Johanna Sepúlveda Flórez (martha.sepulveda@univ-ubs.fr)
Guy Gogniat (guy.gogniat@univ-ubs.fr)
Ricardo Pires (rpires@lme.usp.br)
Marius Strum (strum@lme.usp.br)

NoC-BASED DYNAMIC SECURITY IMPLEMENTATION FOR MULTI-APPLICATION SoC

Lab-STICC
UNIVERSITÉ DE BRETAGNE SUD
UNIVERSITY OF SÃO PAULO
2012

Summary

1. INTRODUCTION.
    - Problem.
    - MPSoCs (Multiprocessor System-on-Chip)
    - NoC (Network-on-chip).
2. RELATED WORK.
3. OUR APPROACH.
    1. Architecture.
    2. Functionality.
4. EXPERIMENTAL WORK.
5. RESULTS.
6. CONCLUSIONS AND FUTURE WORKS.

Introduction

Cellphones

Automotive electronics

Aviation

Electronic money

Electronic banking

Media players

Game console

***SECURITY*:** Critical requirement at the electronics systems design.

Introduction

Intellectual property protection

Secure execution of downloaded SW

Non-repudiation

SoC

Secure personal data

Content security

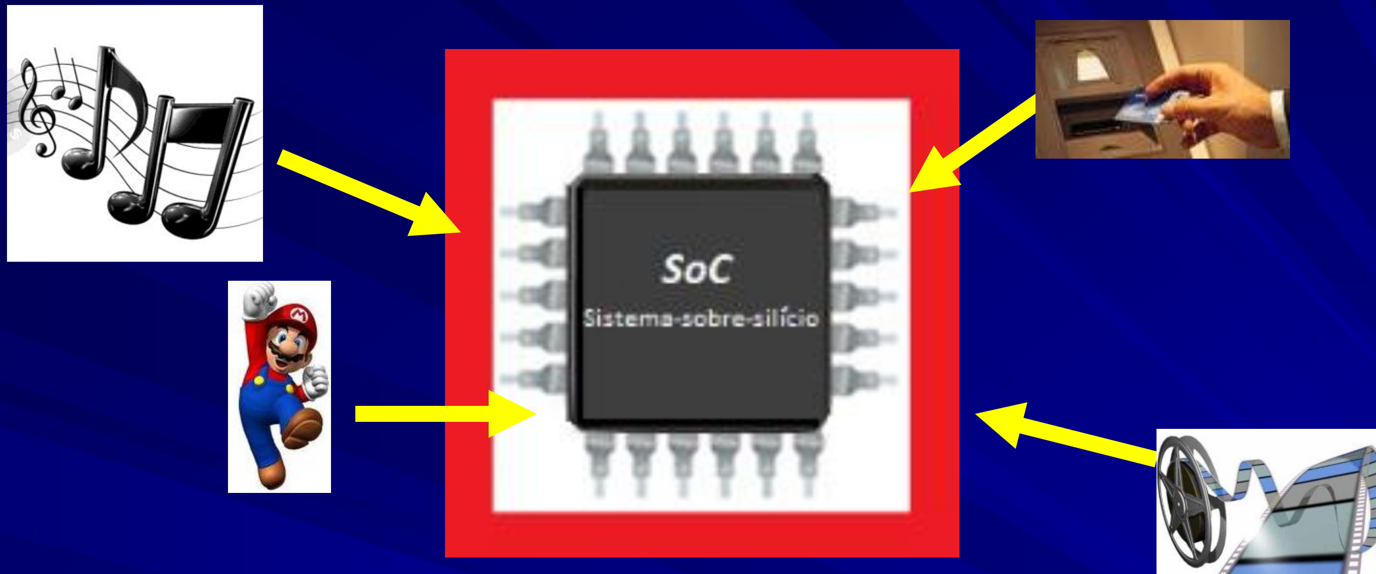
Digital rights management

Fraudulent transactions avoidance

System-on-Chip (SoC) **: Integrated Computing System.**

***SoCs* can be attacked!!**

Introduction



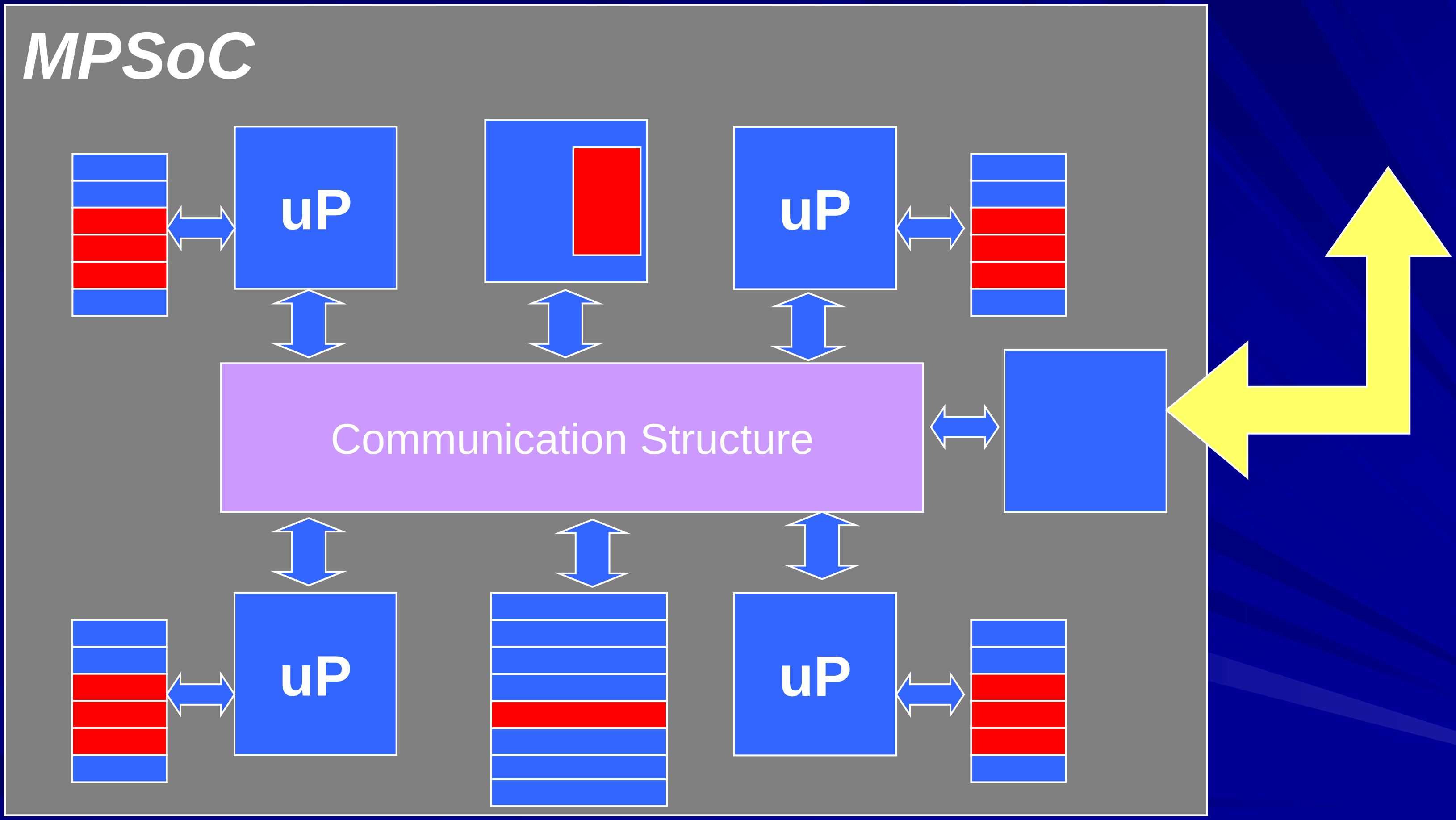
Cost effective:

- * General purpose *SoC*.
- * Integrate different applications on the same chip.

Applications: Communication requirements, security policy and design constraints **(Dynamic security policy)**.

