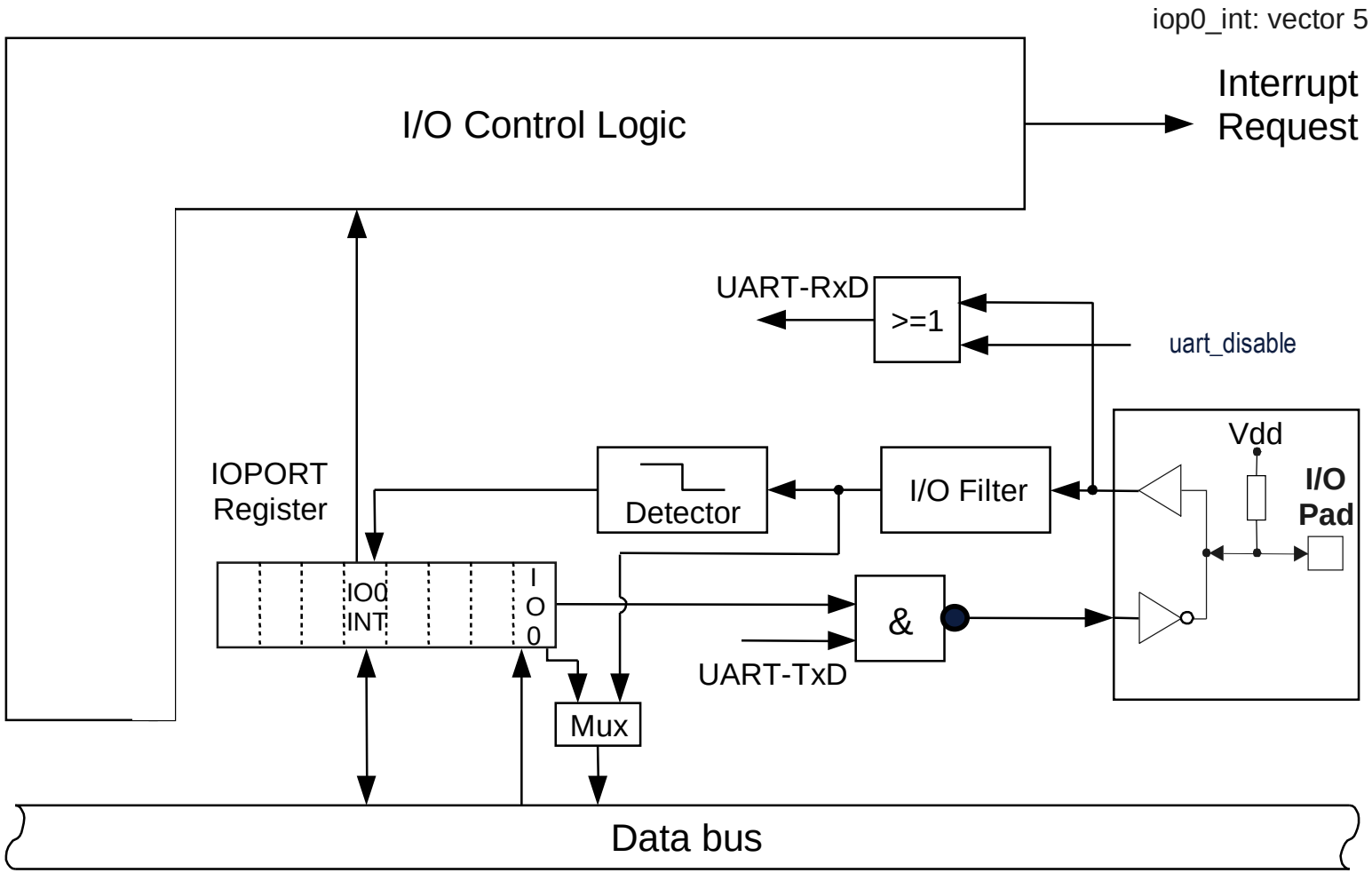
Page Address	Seg.	Module	BondOut	SFR	Size / bit	Physical Address	BPF Value (SL)	Reset Value
0x000100h - 0x00013Fh	IO	Timer0		TCON0	8	0x000100	000b	0x00h
				TCFG0	8	0x000110	000b	0x00h
				T0	16	0x000120	000b	0x0000h
0x000140h - 0x00017Fh	IO	Timer1		TCON1	8	0x000140	000b	0x00h
				TCFG1	8	0x000150	000b	0x00h
				T1	16	0x000160	000b	0x0000h
0x000180h - 0x0001BFh	IO	Timer2		TCON2	8	0x000180	000b	0x00h
				TCFG2	8	0x000190	000b	0x00h
				T2	16	0x0001A0	000b	0x0000h

Infineon technologies
Never stop thinking

UART Block Diagram



Block Diagram I/O Ports



ICO Functional Overview

- The ICO module covers the clock supply for the SLE88 Family
  - It generates **system clock** for the CPU and
  - **Synchronized external clock** for the peripherals
  - The system clock is derived from a terminal or from the internal oscillator, depending on the programmed operating mode
  - For the external clock a **spike filter** and a **frequency sensor** can be configured
- The ICO supports a dual interface mode to combine contact based and contactless operations

Never stop thinking

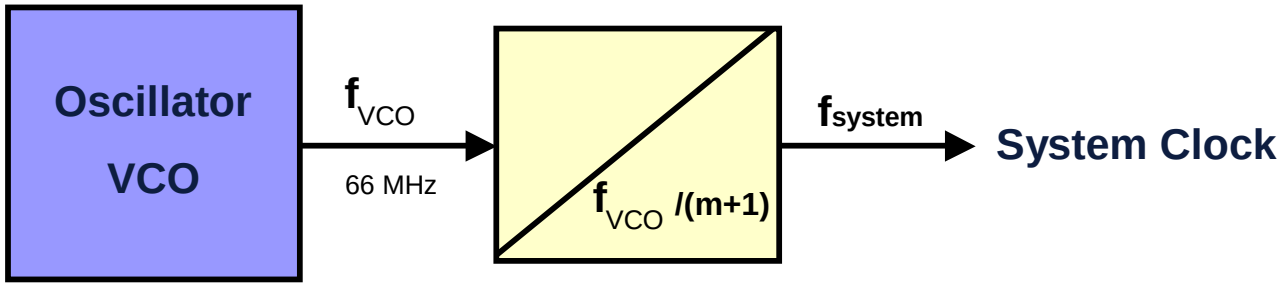
Operation Modes Overview

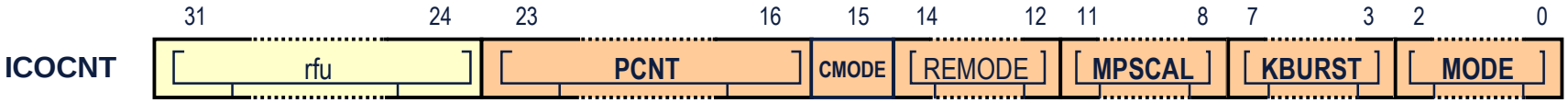
V-enable on	V-enable off
High Performance Mode	**High Performance Mode**
system clock = f_{VCO}/m timer clock = external clock	system clock = f_{VCO}/m timer clock = external clock
Fast Mode	**Fast Mode**
system clock = k * external clock timer clock = external clock	system clock = k * external clock timer clock = external clock
Power Saving Mode	**Power Saving Mode**
system clock = external clock timer clock = external clock	system clock = external clock timer clock = external clock
Sleep Mode	
system clock = 0 timer clock = external clock	

Infineon technologies
Never stop thinking

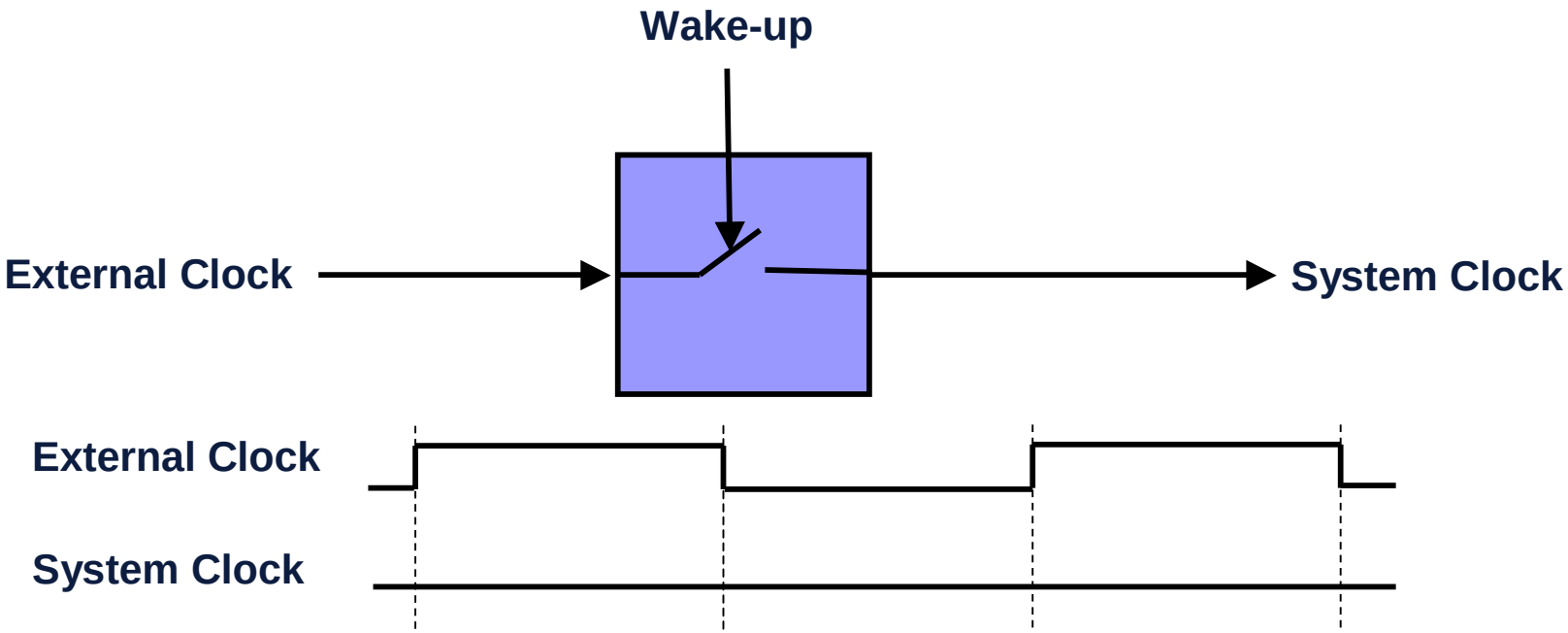
High Performance Mode

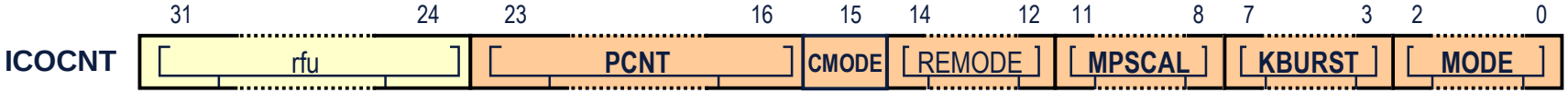
MPSCAL ICOCNT[11:8]	*m*	f_{system}
0000	0	f /1
0001	1	f_{VCO} /2
.....	.....	.....
1110	14	f_{VCO} /15
1111	15	f_{VCO} /16



