Implementation of Quality-of-Security-Service in communication structure for 3D-MPSoCS Protection

M. Johanna Sepúlveda Guy Gogniat, Marius Strum
jsepulveda@lme.usp.br

LAB-STICC, UNIVERSITÉ BRETAGNE SUD, FRANCE
GSEIS, UNIVERSITY OF SÃO PAULO, BRAZIL
2013

SUMMARY

1. Introduction
2. 3D-MPSoCs
3. HoCs: 3D Communication structure
4. Our Work

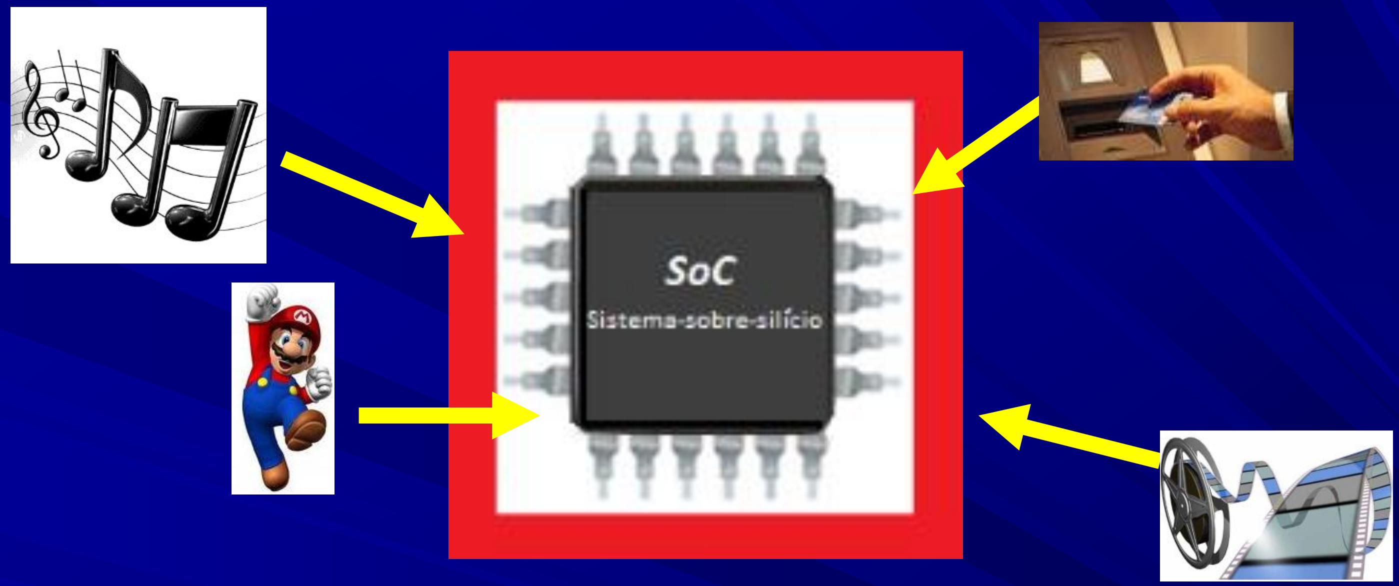
   Goal 1: Mechanisms to support QoSS.

   Goal 2: Evaluation of HoC performance.
5. Results
6. Conclusions

MOTIVATION

- To integrate more functionality into smaller devices.
- To increase performance, reduce costs.