MULTI-APPLICATION SYSTEM

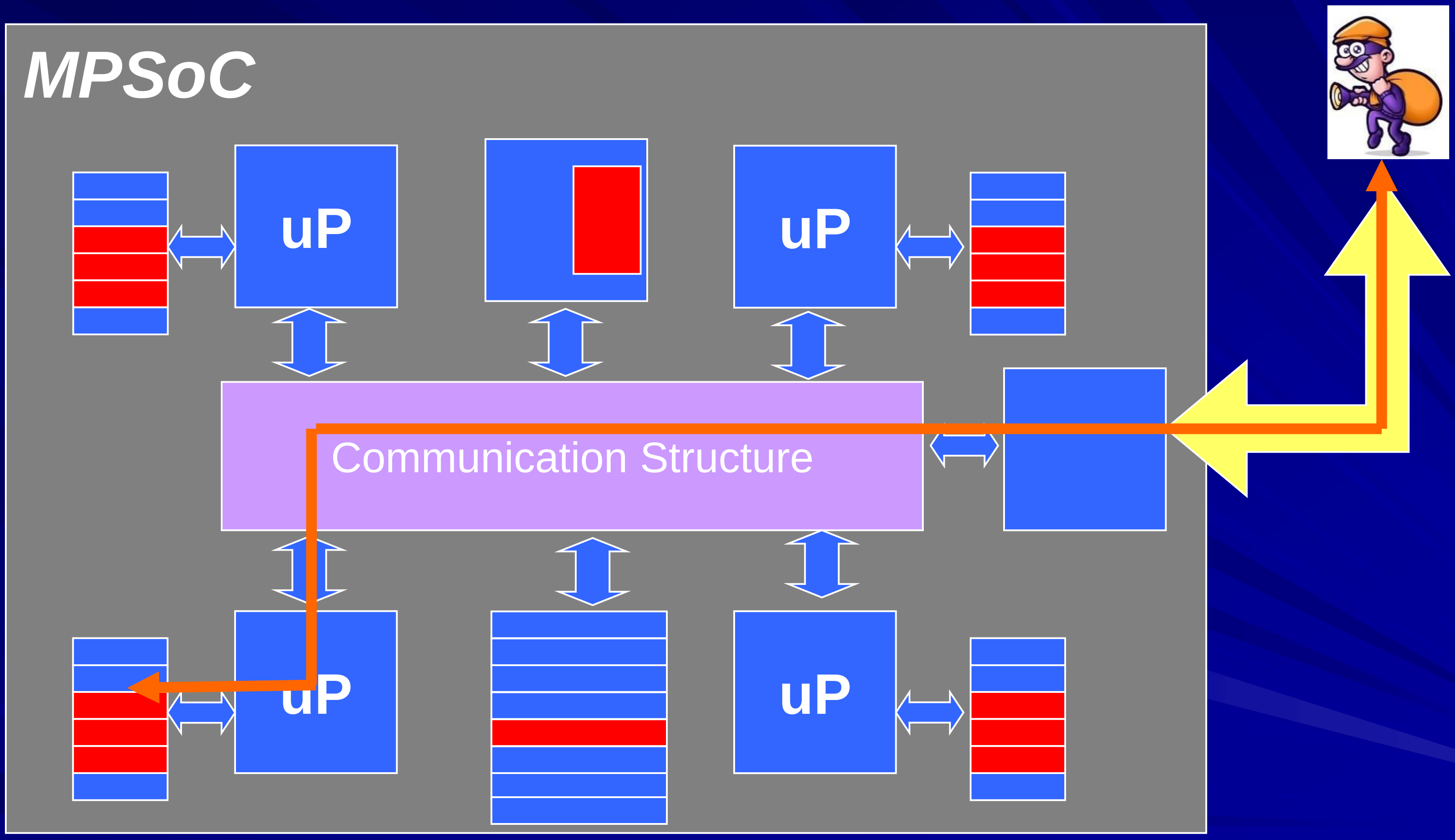
Problem



Software attacks!

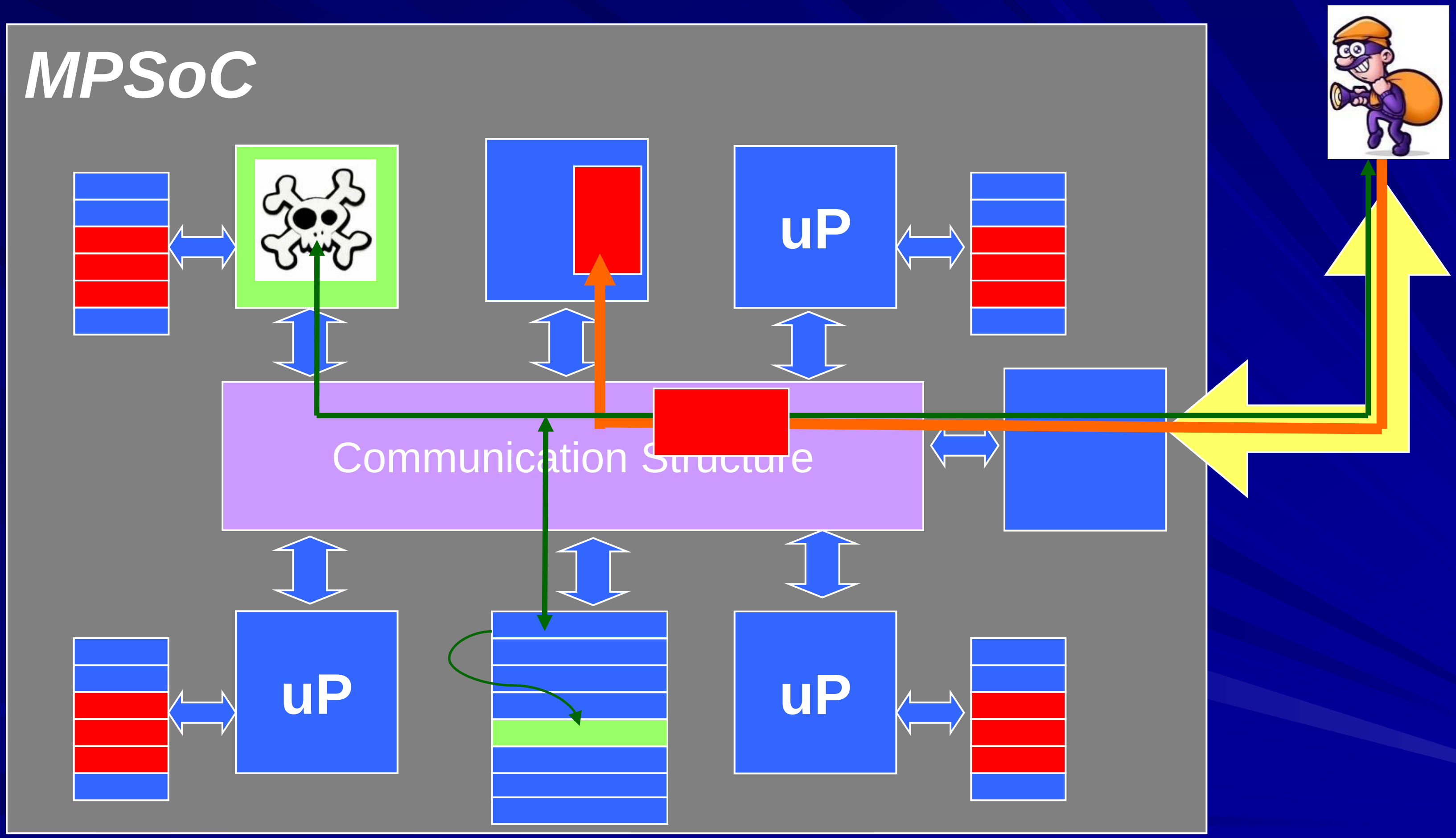
- Security incidents: 80% via software.

Problem



Explore the *SoC* vulnerabilities.