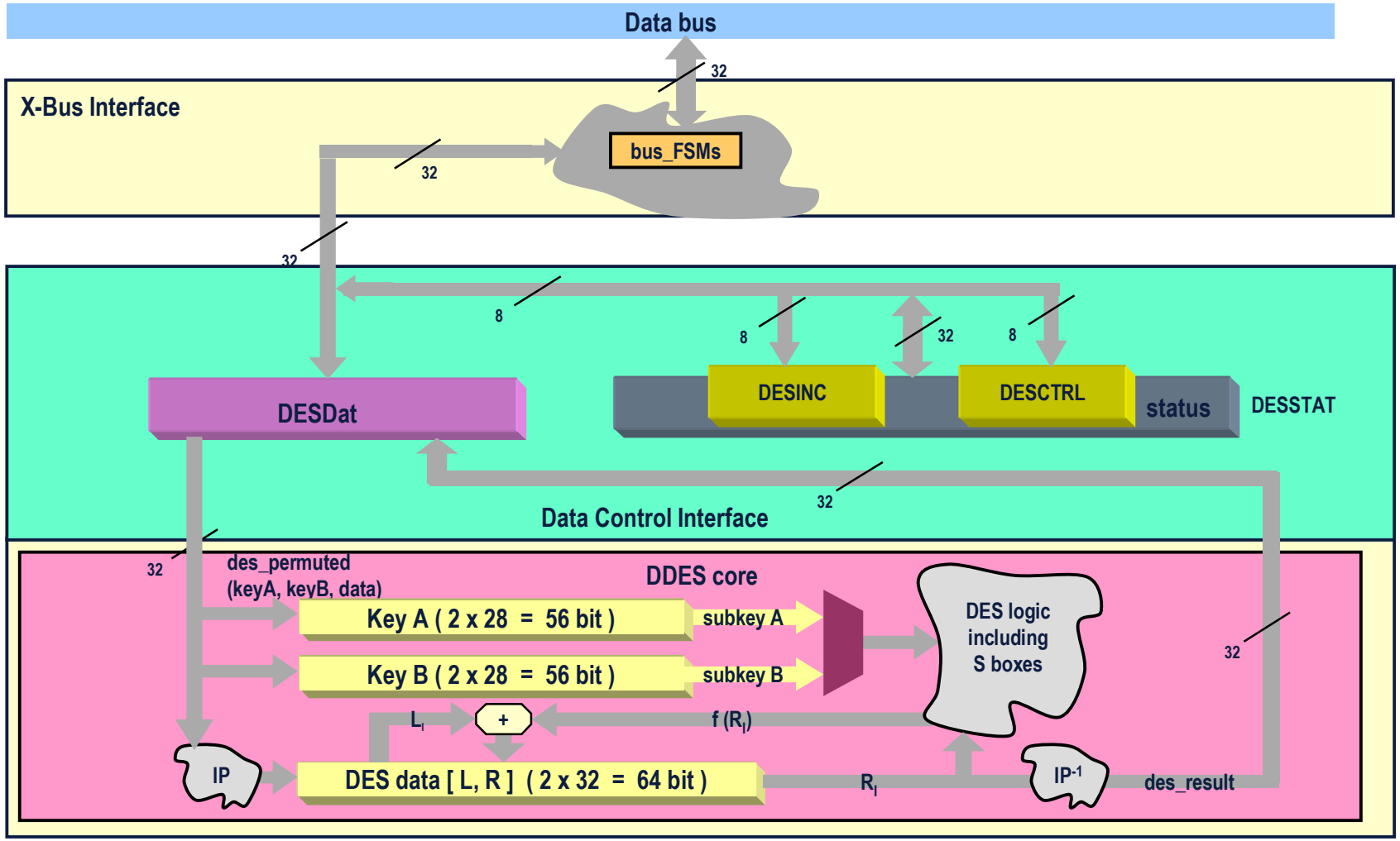


Sleep Mode

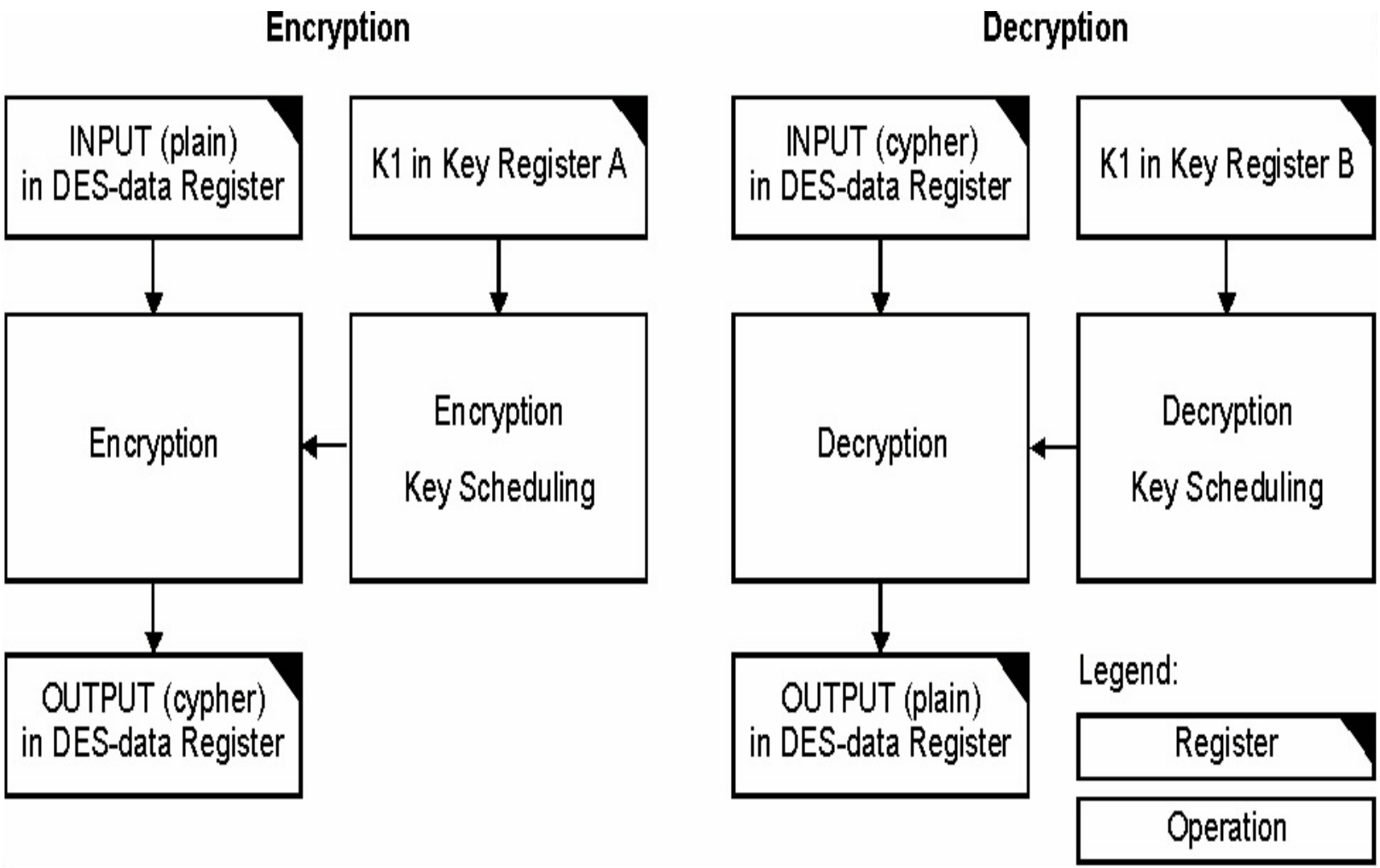

Wake-up
External Clock
System Clock
External Clock
System Clock


ICOCNT
31
24
23
16
15
14
12
11
8
7
3
2
0
rfu
PCNT
CMODE
REMODE
MPSCAL
KBURST
MODE

Virtual SFR DESdat



Single DES High Performance Mode, HPM



Virtual Machine

Program

```
c = a + b
```

Virtual Machine

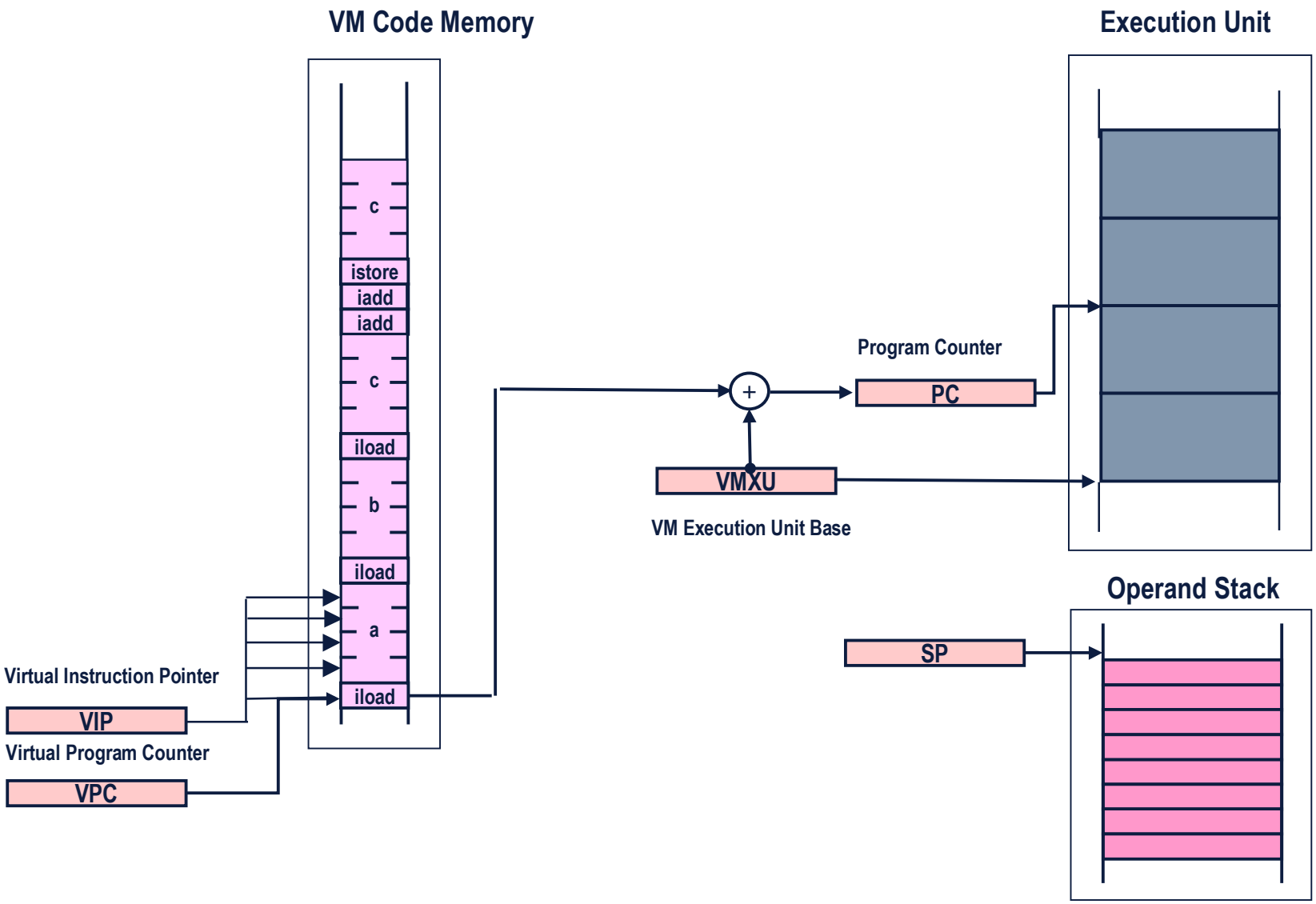
```
iload   a
iload   b
iadd
istore  c
```

Hardware

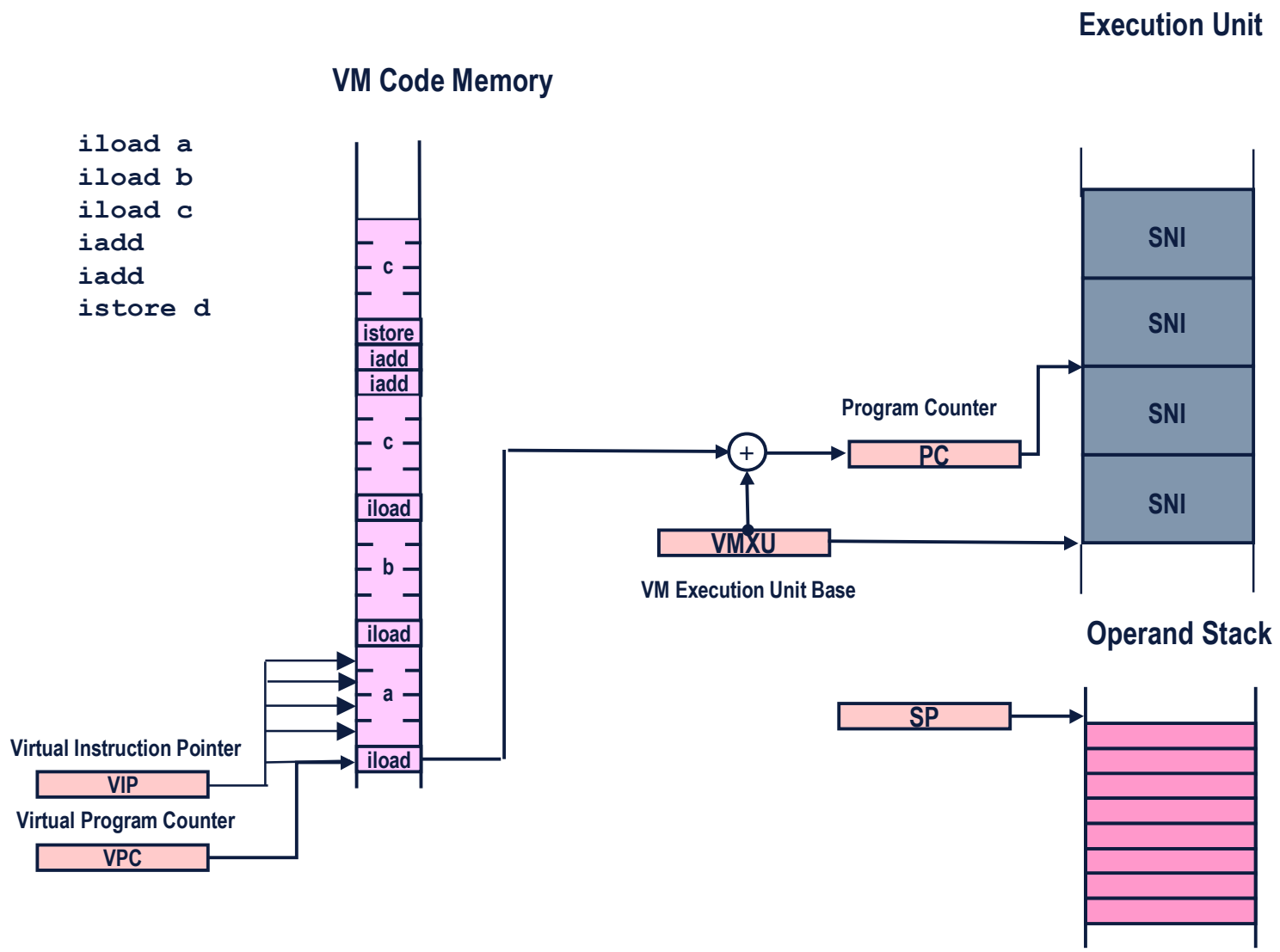
```
iload:
Vlpar.w d15
vlfst.w [-a10],d15,[+[a15]5

iadd:
ld.w    d14,[a10]4
add     d15,d14

istore:
vlfld.w [+a10],d15,[+a15]1
```