MOTIVATION



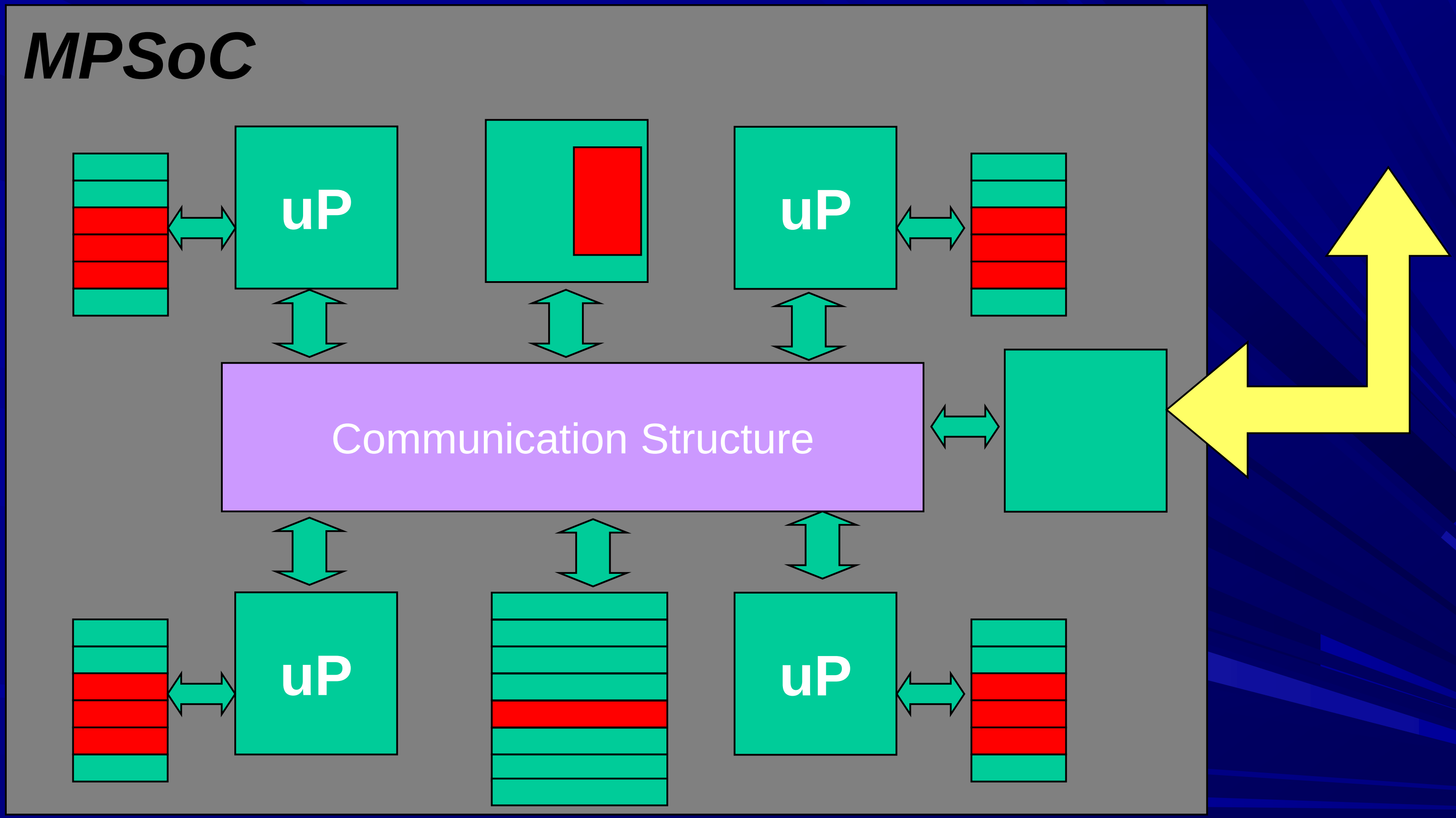
Cost effective:

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

Applications: Communication requirements and design constraints.

MULTI-APPLICATION SYSTEM

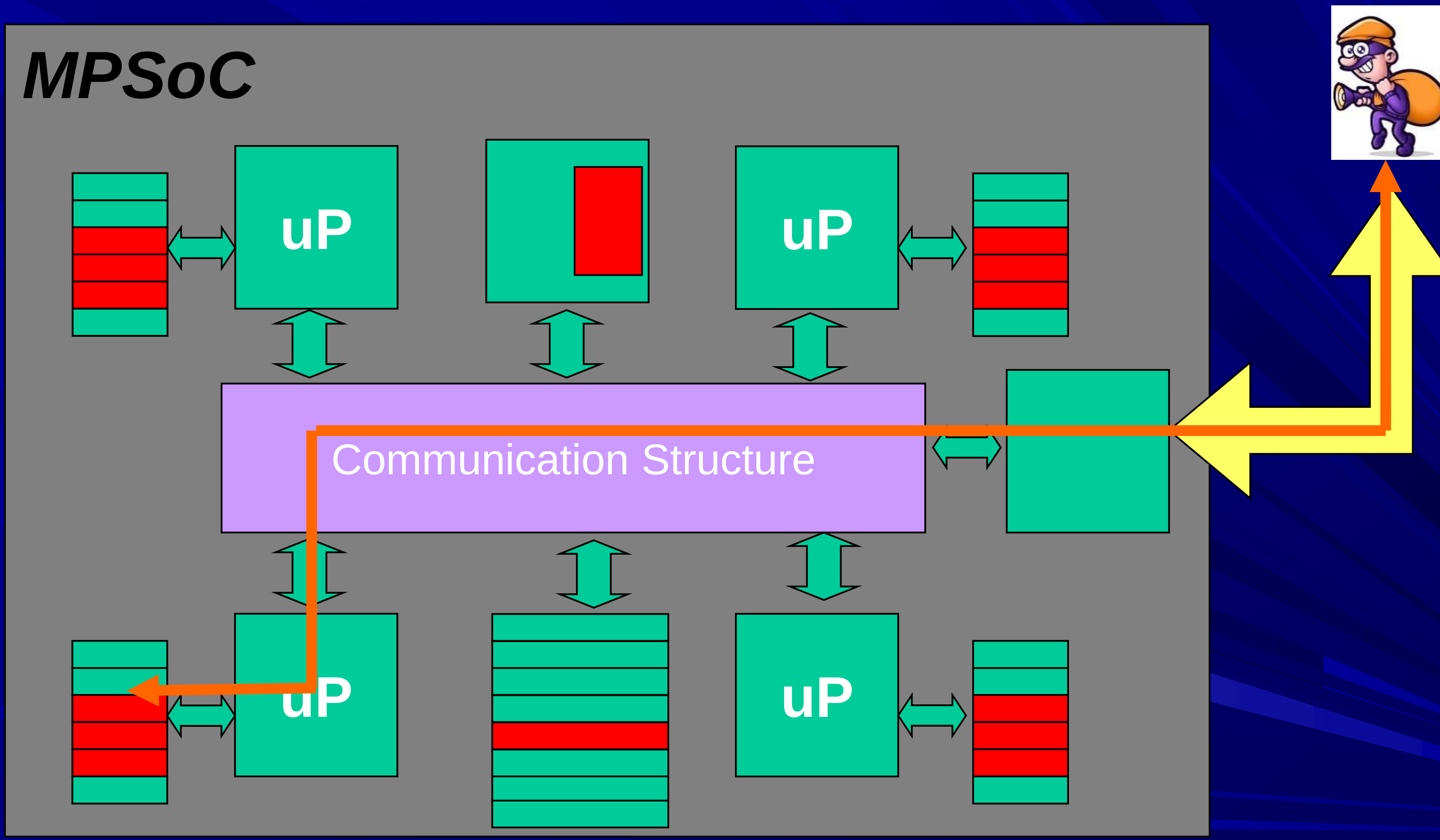
Problem



Software attacks!