Problem

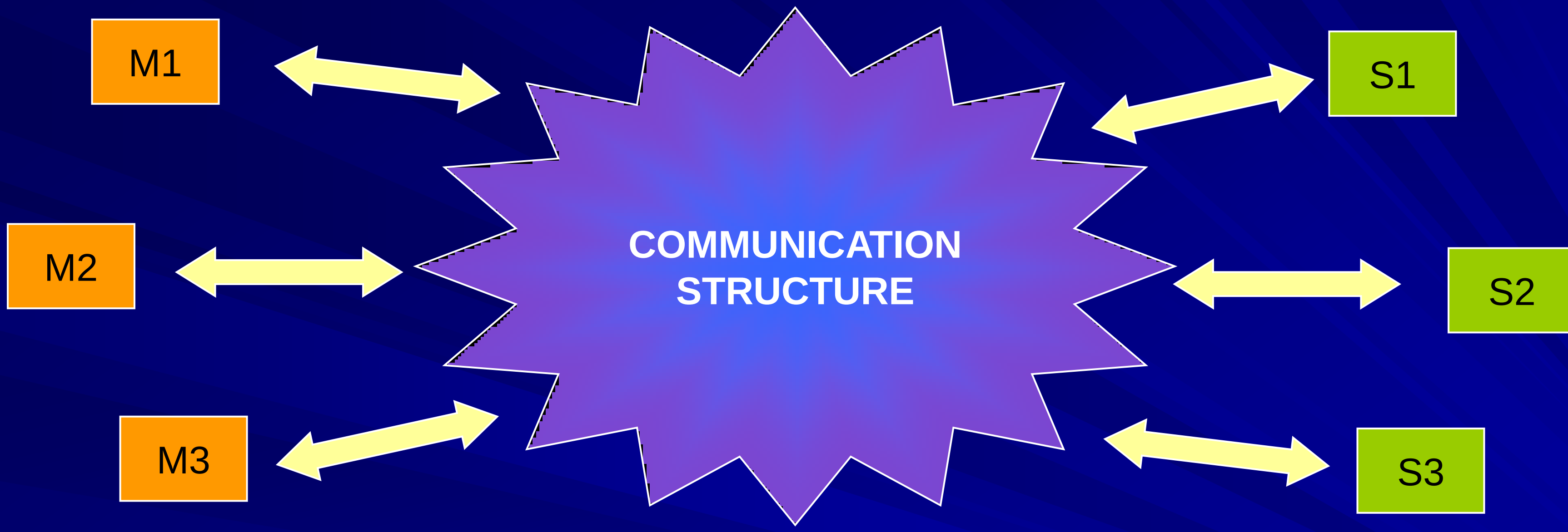


Infection: Takes advantage of the trusty component's rights!!

All software attacks begin with an abnormal communication.

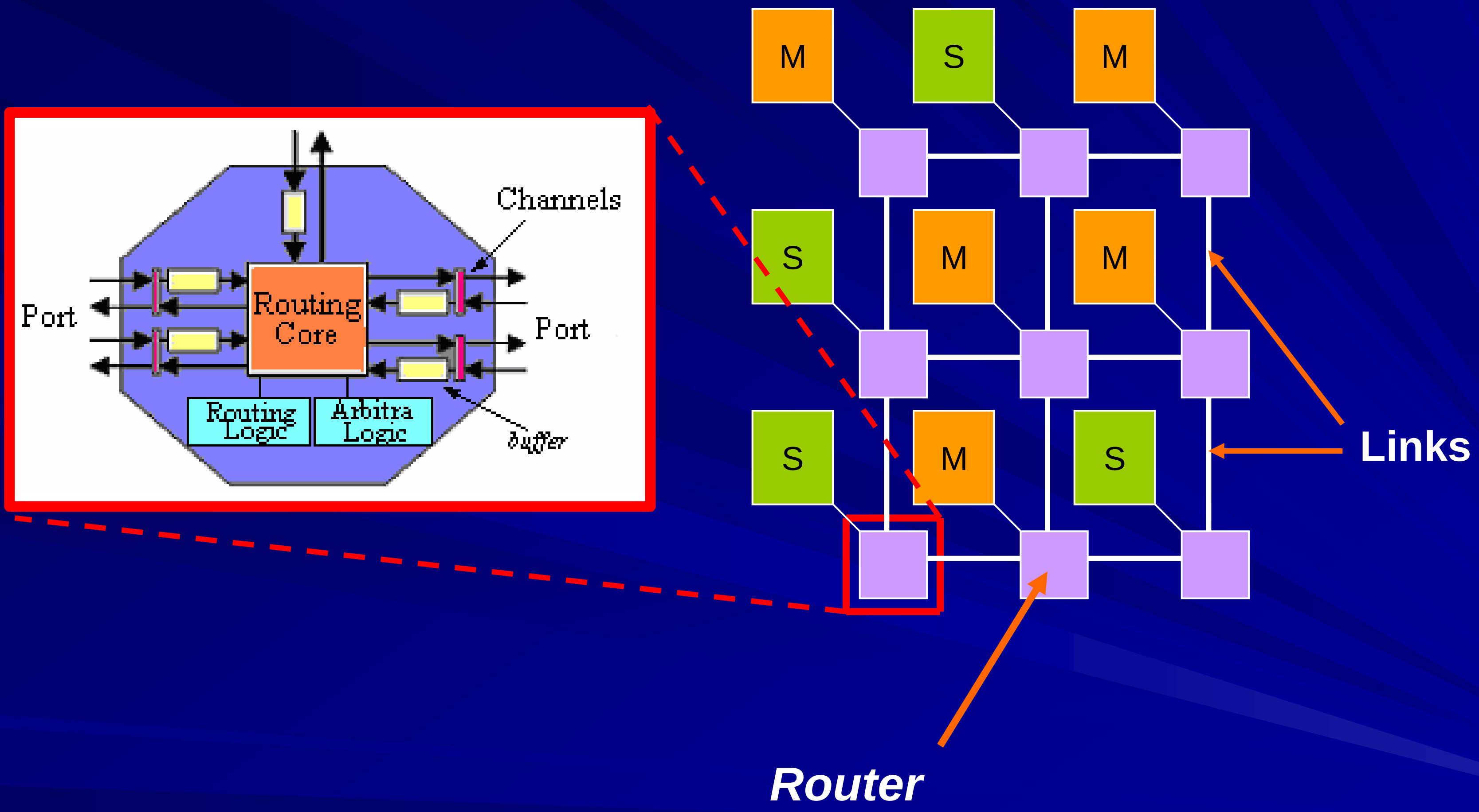
Security at the communication structure

Communication structure



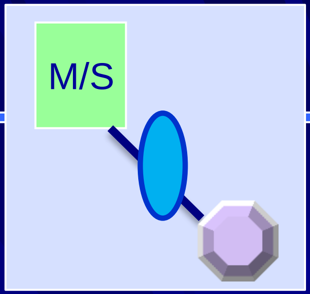
- Monitor information exchange.
- Detect attacks.
- Diagnosis → Trigger recovery mechanisms.

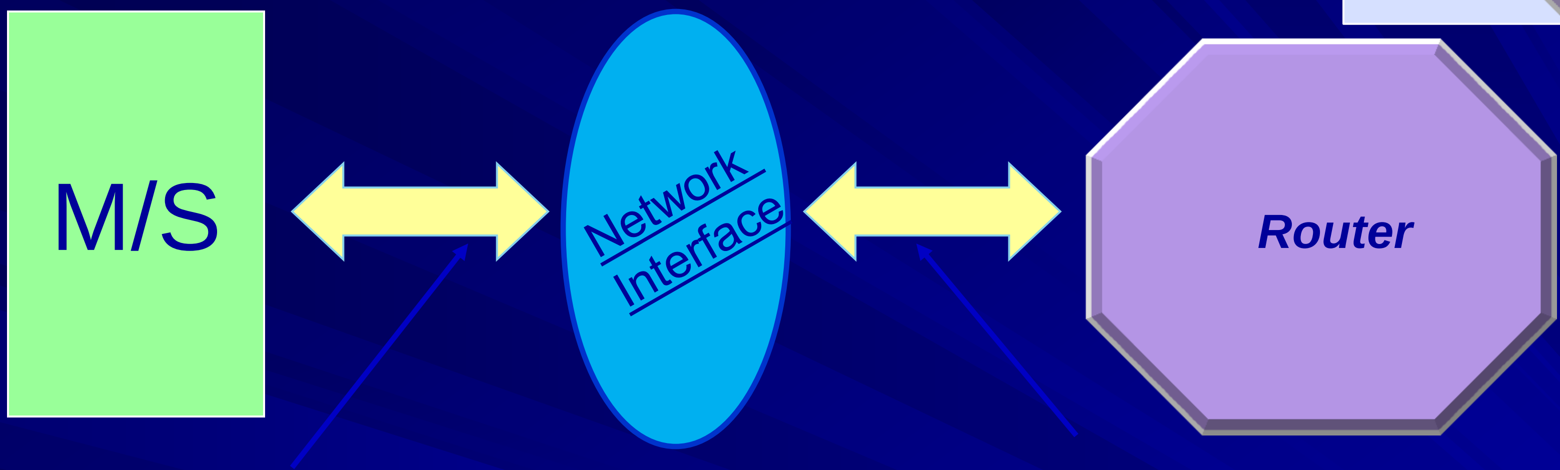
NoC (Network-on-Chip)