Infineon technologies
Never stop thinking

Memory used by the VM

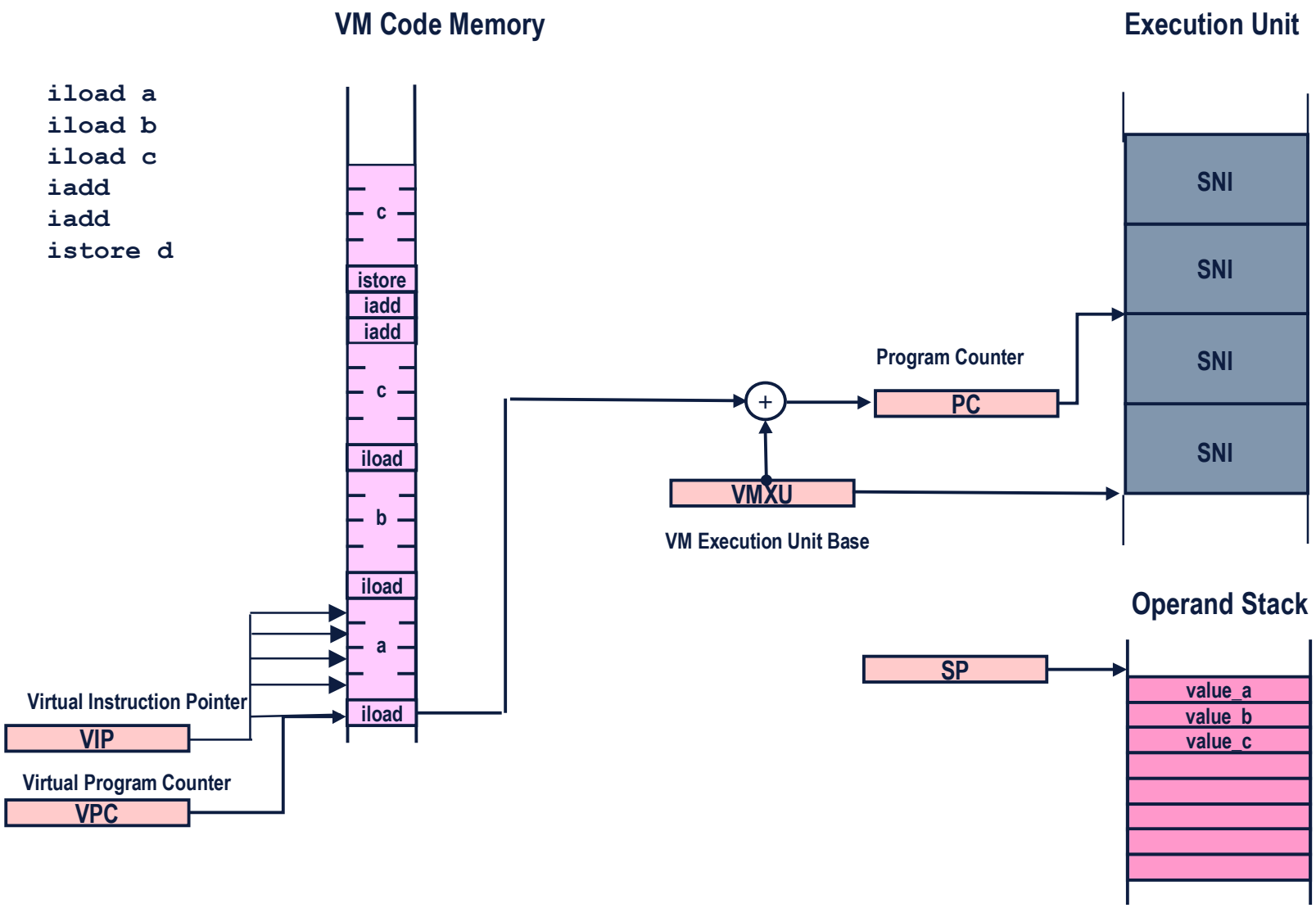


Executing a VM instruction

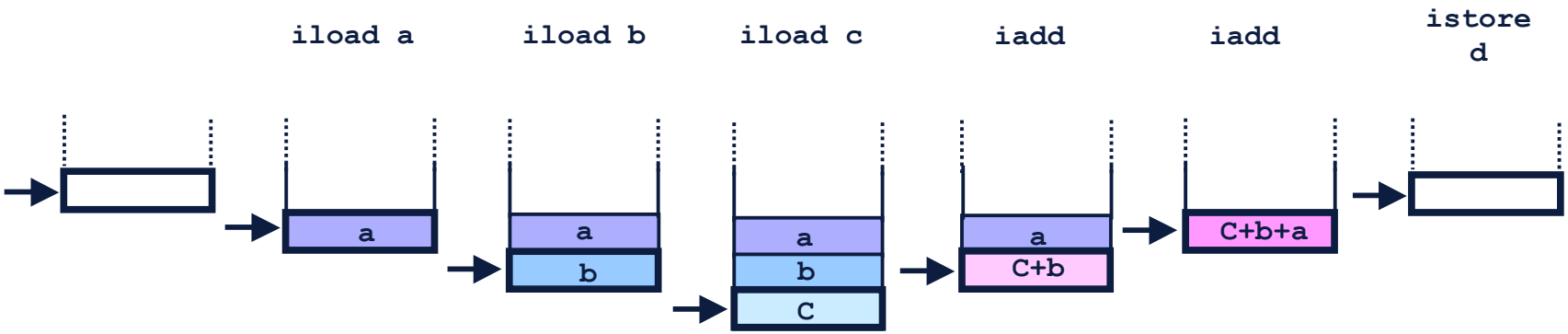


Never stop thinking

Sequence of native Instructions



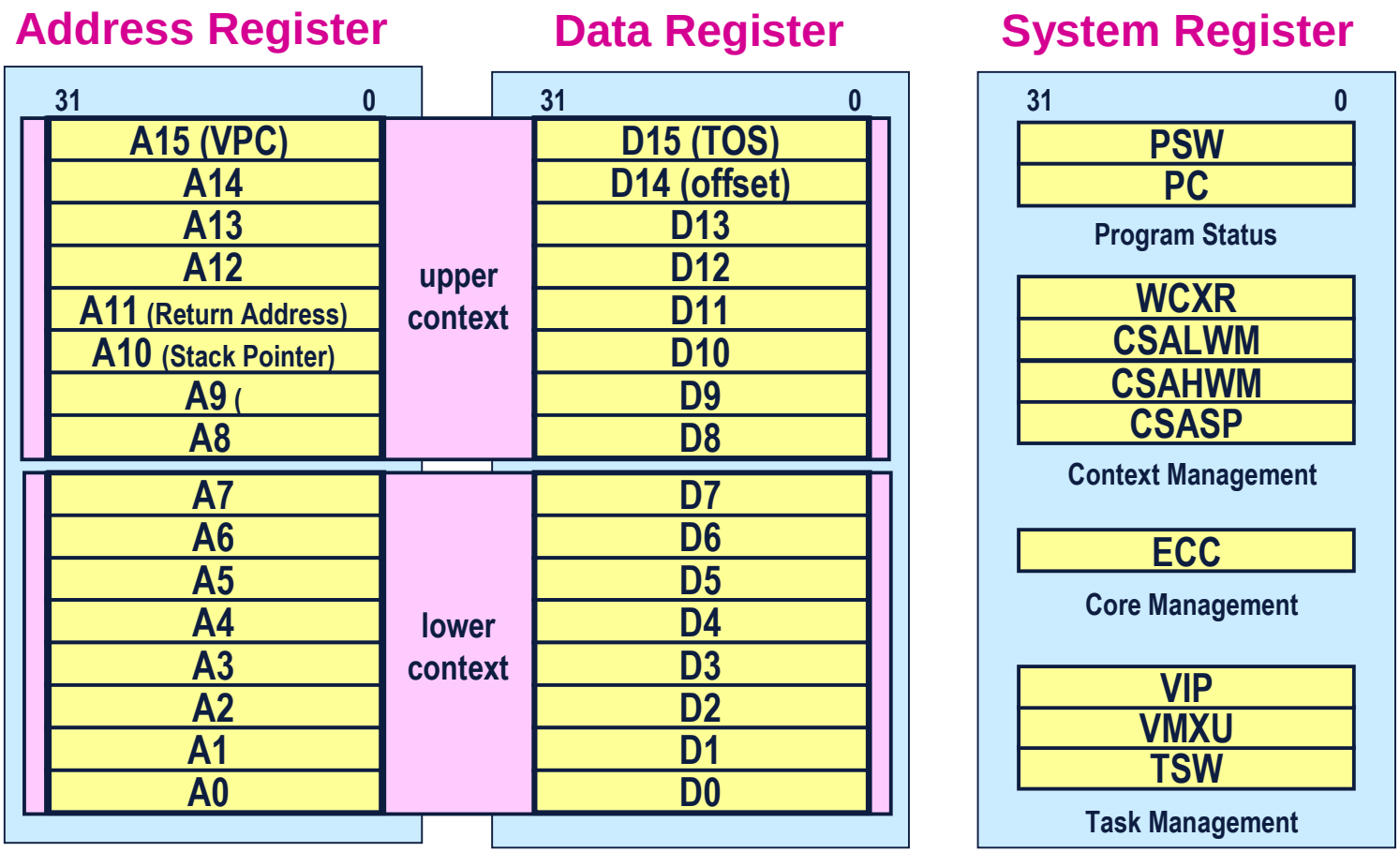
Stack Operations




```
Iload  a   ; push a onto stack
iload  b   ; push b onto stack
iload  c   ; push c onto stack
iadd       ; reads c and b from stack, perform addition
           ; and stores result back onto the stack
iadd                ; reads c+b and a from stack, perform addition
           ; and stores result back onto the stack
istore d   ; reads c+b+a from stack,
           ; and stores result into memory or register
```

Never stop thinking

VM Register Usage



Implementing a Virtual Machine (1)

- Basic steps to execute a Virtual Machine`s Bytecode:
  - Read byte code instruction
  - increment virtual PC
  - branch to byte code specific execution sequence
  - execute sequence

```
switch:   ld.bu     D8,[A15+]1
          addsc.a   A9,A8,D8,3
          ji        A9

sequence:...
          j         switch
```

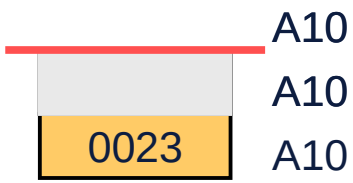
Never stop thinking

Implementing a Virtual Machine (2)

- Stack machine fundamentals
  - Every operation is executed using parameters from TOS
  - The result is returned to TOS
  - Data are pushed to / popped from TOS

e.g. Java code: **`a = b + c`**

```
sload b
sload c
sadd
sstore a
```



Never stop thinking

SLE88CxxS Smart Card Controller Family
Virtual Machine Support

VM Instructions:

VLFLD.x	Fetch VM bytecode, branch to code sequence, load data
VLFST.x	Fetch VM bytecode, branch to code sequence, store data
VLPAR.x	Fetch VM parameter byte
VLPOFF.x	Fetch VM positive offset byte
VLNOFF.x	Fetch VM negative offset byte
VLJ	Jump to new bytecode location

Never stop thinking

Roadmap 32 Bit Security Controller: SLE88 S/P

C9FLR (0.22µ) | C11FL (0.13µ)

EEPROM-Size

272K

144K

80K

72K

SLE 88CX2560P
300 KB Flash
16 KB RAM
272 KB EEPROM
Crypto2000/DES/AES
Caches 1kB / 2kB
66 MHz, 1,8-5V
PSL

SLE 88CX1280P
256 KB Flash
10 KB RAM
144 KB EEPROM
Crypto2000/DES
Caches 1kB / 2kB
66 MHz, 1,8-5V
PSL

qualified

SLE 88CX720P
240 kB ROM
8 kB RAM
80 kB E²PROM
ACE/DES
Caches 1kB / 2kB
55 MHz, 3-5V
PSL

SLE 88CUX723P
240 KB ROM / Flash
8 KB RAM
80 KB EEPROM
Crypto2000/DES
Caches 1kB / 2kB
66 MHz, 1,8-5V
PSL
USB 2.0

SLE 88CX722P
240 KB ROM / Flash
8 KB RAM
80 KB EEPROM
Crypto2000/DES
Caches 1kB / 2kB
66 MHz, 1,8-5V
PSL

SLE 88CX644S
192 kB ROM
6 kB RAM
72 kB EEPROM
ACE/DES
Caches 0.5kB / 1kB
33 MHz, 1,8-5V
PSL

SLE 88CLX723P
240 KB ROM / Flash
8 KB RAM
80 KB EEPROM
Crypto2000/DES
Caches 1kB / 2kB
66 MHz, 1,8-5V
PSL
Contactless Interface
Type A / B (& FeliCa?)