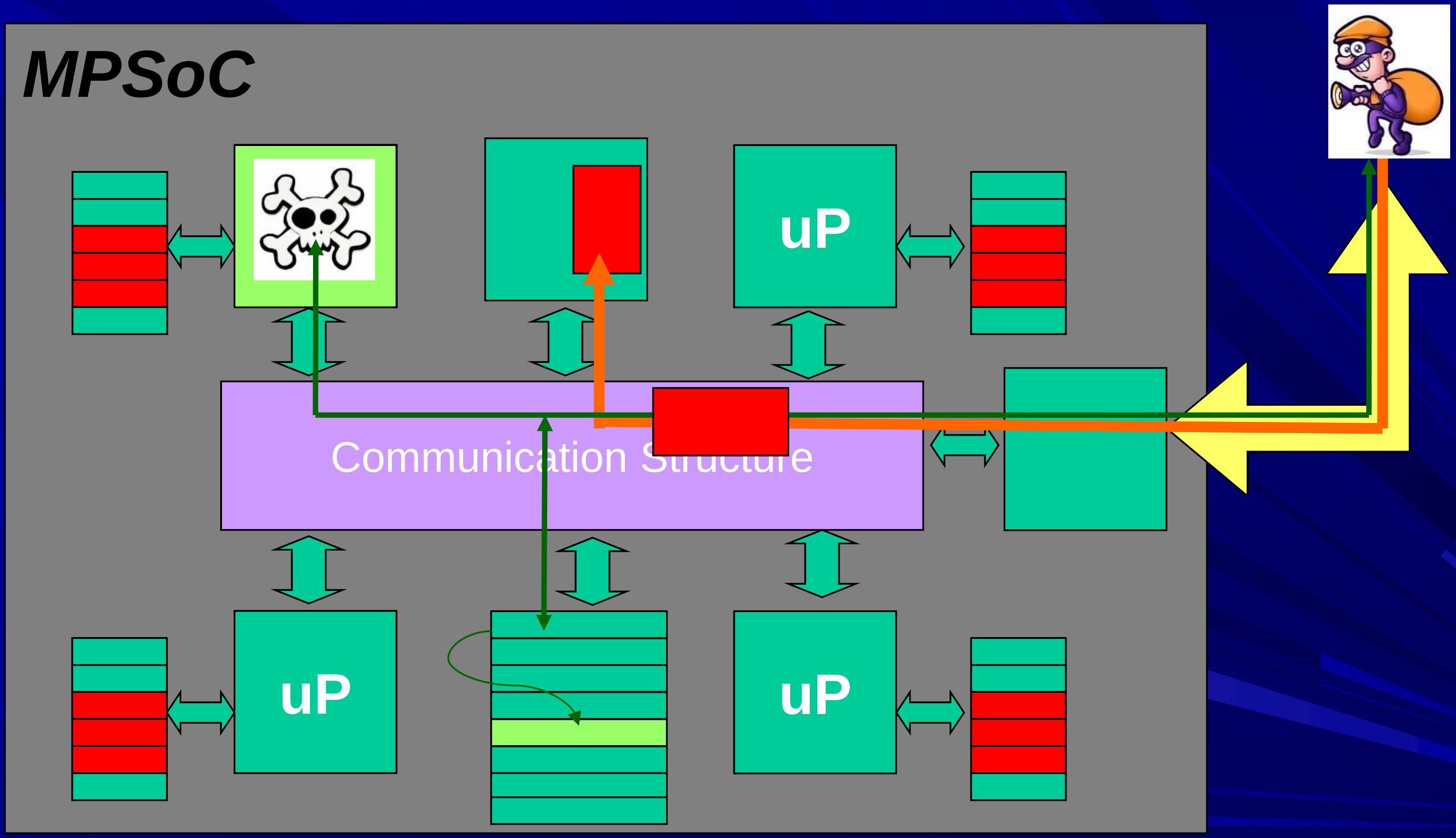
- Security incidents: 80% via **software**.

Problem



Explore the *SoC* vulnerabilities.