Topology: Simple or ***hierarchical***

NoC (Network-on-Chip)

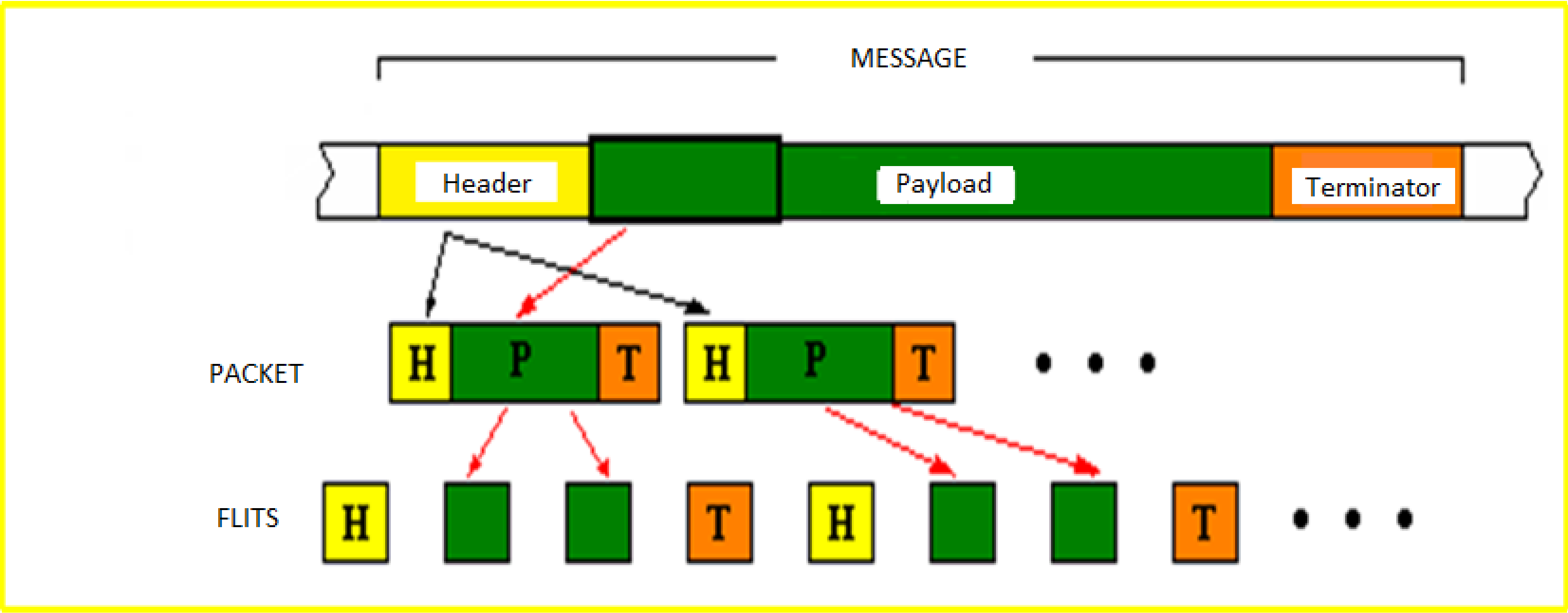


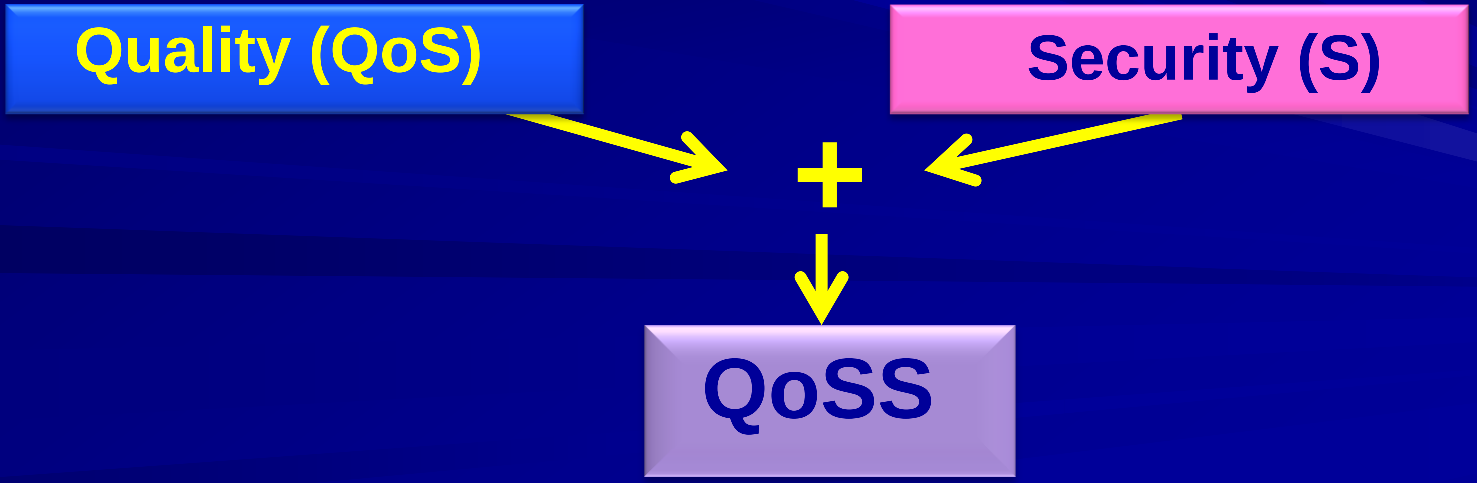


- Transmission
  - Packets building
- Reception
  - Synchronization
  - Separation of routing information

Network protocol

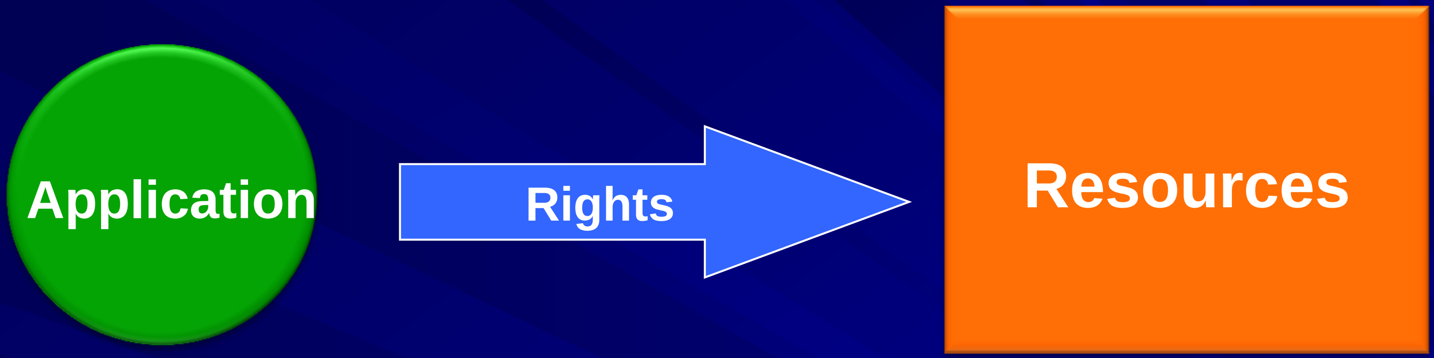
Communication





SECURITY

NoC security – Basic concepts



- ***Security policy:*** Rules the relationship between the application and the resources (static/dynamic).
- ***Safe system:*** Behaves as expected and the vulnerabilities are minimized.
- ***Vulnerability:*** Weakness that may be explored in order to attack a system.
- ***Attack:*** Any **unauthorized** attempt to access or use the resources.