Availability of ES | Functionality

available | Q4/2003 | Q1/2004 | Q3/2004 | Schedule tbd.

available | in development | new idea

Never stop thinking

Availability
88 Family of 32-bit Chip Card Controllers: 88P and 88S

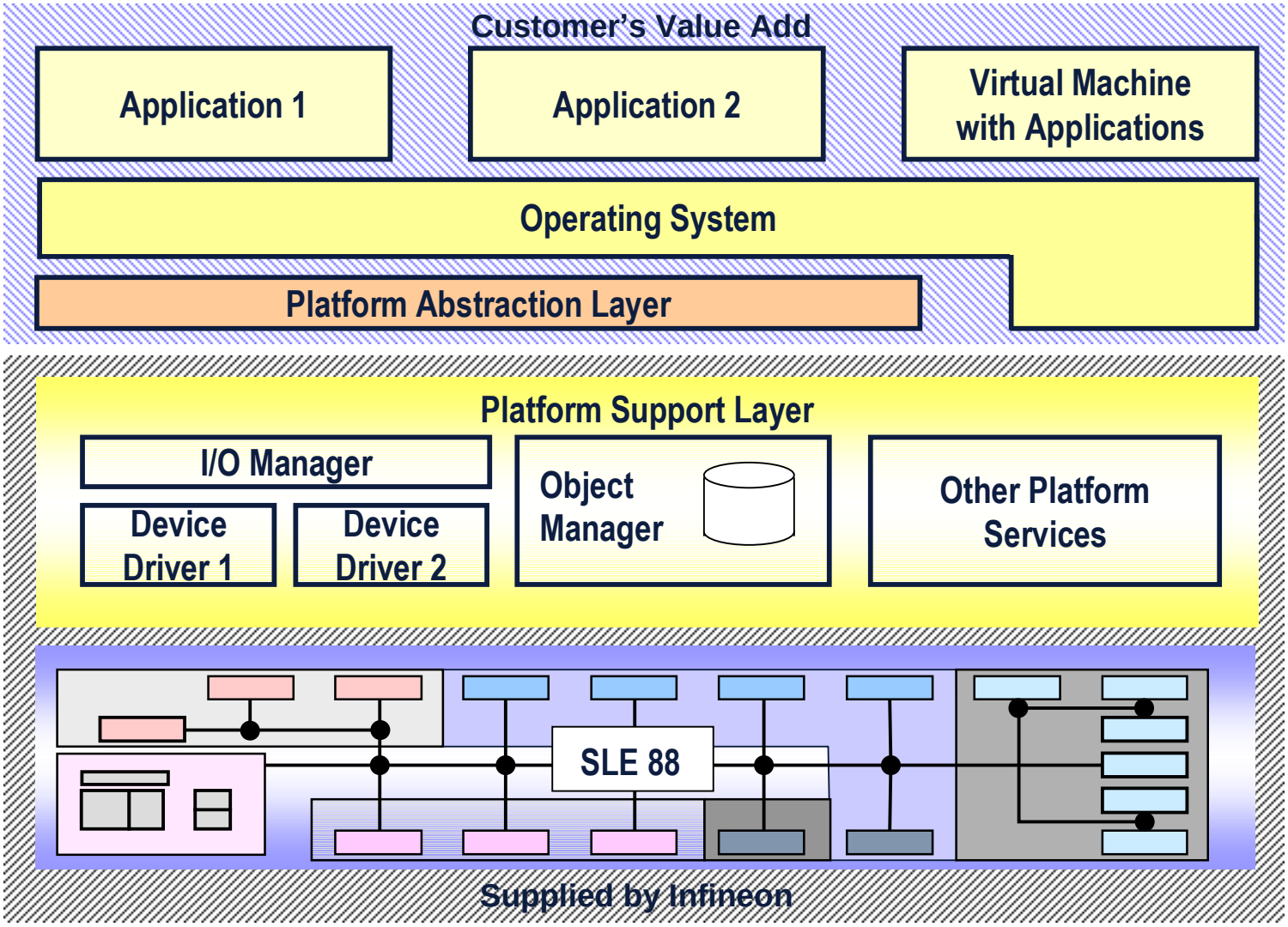
	0,22µm	0,13µm
	SLE88CX720P	**SLE88CFX4000P**
	B12	**A11**
Product ES CDIP/Module	available	Nov 03
Smartmask Card	Jan 03	Dec 03
SDK	available	May 03
Emulator/Bondout	B13 usable, C12 Mar 03	July 03
CC Certification	May 03	Mar 04
Visa level 3	June 03	Apr 04
	Qualified	final product qualification Jan 03

Never stop thinking

Never stop thinking

Overview
Platform Support Layer
PSL

Architectural Overview



PSL Versionen

PSL Version	Small*	medium**	large***
IO-Manager	2		
Kernel	1,5		
ObjectManag.	2,5	3	
MMU	6,8	2	
EEPROM	4,9	2	
ICU	1,8		
ICO	0,5		
RNG	0,8		
DES	1		
UART	1,6		
Timer	0,8		
ACE	2,5	3	5,5
Loader	2,6		
Protocol	5		
SHA		1	
AES			2,5
CRC			0,5
Total ROM	**34,3**	**45,3**	**53,8**
Rollback buffer	6	6	6
others	2	2	2
Total E²	**8**	**8**	**8**
Receive buffer			
RNG buffer			
ITR & Trap handler			
others			
CSA stack	0,8	1	1
Task stack	0,8	1	1
Total RAM	**2,8**	**3,5**	**3,5**

* Recommendation for „s“ Version

** Recommendation for „p“ Version

*** Contents of Smartmask

Infineon technologies
Never stop thinking

SLE88 Family Tool Concept

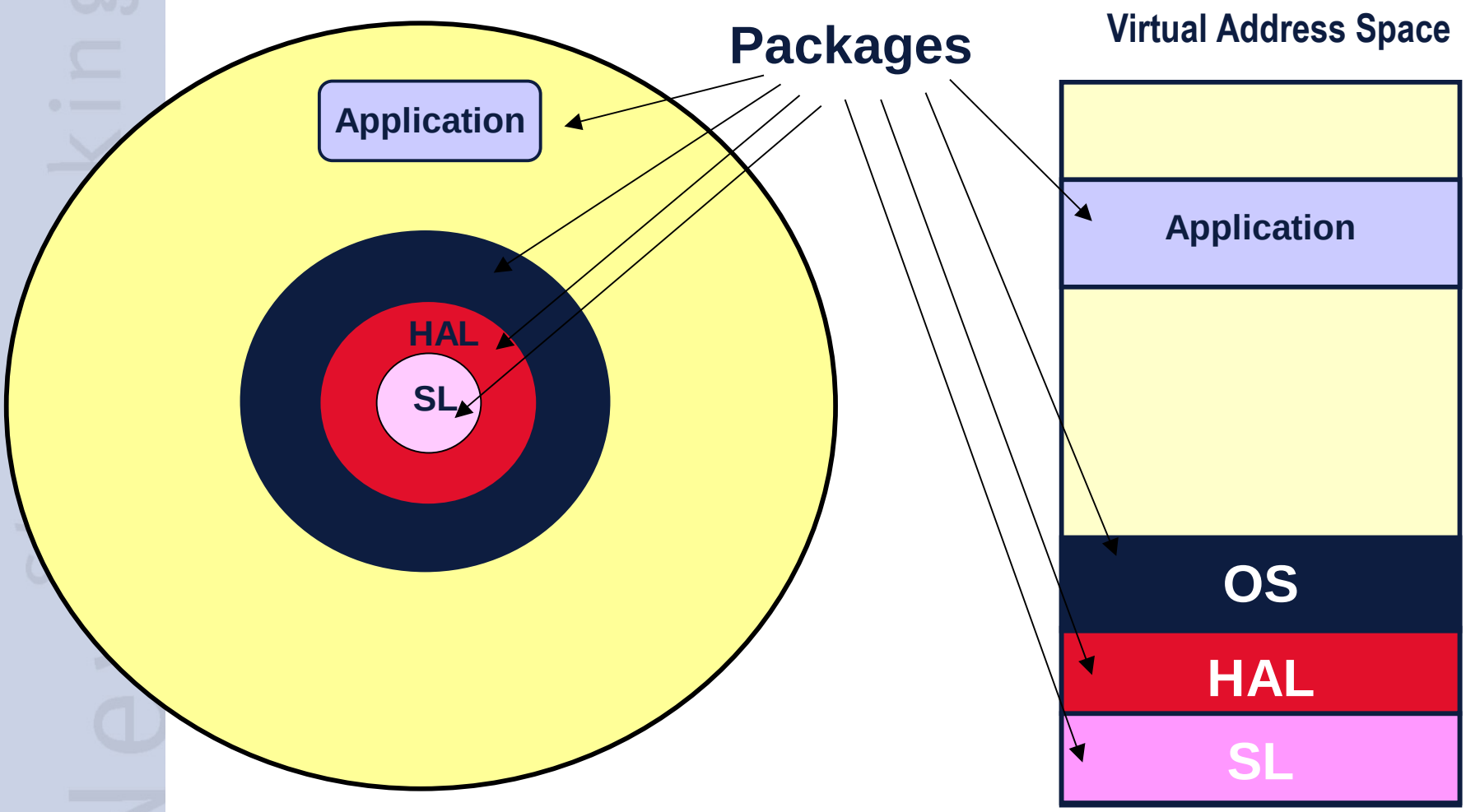
Never stop thinking

Contents

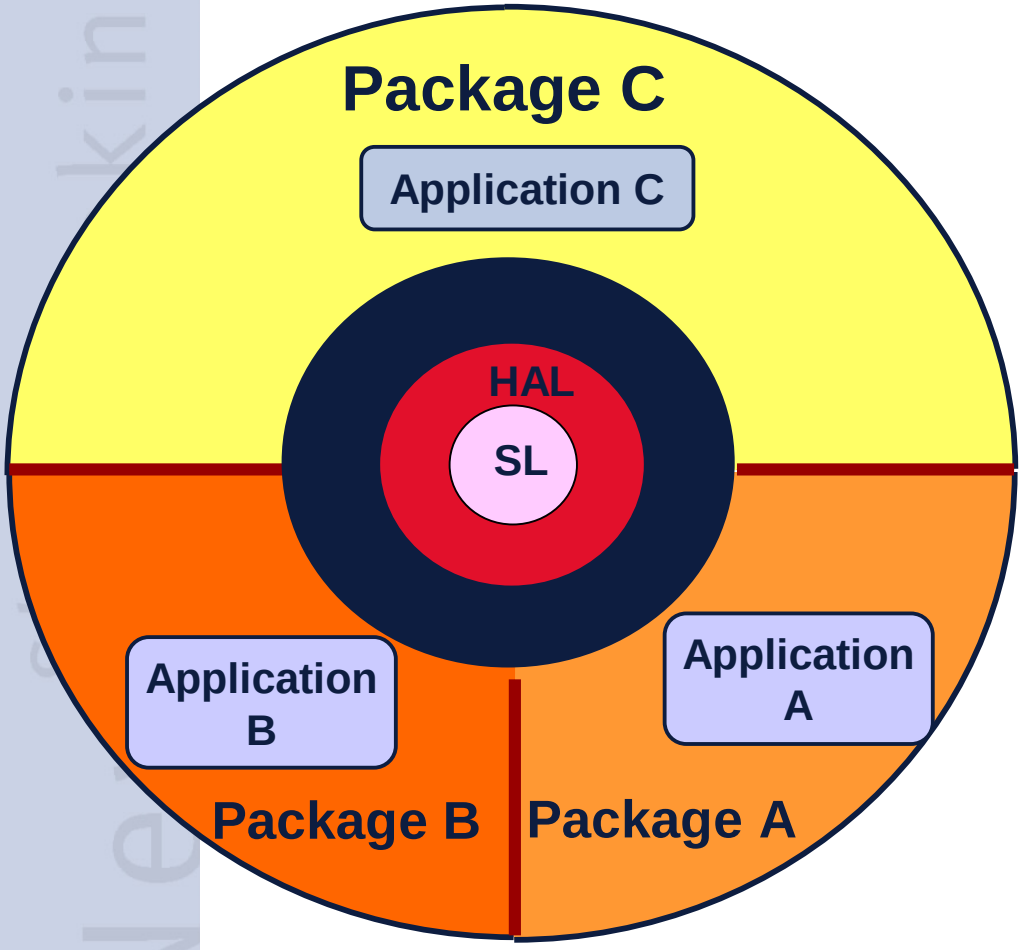
- Single Package Concept
- Multiple Package Concept
- Package Generation
- Mask Generation
- ROM Mask Generation
- Starting an Application