Problem



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

3D-MPSoCs

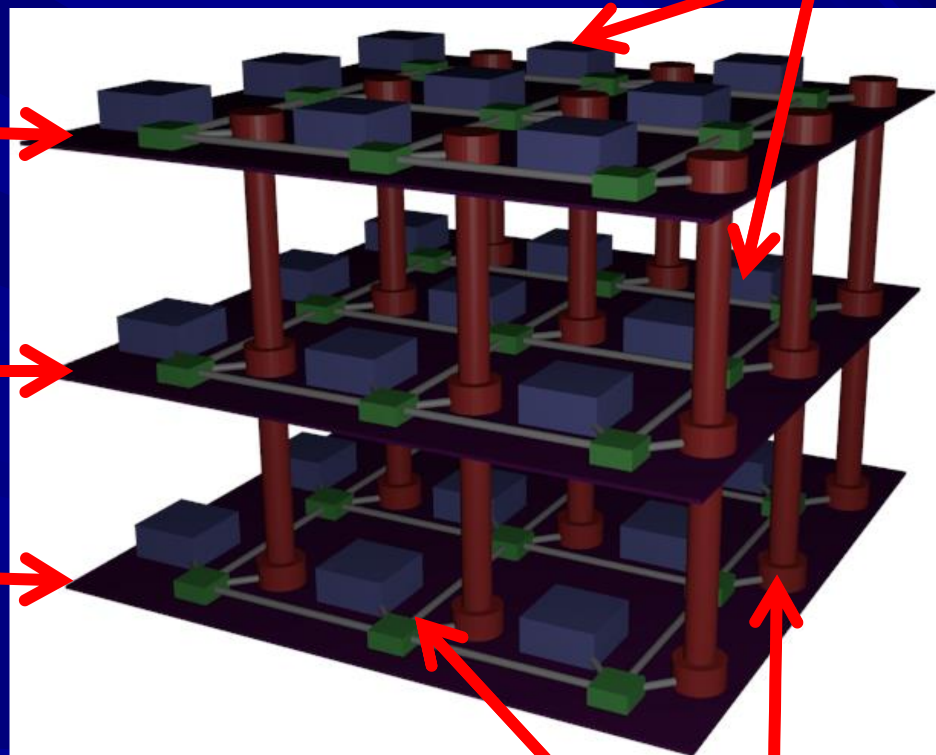
3D-MPSoC

Computation structure

Layer 3

Layer 2

Layer 1

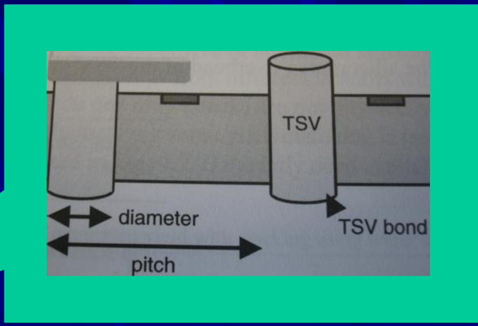


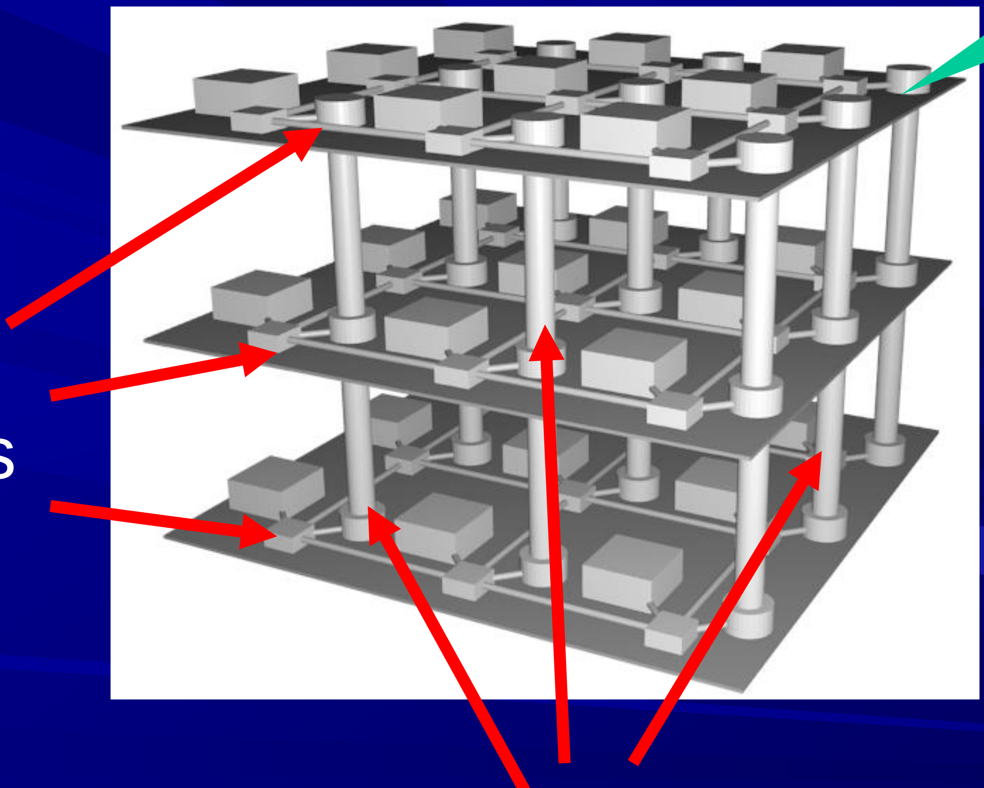
Communication structure

Notation: L(S1)/(S2/n)
3(3x3)/(9/32)