NoC security – Basic concepts

SECURITY SERVICES

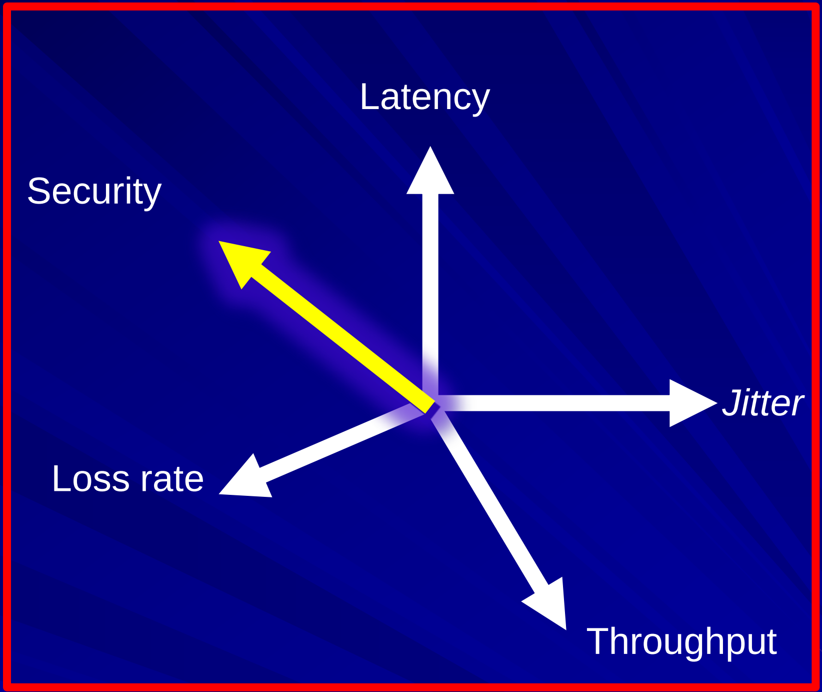
Protect the system resources and mitigate the attacks.

1. **CONFIDENTIALITY: Secrecy of information.**
2. **INTEGRITY: Correctness of the information.**
3. **AUTHENTICATION: Source integrity.**
4. **ACESS CONTROL: Authorized use of the resources.**
5. **AVAILABILITY: Resources can be used.**
6. **NO REPUDIATION: Evidence of communication.**

QoSS (Quality of Security Service)

QoSS = **QoS + Security**

- Security as a *QoS* dimension.
  - Security level.



- **Selection:**
  - Security requirements and resources availability.
  - Operation mode and security/cost trade-off.

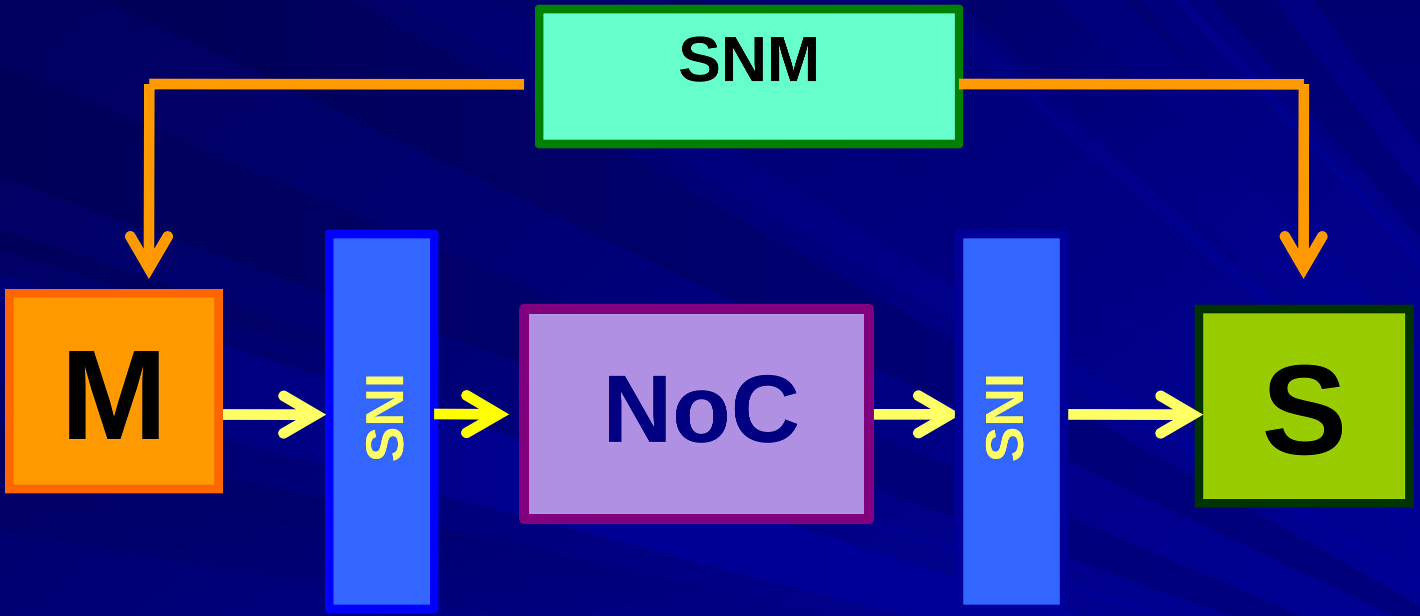
QoSS (Quality of Security Service)

- **Advantages:**
  - Lower protection cost.
  - Enhance the efficiency of the resources utilization.
  - Better system control.
  - Flexibility.
- **Disadvantages:**
  - System complexity.

Previous works

Previous works - Static policy

[EVA05, DIG07]



Security services: Non repudiation, confidentiality.

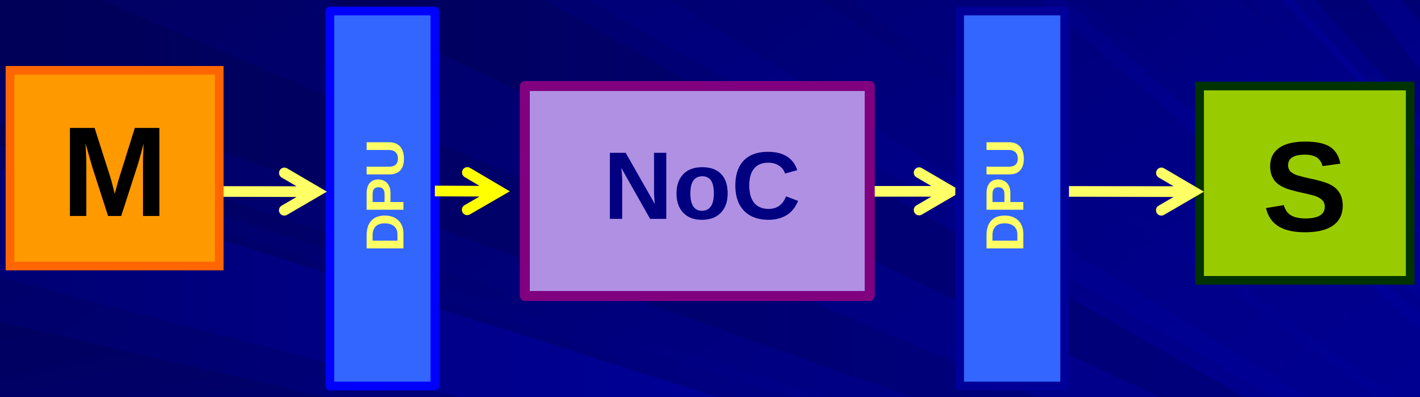
Componentes:

SNI: Secure network interface.

SNM: Secure network manager (monitor).