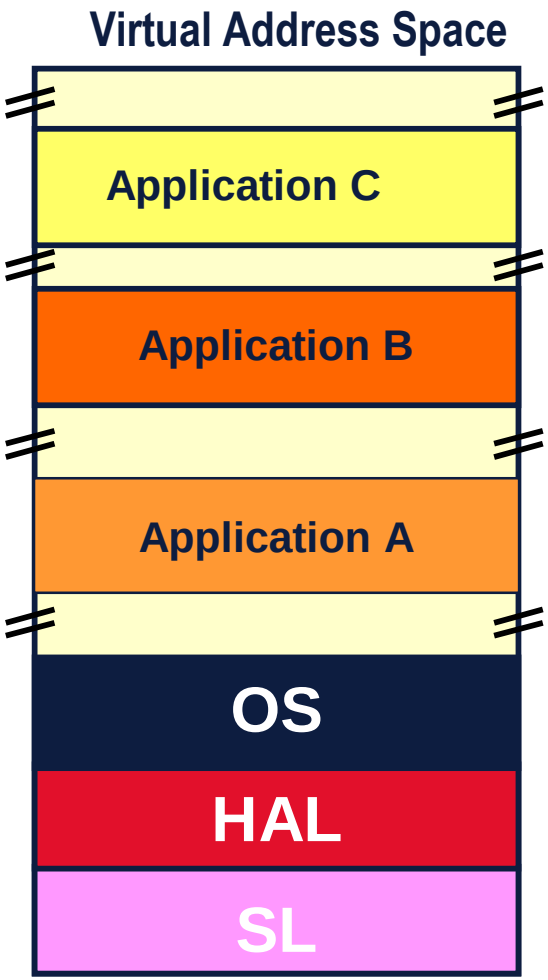
Never stop thinking

Single Package Concept

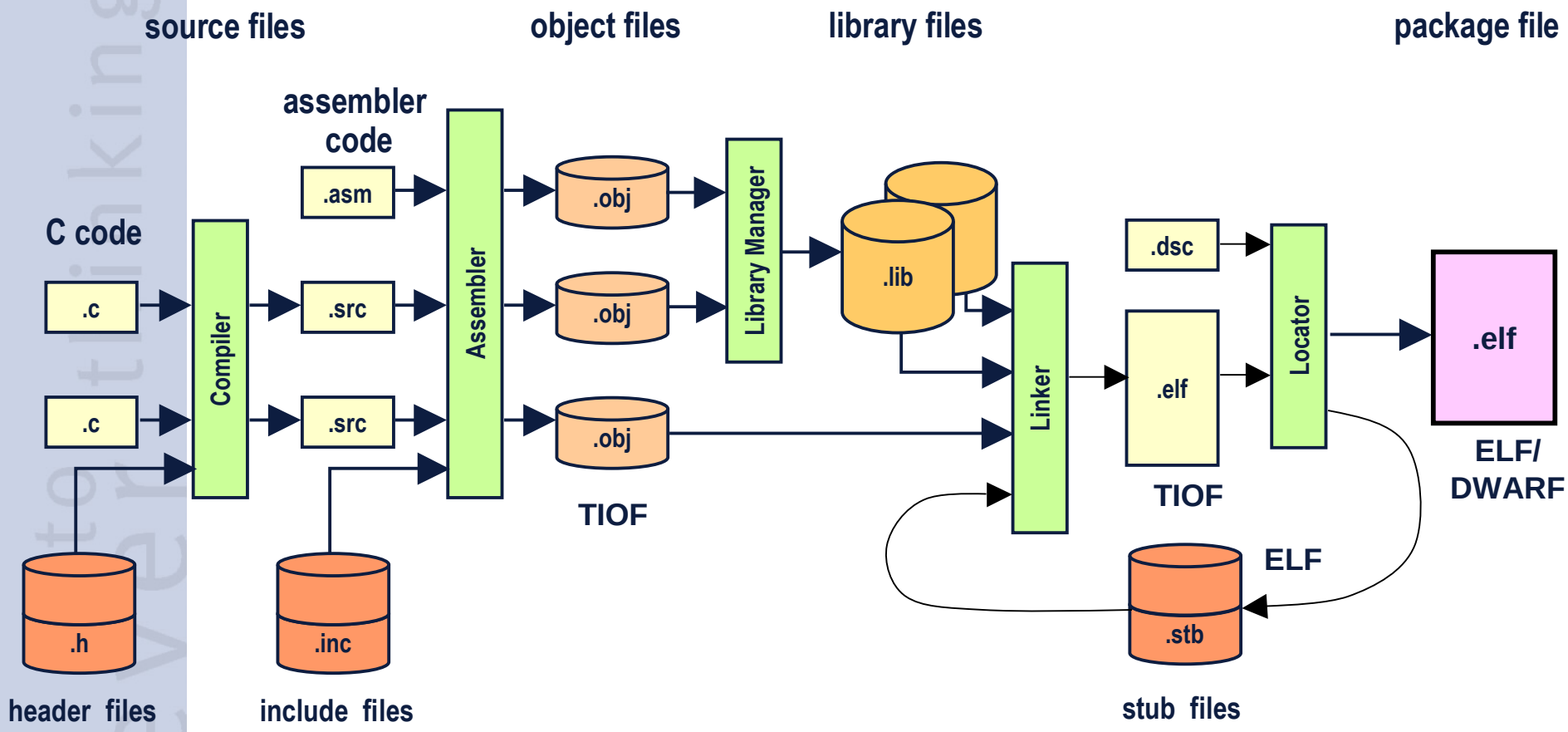


Multiple Package Concept



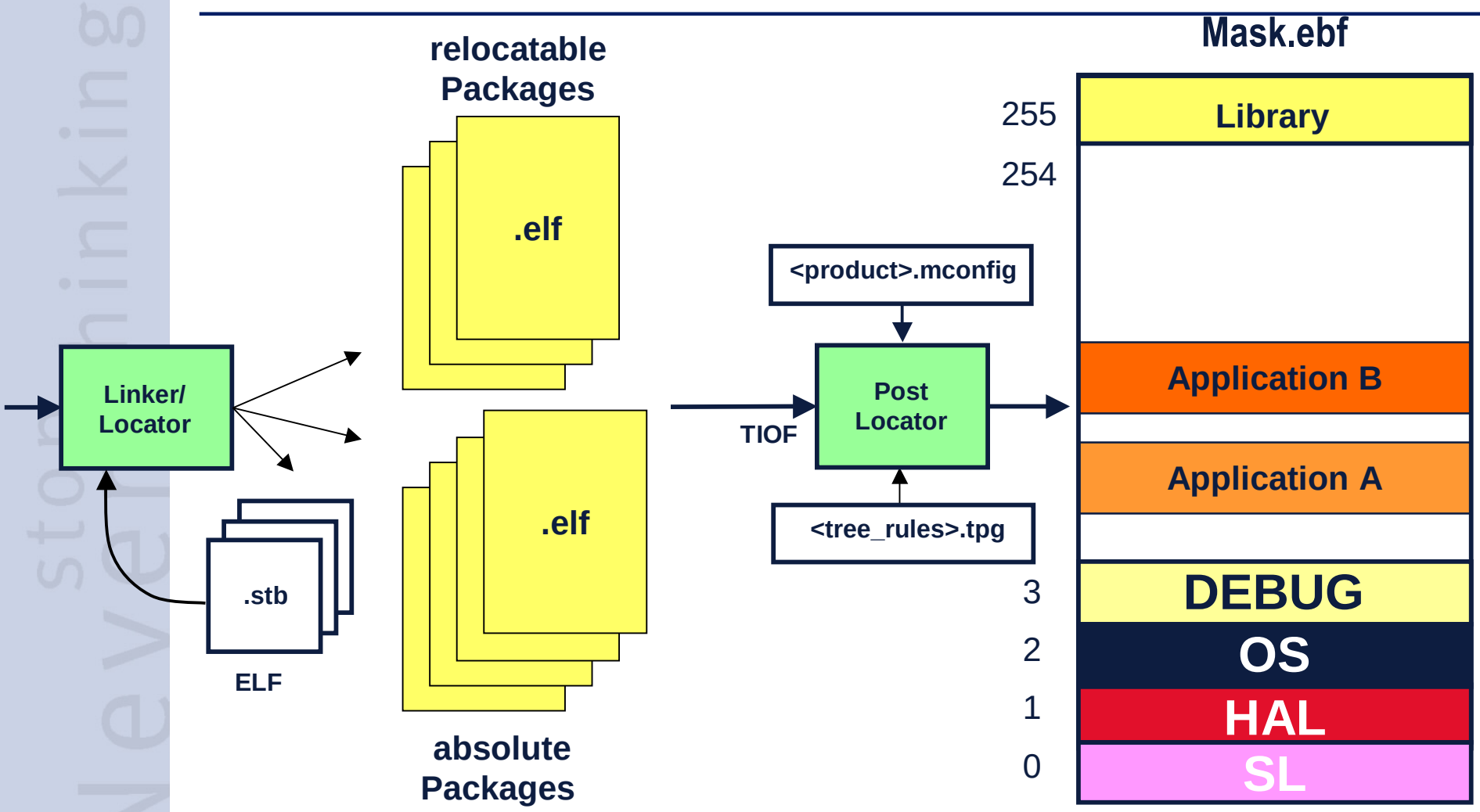


Package Build Process Overview

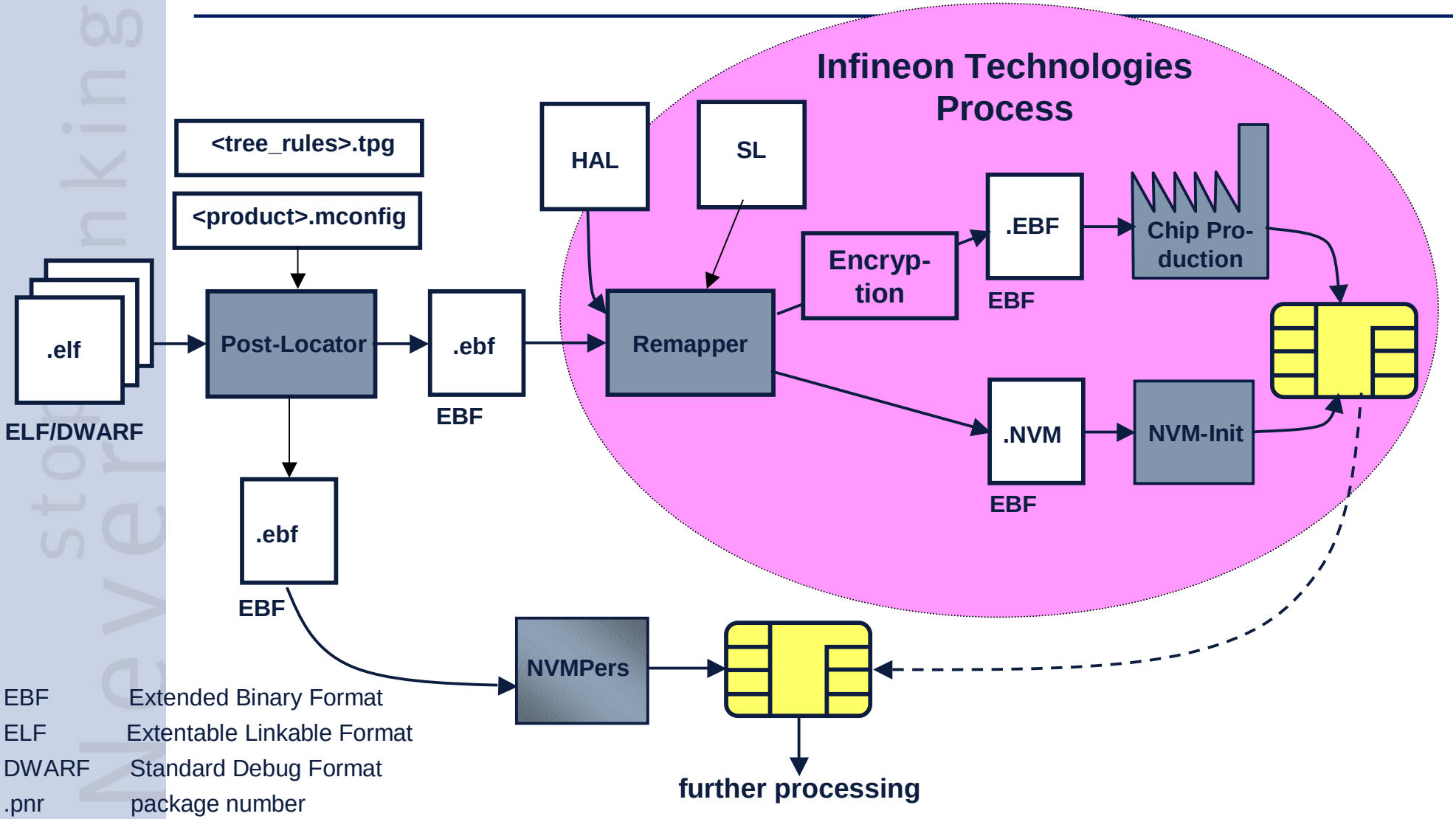


ELF	Extentable Linkable Format
TIOF	Target Independent Object fFormat
.stb	Stub File

Mask Generation

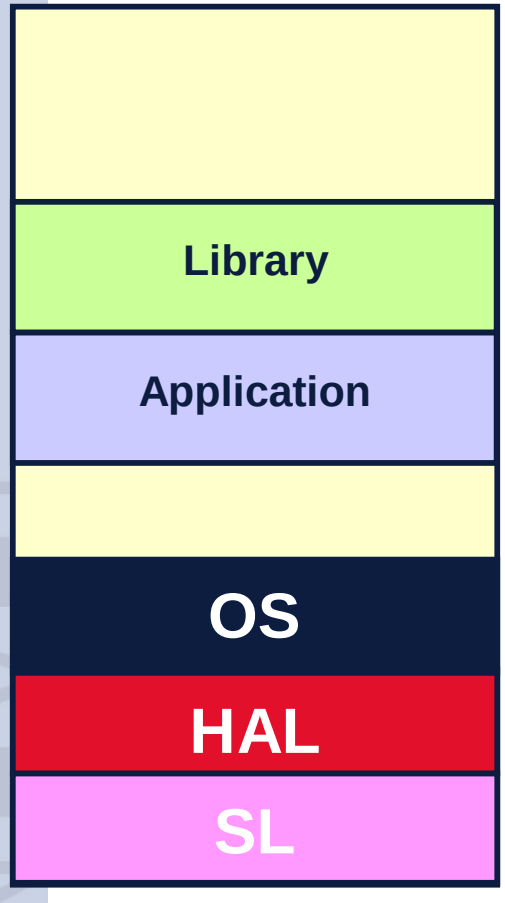


ROM Mask Generation



EBF	Extended Binary Format
ELF	Extentable Linkable Format
DWARF	Standard Debug Format
.pnr	package number