HoCs: 3D-MPSoC Communication Structure

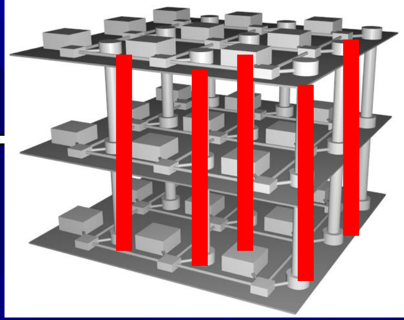
HoCs: Hybrid-On-Chip CS



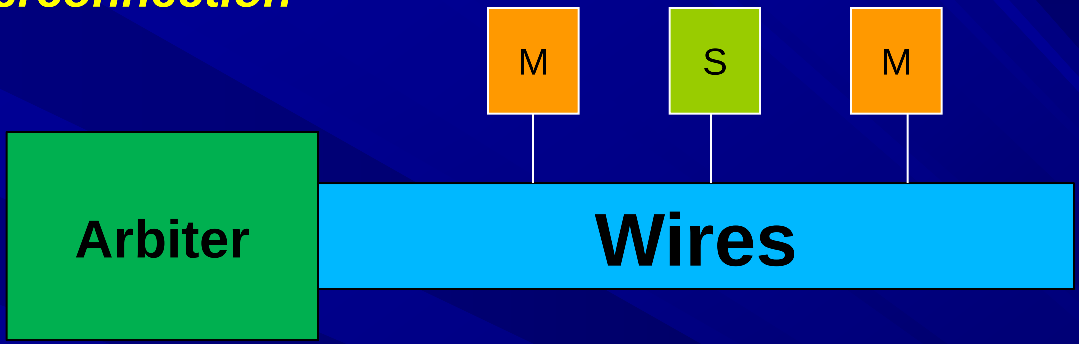


- Short connections.
- Low capacity.
- High frequency.
- Defects.
- Area consumers.