Previous works - Static policy

[FIO07, FIO08]



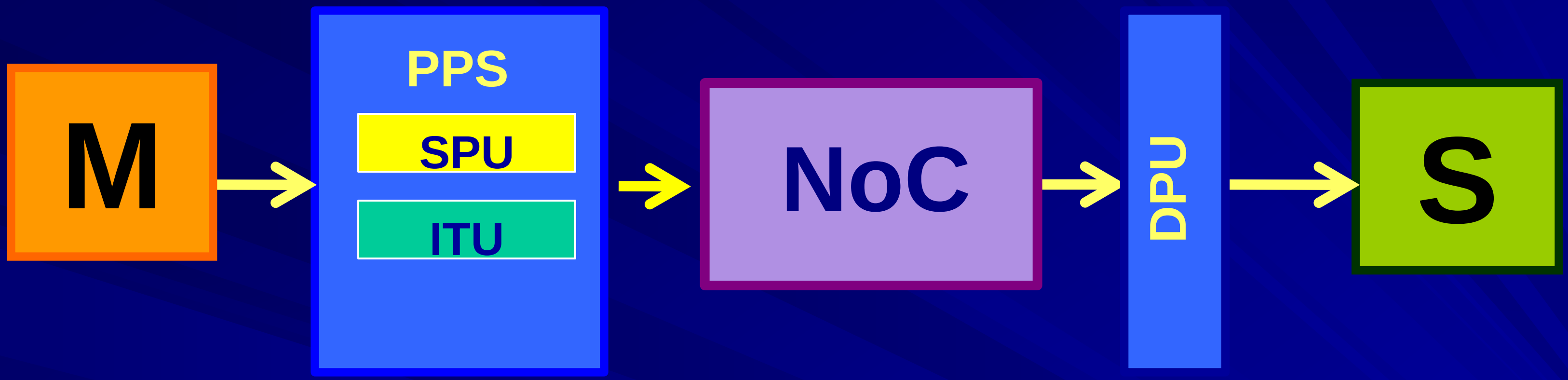
Security service: Access control.

Components:

DPU: Data protection Unit (memory access).

Previous works - Static policy

[LUK10]



Security service: Access control, availability.

Components:

PPS: Processor protection Unit.

SPU: Stack protection unit.

ITU: Instruction trace unit.

DPU: Data protection Unit (memory access).

Previous works - Static policy

Advantage

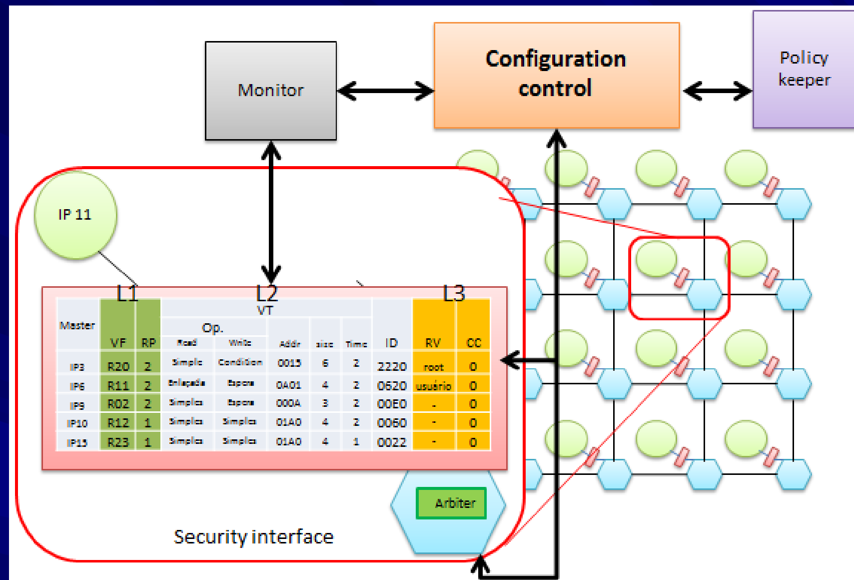
Show that *NoC* can be a useful structure to handle different security services.

Limitations

1. Support a **static** security policy.
2. Support a **single level** of security.
3. Lack of system performance evaluation.
4. Lack of security efficacy evaluation.

Previous works - Dynamic policy

[SEP11]



- Large link overhead.
- Single level (No QoSS).

Security service: Access control and authentication.

Components:

Configuration control
Policy keeper
Monitor

OUR WORK

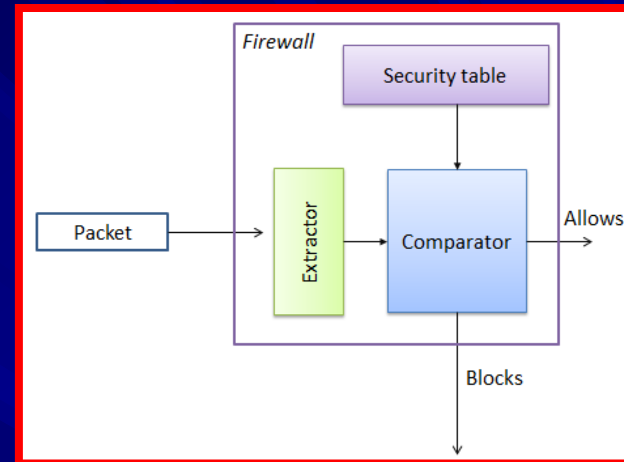
INTEGRATION OF QoSS INTO A HIERARCHIC NoC FOR MPSOC DYNAMIC PROTECTION

To provide security for MPSoCs and guarantee that performance and security requirements are met.

Access control implementation

FIREWALL:

- Allows or blocks a transaction.
- According to a security policy.
- Implemented at the network interface.
  - At the packet arrival.
  - Before the packet injection to the NoC
- Security levels.
- Control information: source, type, role.



Access control			
	SV	TV	RV
Level 0			
Level 1	X		
Level 2	X	X	
Level 3	X	X	X

VF: Source verification.
VT: Type verification.
VP: Role verification.

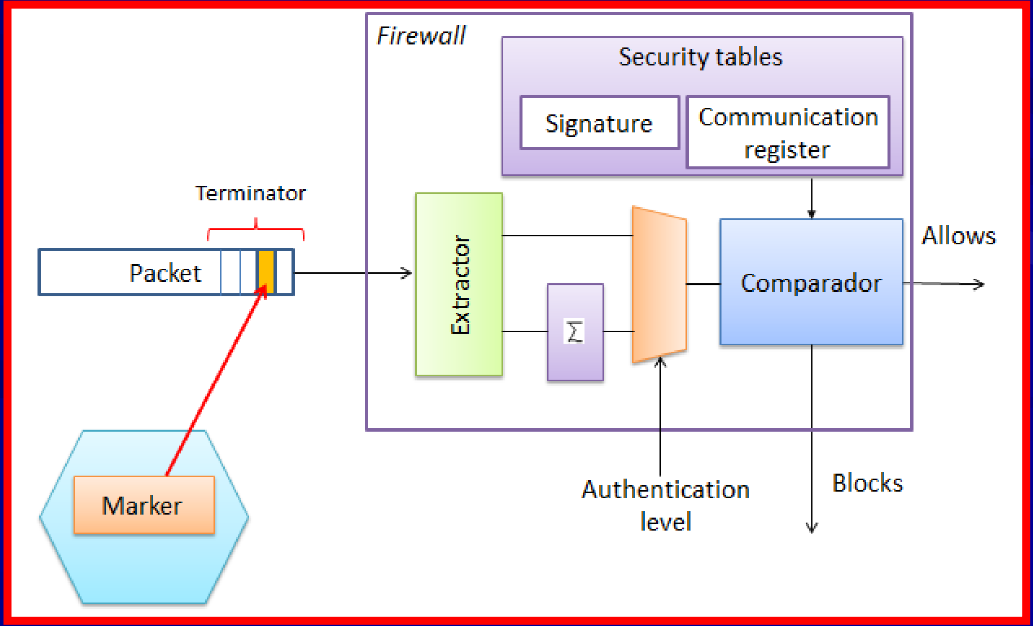
Authentication implementation

- Implementation: at the network interface.
- 4 security levels.
- Uses the NoC characteristics.