Starting an Application



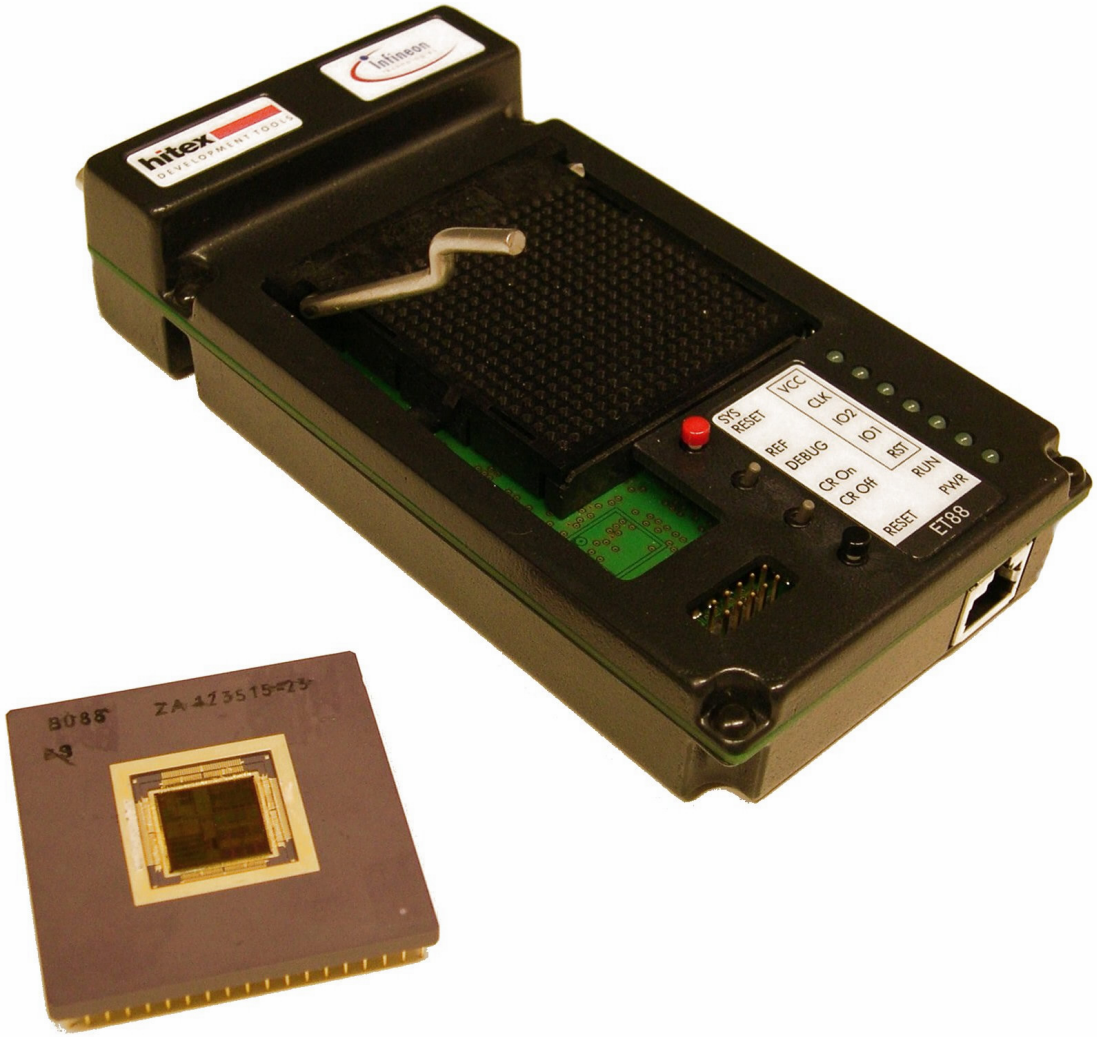
4th Application is called first time by OS layer, it process the user application