HoCs: Bus

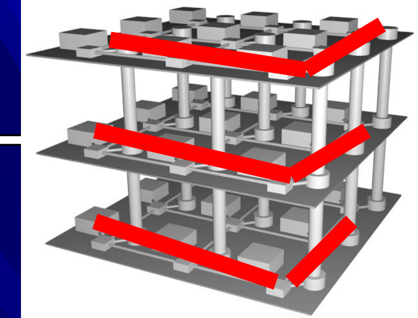


Vertical interconnection

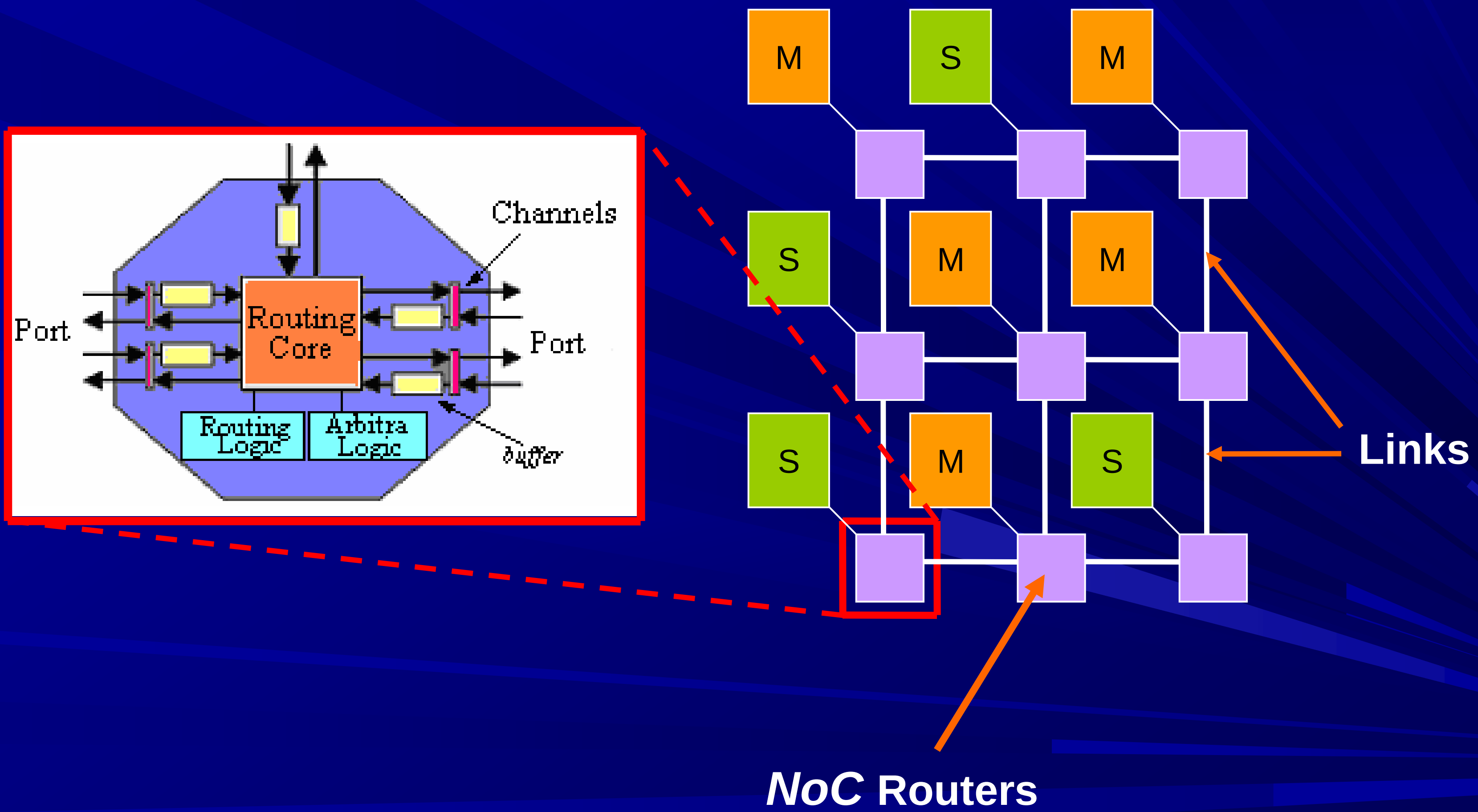


- Low cost CS with predictable latency.
- Not scalable.
- Number of interlayer links (performance/cost-reliability)
  - Higher: Improve performance of the system.
  - Lower: Prone to defects.