Authentication			
	NR	RP	CC
Level 0			
Level 1	X		
Level 2	X	X	
Level 3	X	X	X

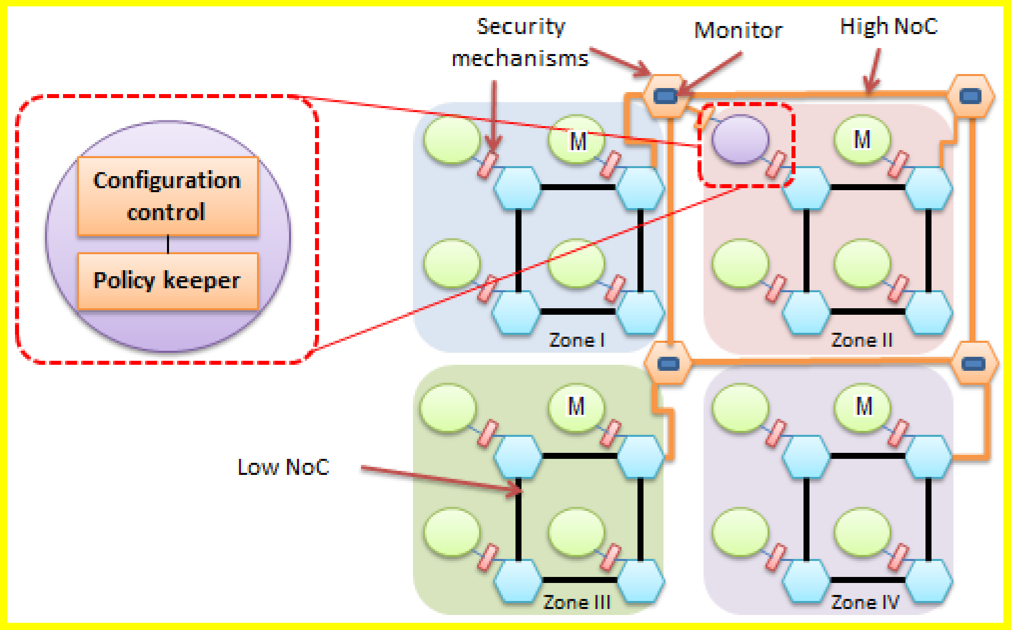
NR: Number of routers.
RP: Routers through the path.
CC: Communication code.

FIREWALL:

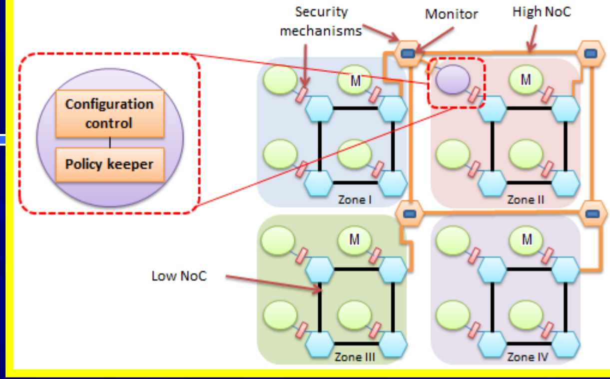


Our approach

- Layered security implementation (Hierarchic NoC).
- MPSoC organized as independent clusters (IP **security** and **communication** characteristics): **Security zones**.
- Distributes the security policy management (*global and local*) by partitioning the NoC topology (*High-NoC*, *Low-NoC*).



Our approach



Global security:

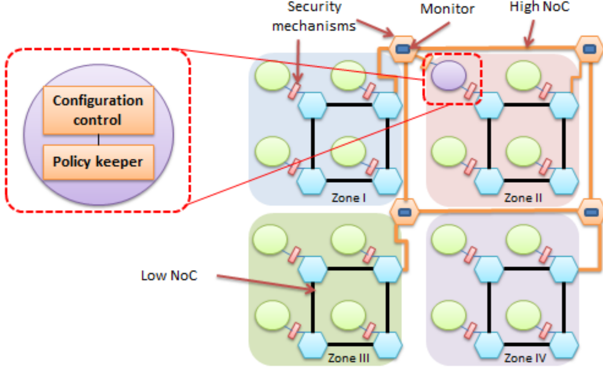
* Configuration control.
* Policy keeper.
* Monitor

Local security:

* Security mechanisms.
* Local configuration control (Manager)

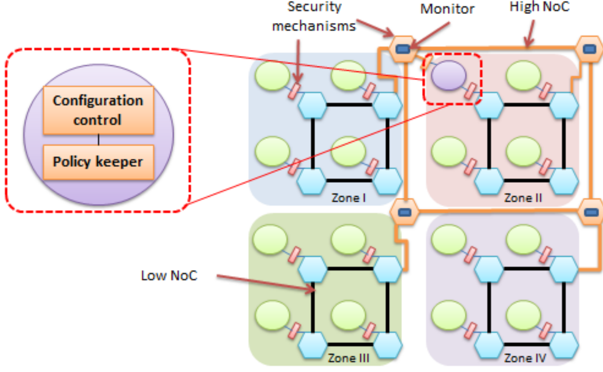
- ***QoSS needs.***

Our approach



- Security policy changes:
- The global configuration control (High-NoC) notify the manager of the corresponding security zone.
- The *Manager* of the security zone (Low-NoC) modifies the security tables of the firewalls.
- The reconfiguration doesn't take place until the arrival of the packets that are inside the network and whose destination is any of those interfaces that are going to change.

Study case



- 3 applications of the MiBench benchmark
  - Automotive.
  - Consumer electronics.
  - Telecommunication.
- 3 different security policies.
- All possible combinations.
- Predefined mapping cases.

Auto./Industrial	Consumer	Telecomm.
basicmath	jpeg	CRC32
bitcount	lame	FFT
qsort	mad	IFFT
susan (edges)	tiff2bw	ADPCM enc.
susan (corners)	tiff2rgba	ADPCM dec.
susan (smoothing)	tiffdither	GSM enc.
	tiffmedian	GSM dec.
	typeset	

Functions of the 3 applications

Implementation

Application	Function	Authentication	Access control	Performance
Automotive	basicmath	Level 0	Level 2	
	bitcount	Level 0	Level 0	
	qsort	Level 3	Level 3	
	susan (edges)	Level 2	Level 2	
	susan (corners)	Level 2	Level 2	
	susan (smoothing)	Level 2	Level 2	
Consumer electronics	jpeg	Level 2	Level 2	Latency
	lame	Level 1	Level 1	
	mad	Level 0	Level 0	
	tiff2bw	Level 0	Level 0	
	tiff2rgba	Level 0	Level 0	
	tiffdither	Level 0	Level 0	
	tiffmedian	Level 0	Level 0	
	typeset	Level 0	Level 0	
Telecommunications	CRC32	Level 2	Level 2	
	FFT	Level 1	Level 1	
	IFFT	Level 1	Level 1	
	ADPCM enc	Level 0	Level 0	
	ADPCM dec	Level 0	Level 0	
	GSM enc	Level 3	Level 3	Latency
	GSM dec	Level 3	Level 3	Latency