3rd OS layer is called first time by HAL layer, it will call the application

2nd HAL layer is called first time by SL layer, it will call the OS layer

1st Processed first and will call the HAL layer

SLE88 Tools
Emulator Hitex



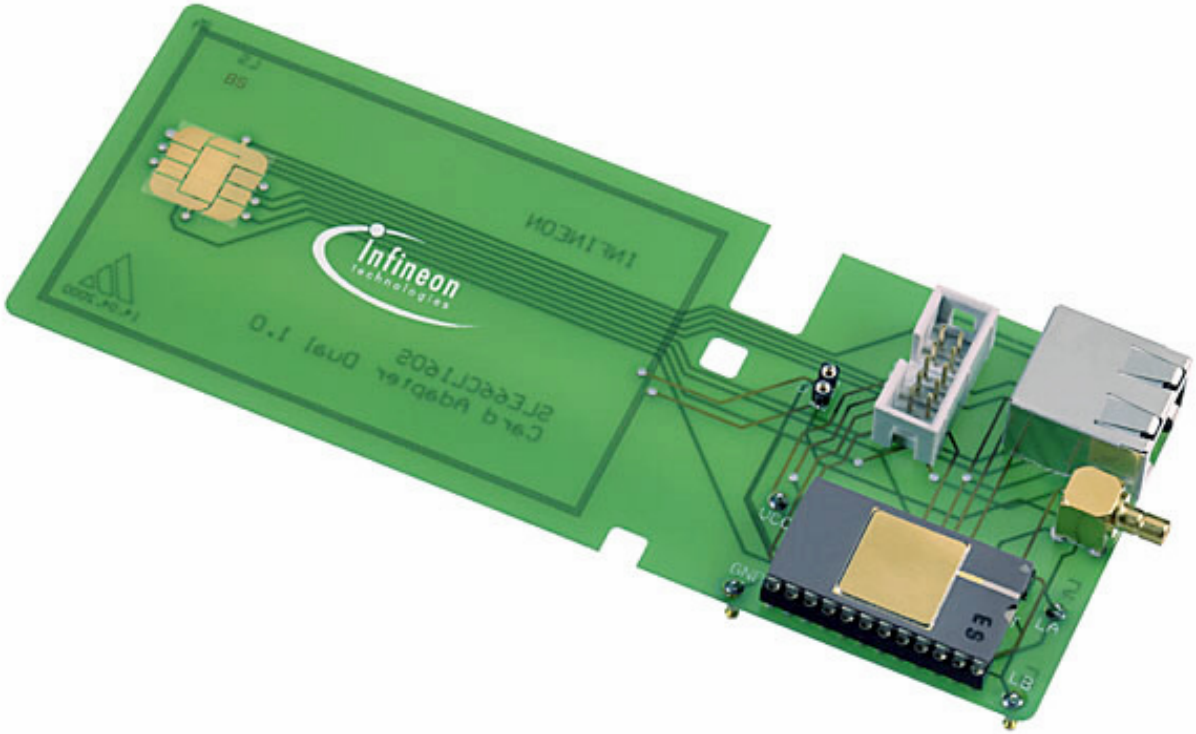
Never stop thinking

SLE88 Tools
Emulator Sci Worx

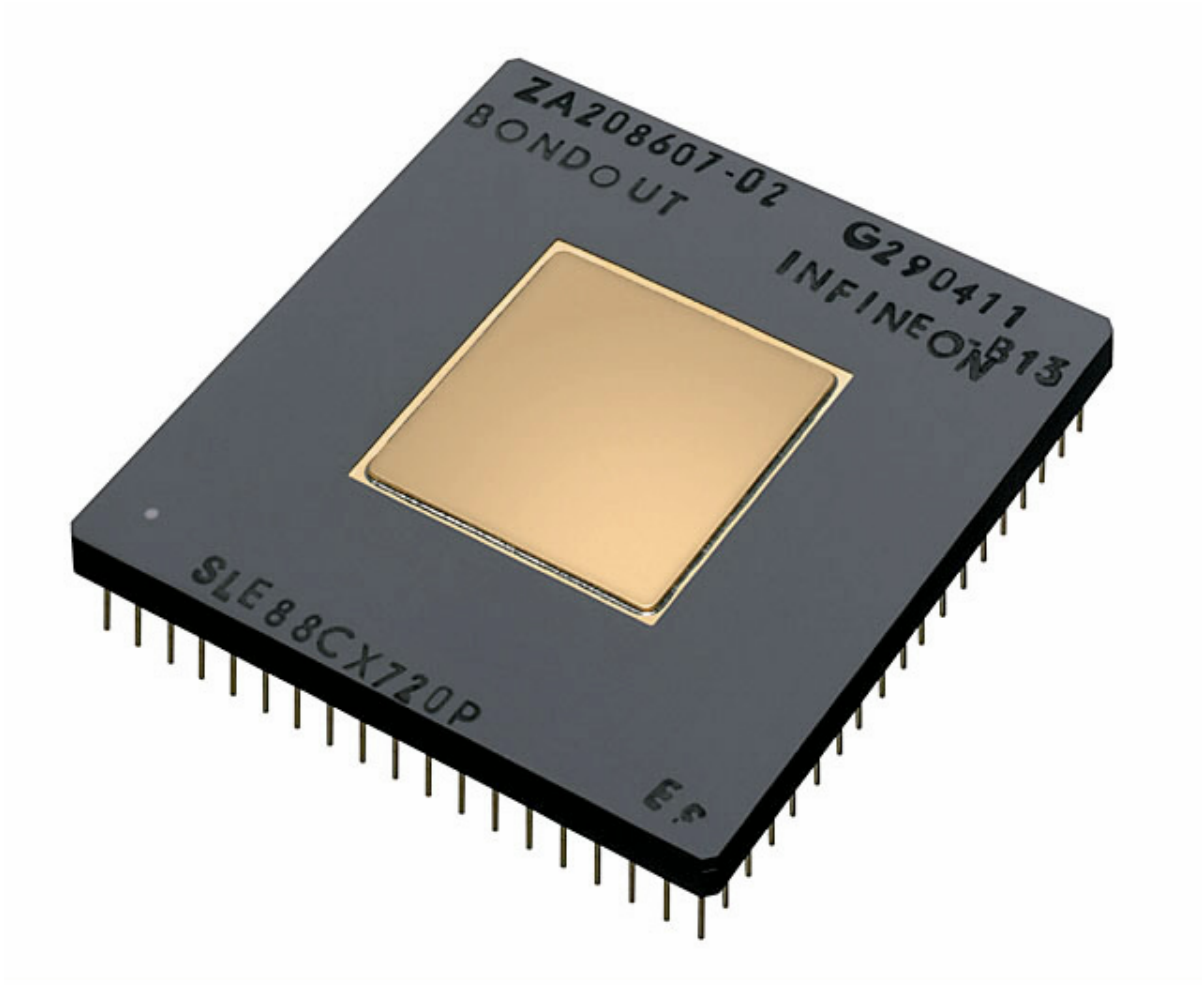
SLE88 Tools
SDK

SLE88 Tools

CDIP + Card Adapter

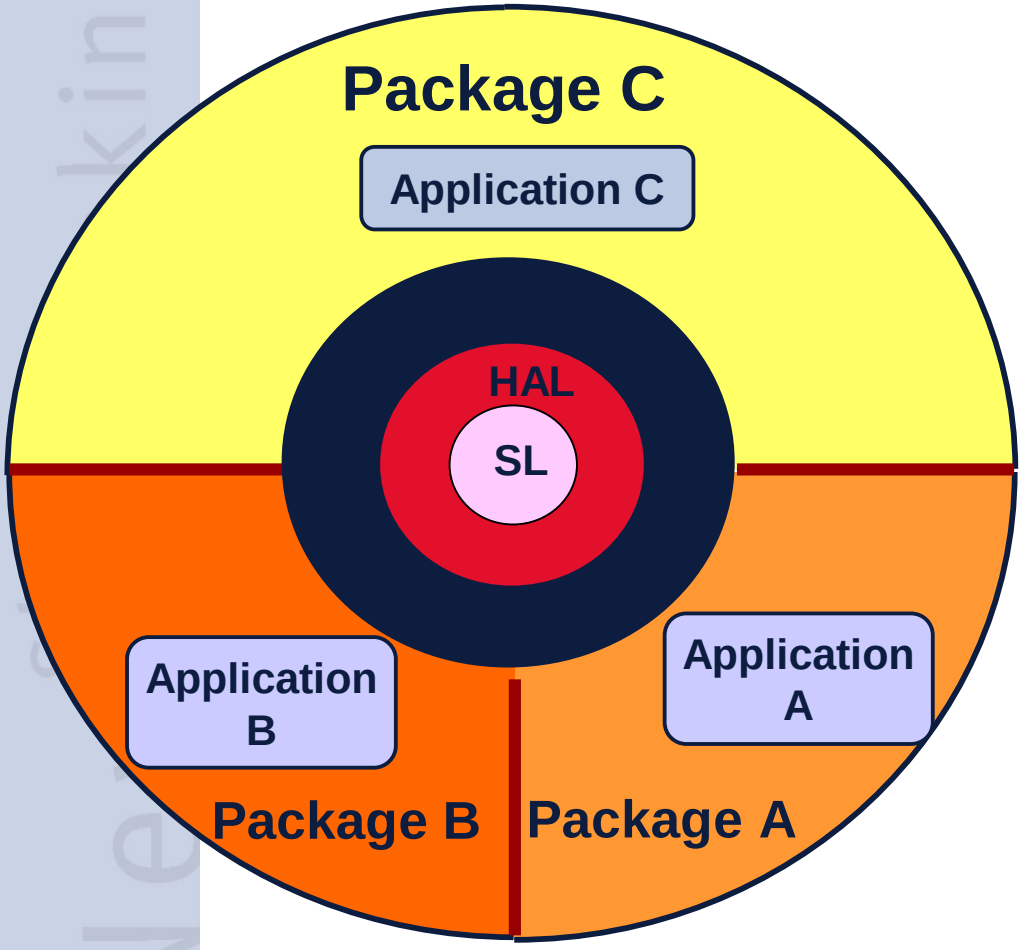


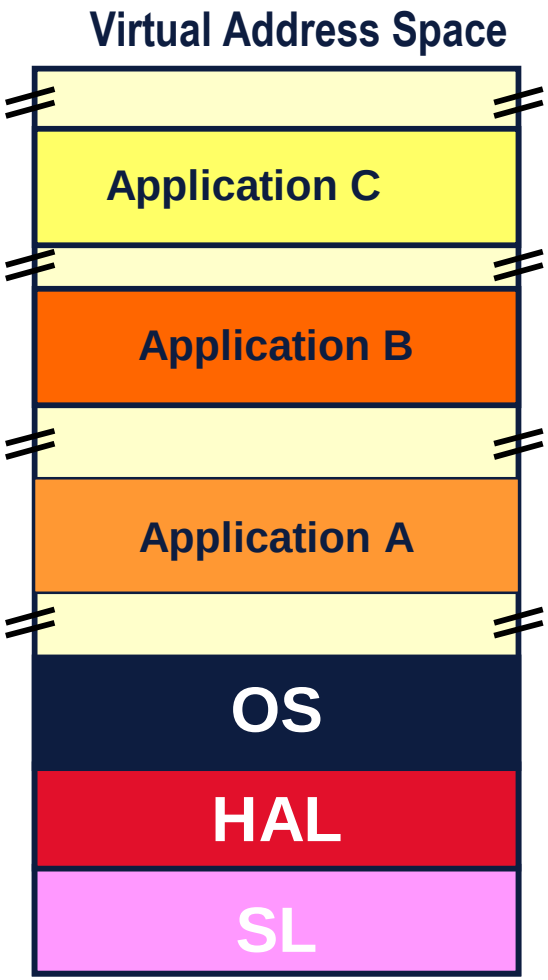
SLE88 Tools
Bondout



SLE88 Tools
Sample Card

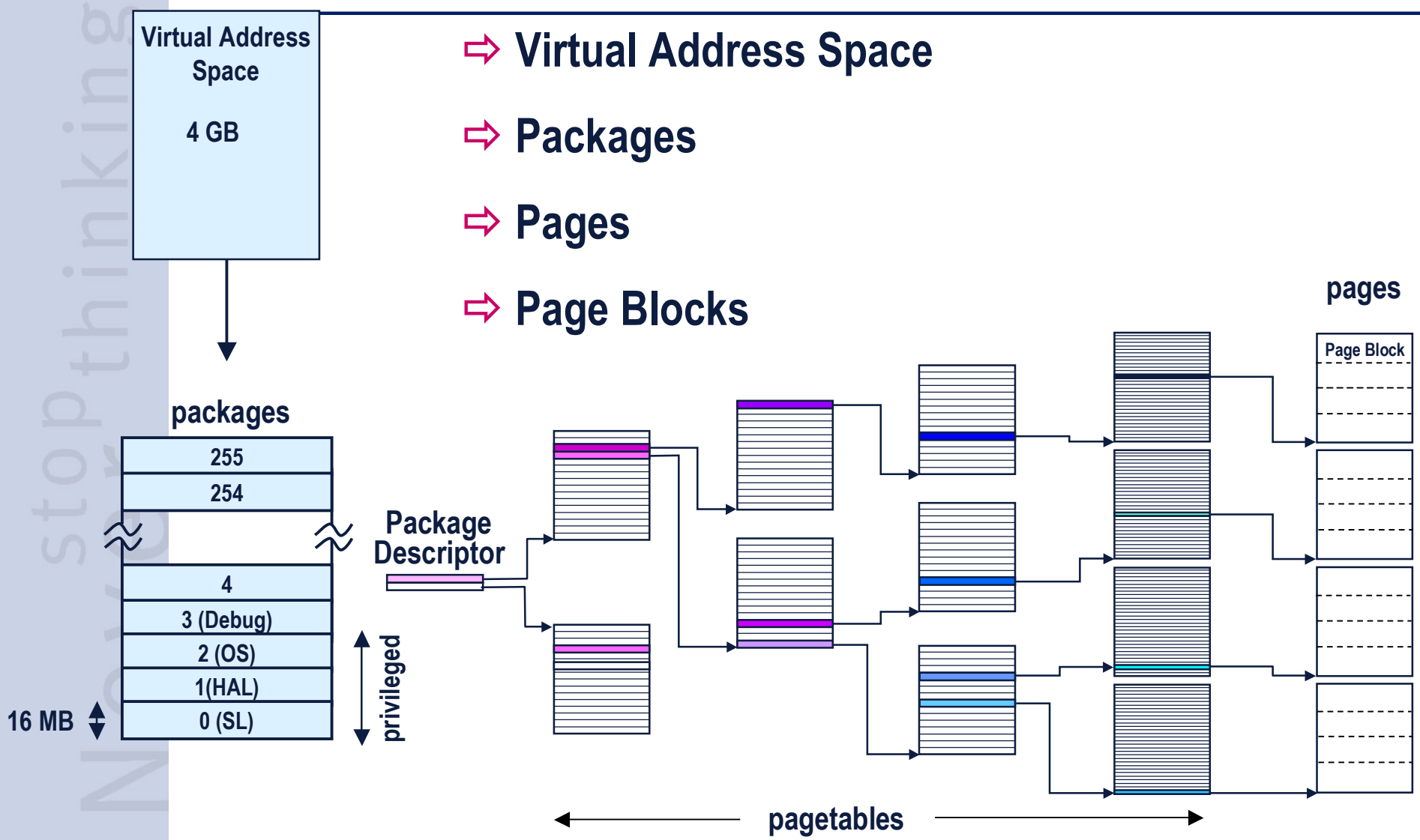
Memory Protection Mechanisms





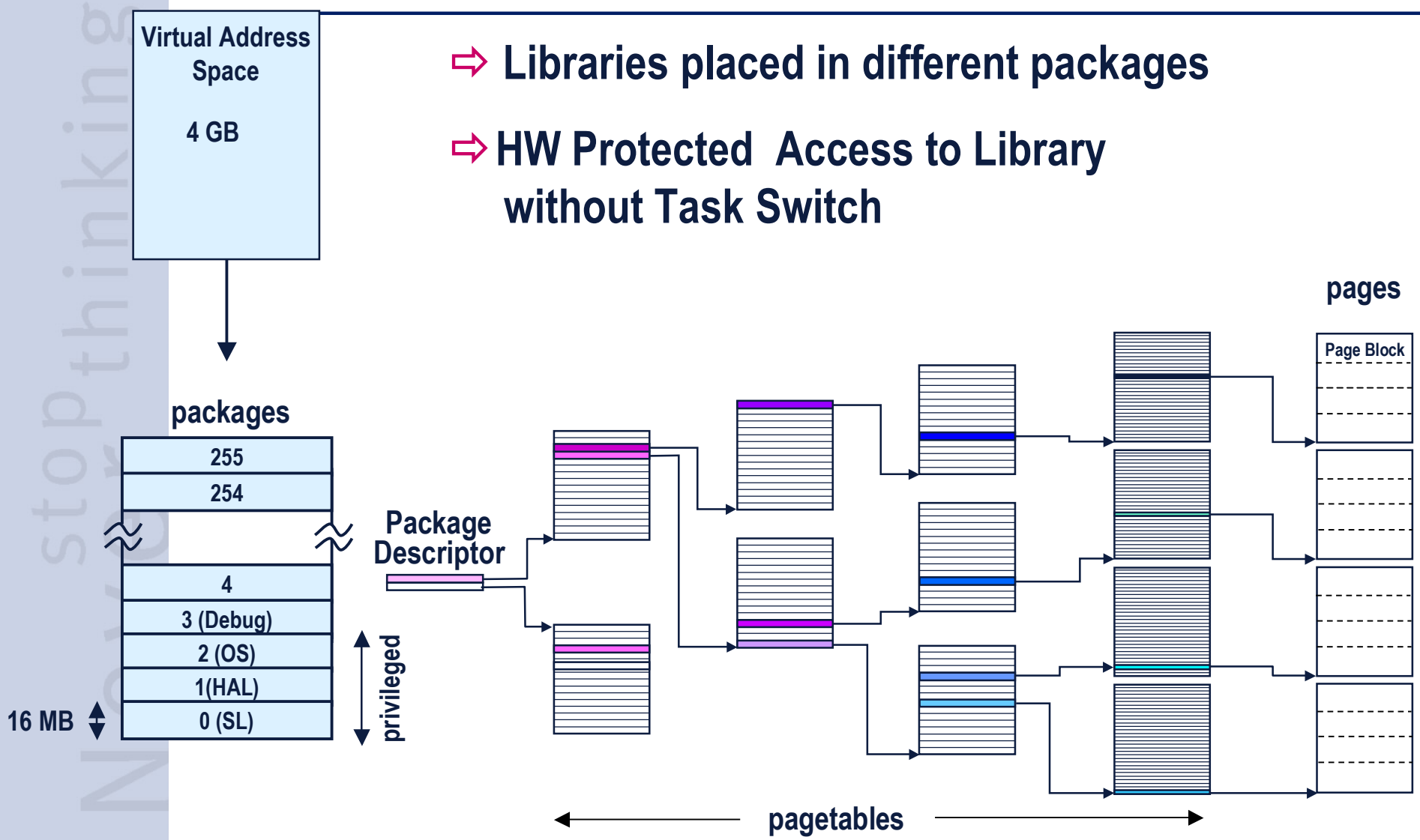
Security Layer Overview

- ⇨ Virtual Address Space
- ⇨ Packages
- ⇨ Pages
- ⇨ Page Blocks



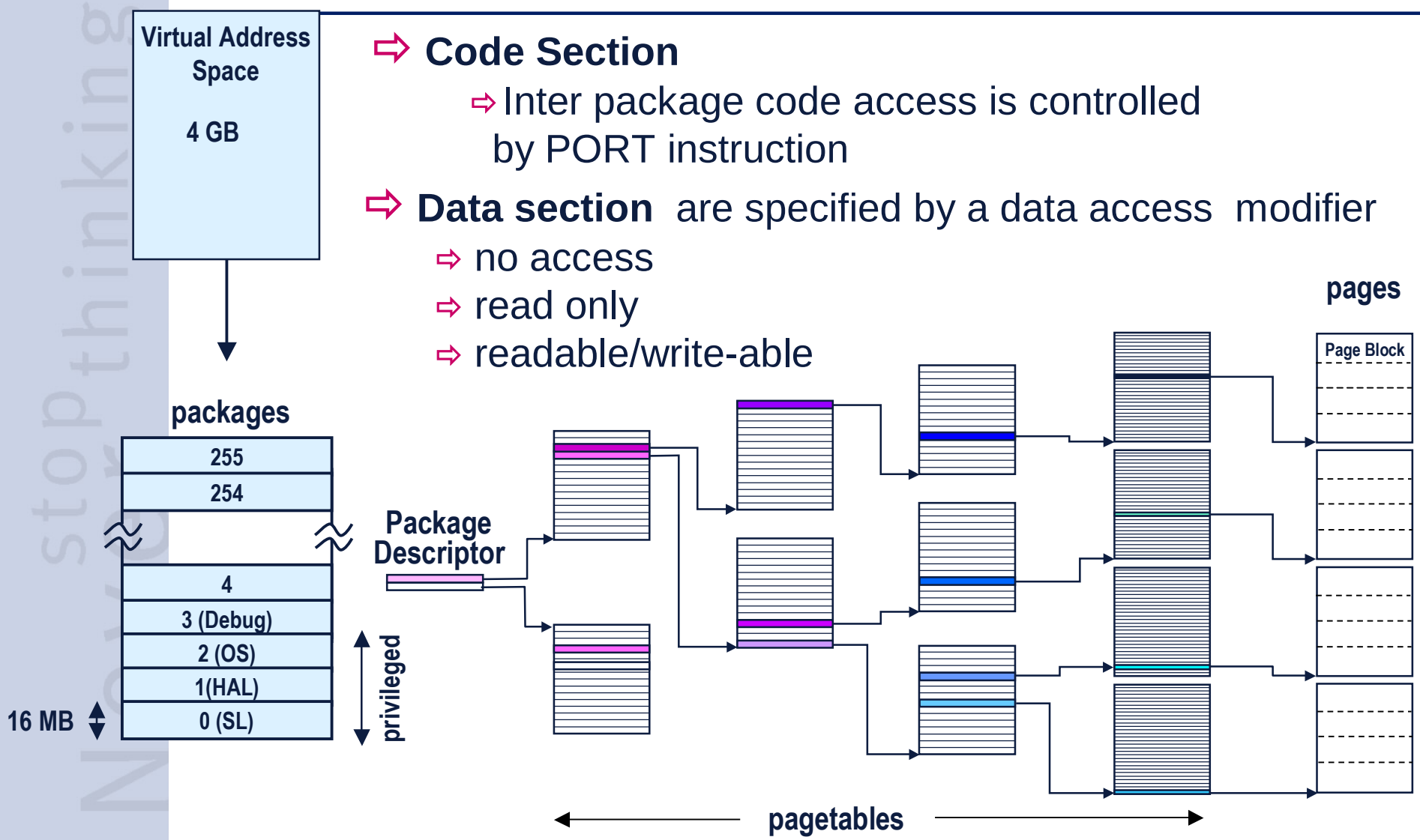
Protection on Package Level

- ⇨ Libraries placed in different packages
- ⇨ HW Protected Access to Library without Task Switch