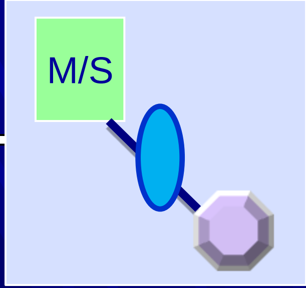
HoCs: NoCs

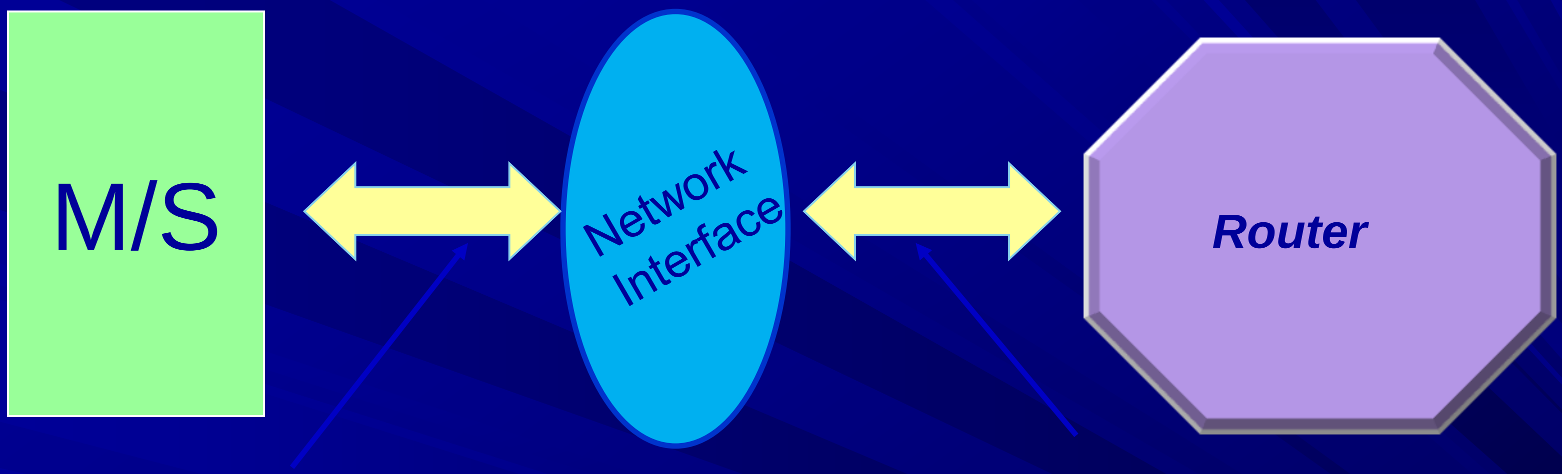


Horizontal interconnection



HoCs: NoCs



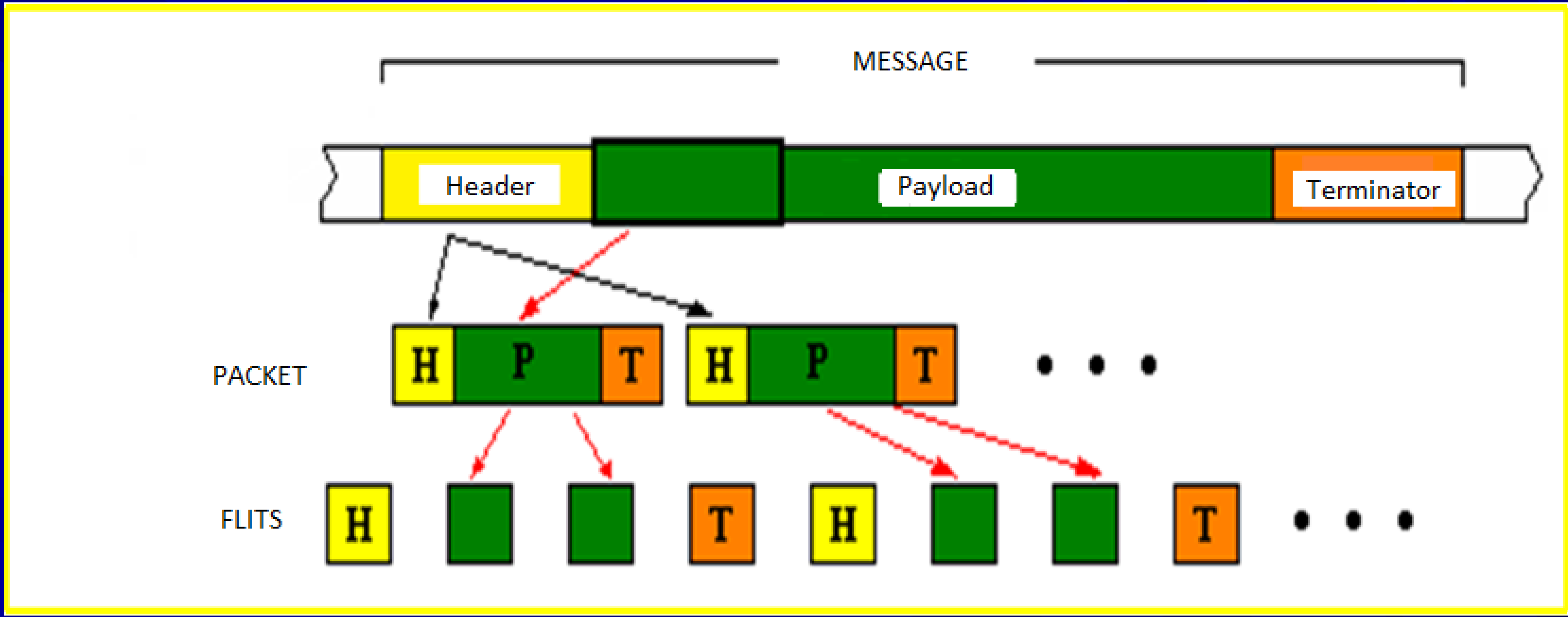


Network Protocol

Source
* Accesses routing tables.
* Assembles packets.
* Splits into flits.

Destination
* Synchronizes.
* Drops routing information.

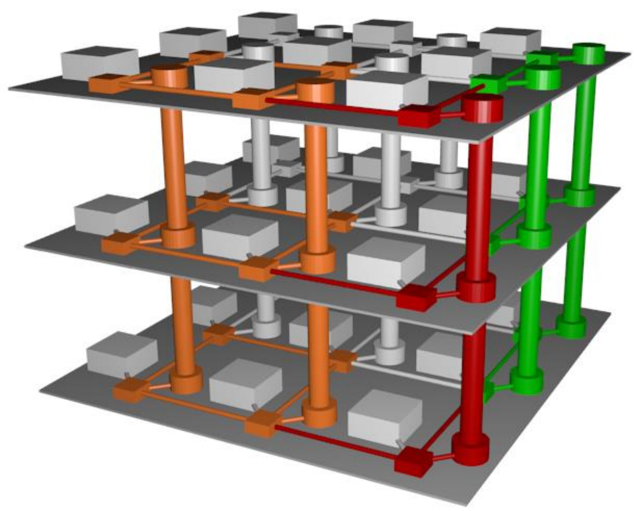
Communication



Quality (QoS)

Security (S)

QoSS (QoS)

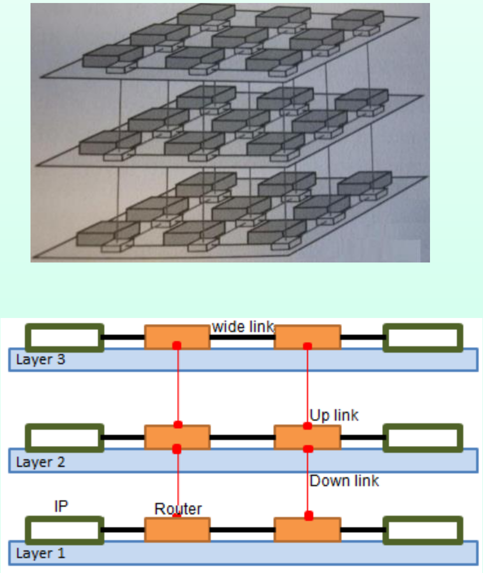


Challenges

1. Efficiency

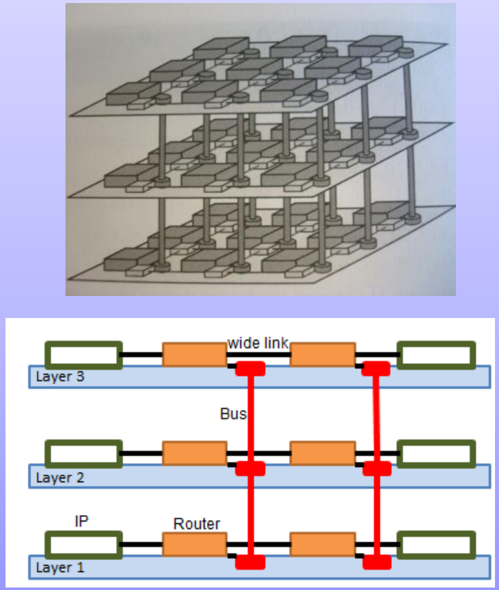
- CS is the bottleneck of the 3D-MPSoC.
- Several works adress the design of 3D-CS.