Automotive — Sec. policy

Consumer electronics — Sec. policy

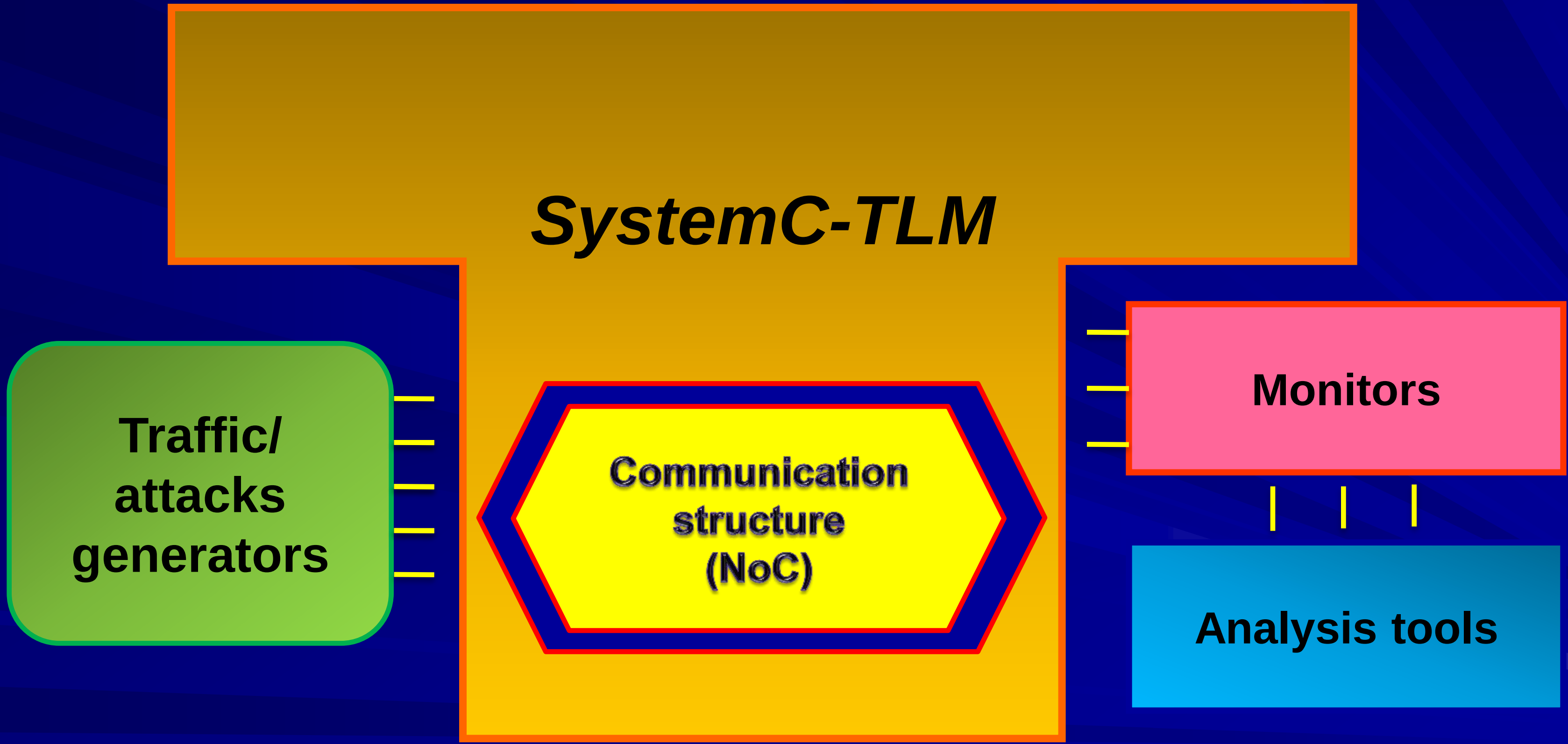
Telecomm. — Sec. policy

Implementation

NoC parameters

Layer	Configuration parameter	Low NoC	High NoC
Application	Service	QoS, security	QoS, security
Presentation	Interface type	OCP	OCP
Session	Synchronization	Synchronous	Synchronous
Transport	Switching technique	Packet	Packet
	Interface buffer	2 flits	4 flits
	Flow control	Virtual channel	Single channel
	Network type	Homogeneous	Homogeneous
Network	Mapping	Static	Static
	Size	2x2	2x2
	Topology	Mesh	Mesh
	Routing strategy	XY	XY
	Ports per router	3-5 (according to router)	
	Routing granularity	Packet	Packet
Link	Arbitration	Round-Robin	TDMA
	Link wide	16 bits	16 bits
	Buffers per router	3-5 (according to router)	3-5 (according to router)
	Buffer size	4 flits	6 flits
	Transaction type	Split transaction	Split transaction
	Information codification	Nothing	Nothing
	Multiplexing technique	Nothing	Nothing

Evaluation


SystemC-TLM
Traffic/
attacks
generators
Communication
structure
(NoC)
Monitors
Analysis tools

Simulation

Simulation Conditions

- *5 flits Payload.*
- *600.000 simulated cycles.*
- *Poisson traffic, LRD (Long Range Dependence).*
- *3 Types of attacks:*
  - **Extraction**.
  - **Modification.**
  - **Denial-of-Service (DoS)**.

30% are critical data

Results

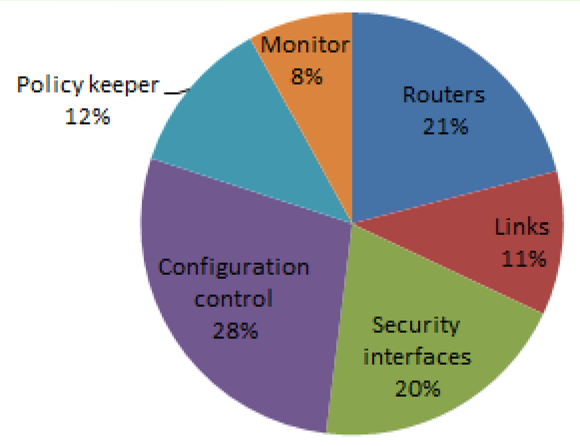
Security efficacy

Attack scenario	Authentication efficacy	Access efficacy
Send critical information	87%	100%
Read critical information	83%	100%
Write not authorized areas	100%	100%
Nonexistent target	100%	100%
Repeated information	89%	100%
Communication target=source	100%	100%

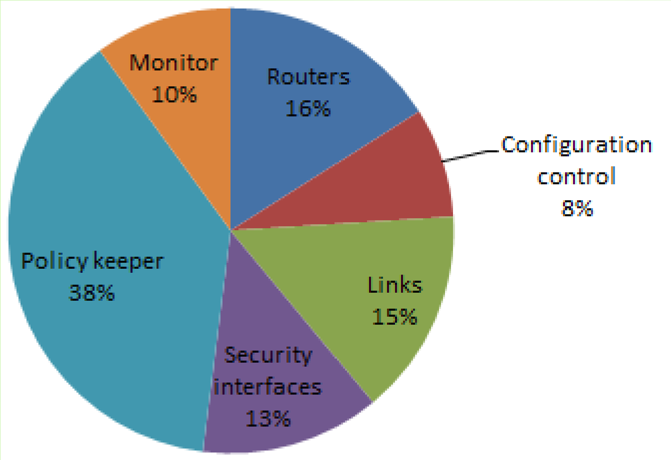
Security policy should change in order to achieve 100%.

Security efficiency

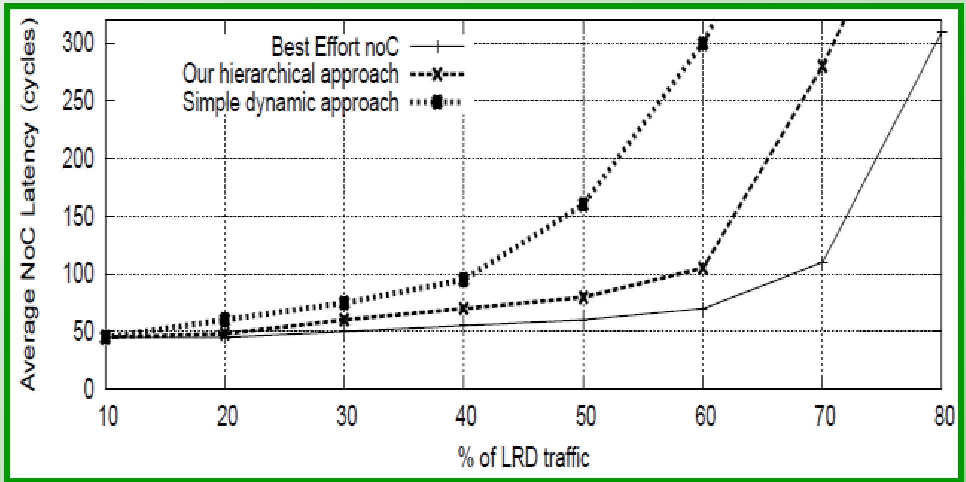
Latency



Power



Results



- The hierarchical approach **always** performs better than the simple dynamic.
- *Layered* approach:
  - Doesn't interrupt other security zones.

Performance penality

Parameter	Dynamical approach	Our hierarchical approach
Latency increment	4.1%	3.8%
power increment	19.6%	7.6%
area increment	26.7%	5.2%

Conclusions and future work

- We proposed a layered dynamic NoC-based security implementation for MPSoCs (security zones).
- Our approach provides an effective way to handle security policy changes and improves the overall system performance.
- We adopt the QoSS concept that allows the designer to customize the MPSoC protection in order to satisfy both, security and performance requirements.
- Results show that the inclusion of security issues in the hierarchic NoC performs better that the simple dynamical NoC architecture.

Conclusions and future work

- As a future work, we will study different techniques that allow an improvement in the implementation of the proposed security mechanisms.

- We will explore different security services (confidentiality and integrity).

Thanks!!!