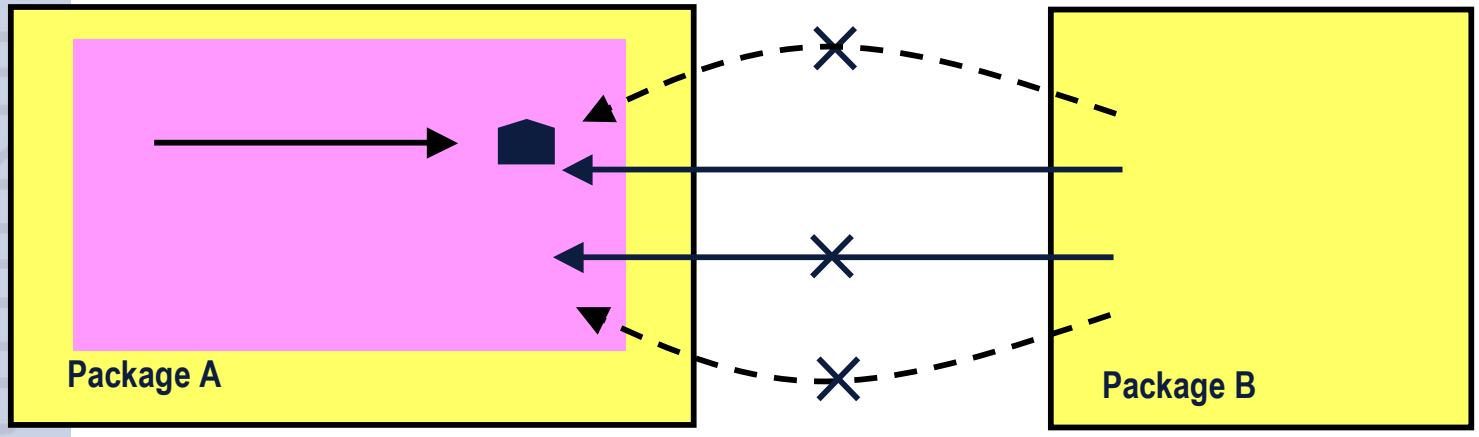


Access Control

- **Code Section**
  - Inter package code access is controlled by PORT instruction
- **Data section** are specified by a data access modifier
  - no access
  - read only
  - readable/write-able



Code Access Control



export function (PORT)

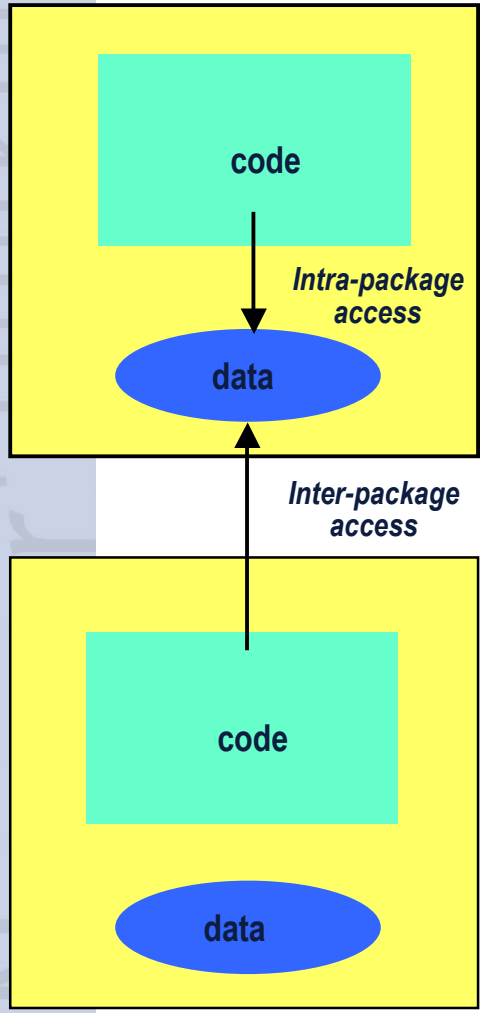
direct or indirect function call

jump

- **Inter-Package code access**
  - Inter-package jumps are illegal.
  - Inter-package calls only via PORT
  - Return addresses cannot be manipulated.
- **Intra-Package code access**
  - without any restriction
  - any illegal jump or call results in a trap PRIV.

Data Access Control

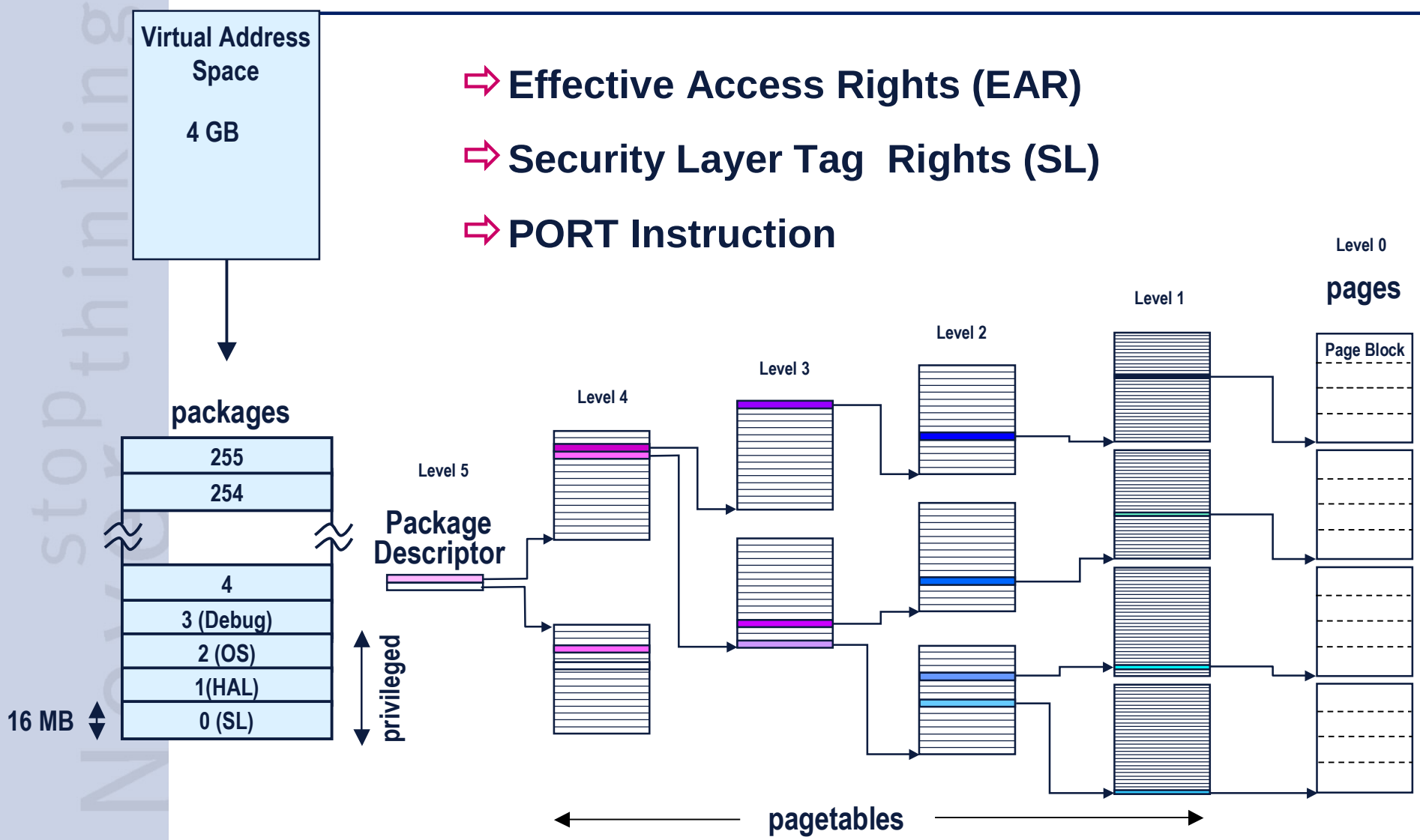
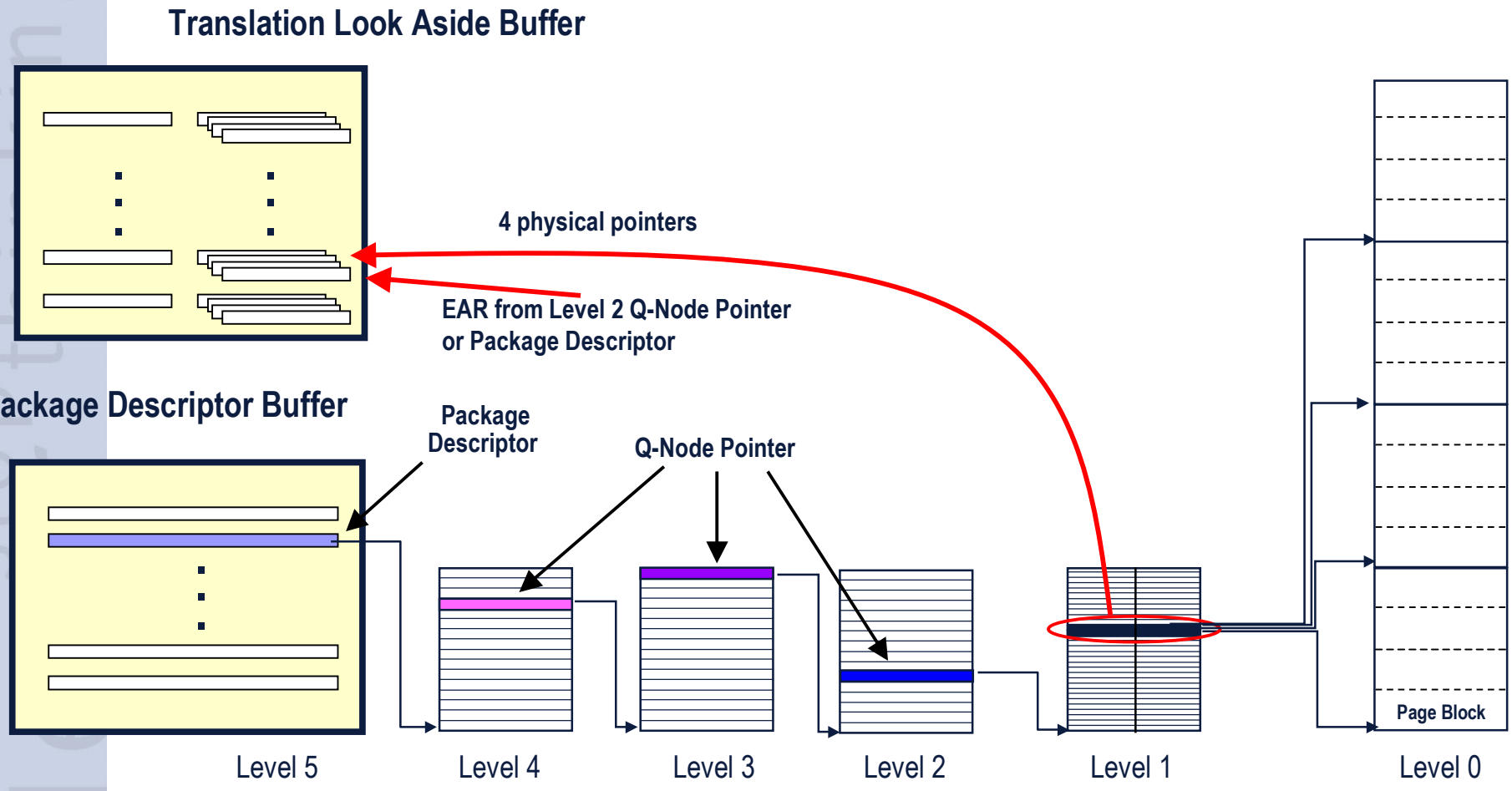
Data Access Modes



			Source Package (package access type)		
			Intrapackage	Interpackage	
				executing package type regular	executing package type SL,HAL,OS
Target Package SL	EAR	code			
	WW	0x8	rw	rw	rw
	WR	0x9	rw	r	r
	RR	0x1	r	r	r
	W	0xD	rw	MPA	MPA
	R	0x5	r	MPA	MPA
	code	0xF	MPA	MPA	MPA
	other	-	MPA	MPA	MPA
Target Package not SL	WW	0x8	rw	rw	rw
	WR	0x9	rw	r	rw
	RR	0x1	r	r	rw
	W	0xD	rw	MPA	rw
	R	0x5	r	MPA	rw
	code	0xF	MPA	MPA	rw
	other	-	MPA	MPA	MPA

Access Rights for Data and Code Access

- ⇨ Effective Access Rights (EAR)
- ⇨ Security Layer Tag Rights (SL)
- ⇨ PORT Instruction



Effective Access Rights, EAR