Single 3D



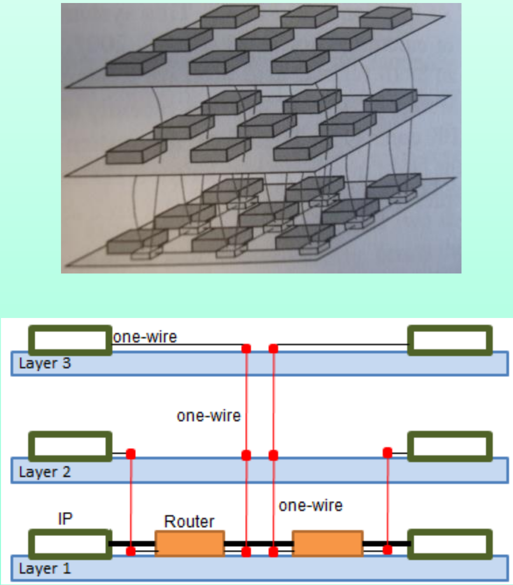
[HEA10]

Stacked



[SHE10]

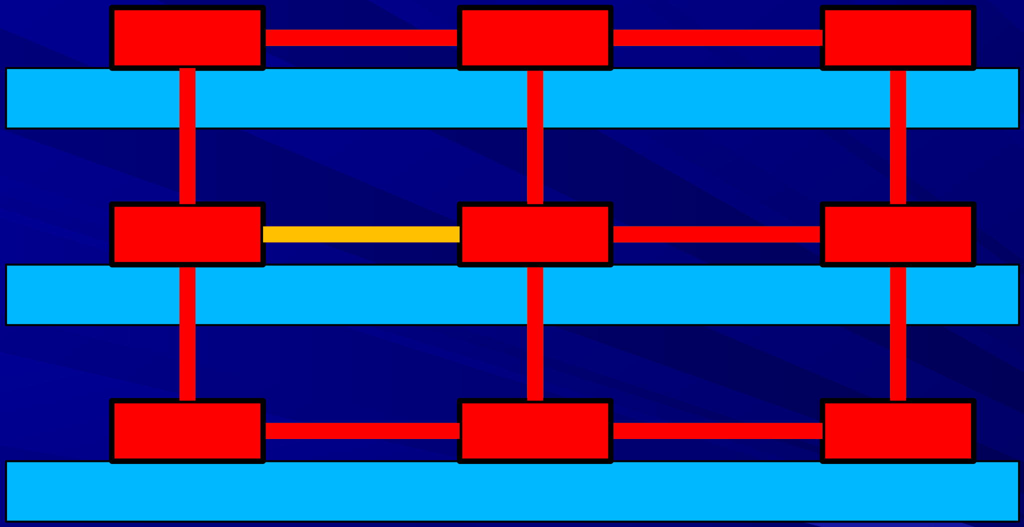
Ciliated



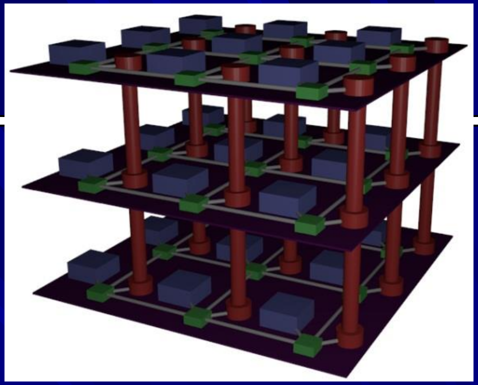
[STA11]

BEST EFFORT ARCHITECTURES!
WITHOUT SECURITY

2. Security



3D-MPSoC characteristics



- Multi-application
  - Different
    - ***Functional/Communication requirements***.
    - ***Security requirements*** (multi security-policies).
- Dynamicity
  - Applications may change (***dynamic security requirements***).
  - New applications may have
    - Tighter communication requirements.
    - Stronger/weaker security requirements.
- Heterogeneity
  - Components with different performance.
  - From different providers (are they trusty?).
- Obserbability
  - Track of critical information (i.e. state of IPs for tasks migration).

Dynamic security requirements

•The security policy of the 3D-SoC can change as a consequence of three factors:

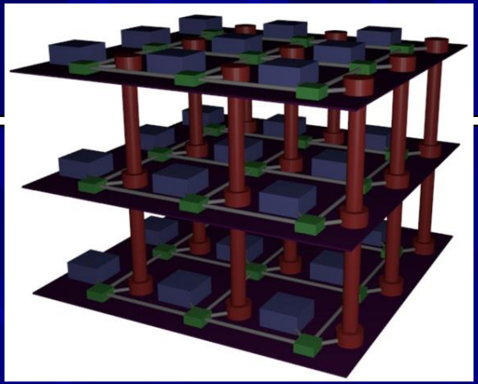
• ***New application*** is mapped on the 3D-SoC.

• ***Current application is reallocated*** on the 3D-SoC (i.e. Task migration).

•***New 3D-SoC operation scenario***.

Islands: IPs or clusters of IPs.

3D-HoC services



- Just an extension of 2D?

NO

- 3D presents new challenges
  - All get worst: multi-application, dynamicity, heterogeneity.
  - Increase of faults (TSVs and thermal effects).

- 3D presents new opportunities:
  - Promote design strategies (prohibitive in performance at 2D-SoC)
    - Huge amount of task migration.
    - Layers specialization.
    - Cluster-style design (clusters linked through a 3D-HoC).
  - Huge set of configuration parameters
    - Computation structure
    - Communication structure

Oportunities

Security Opportunities

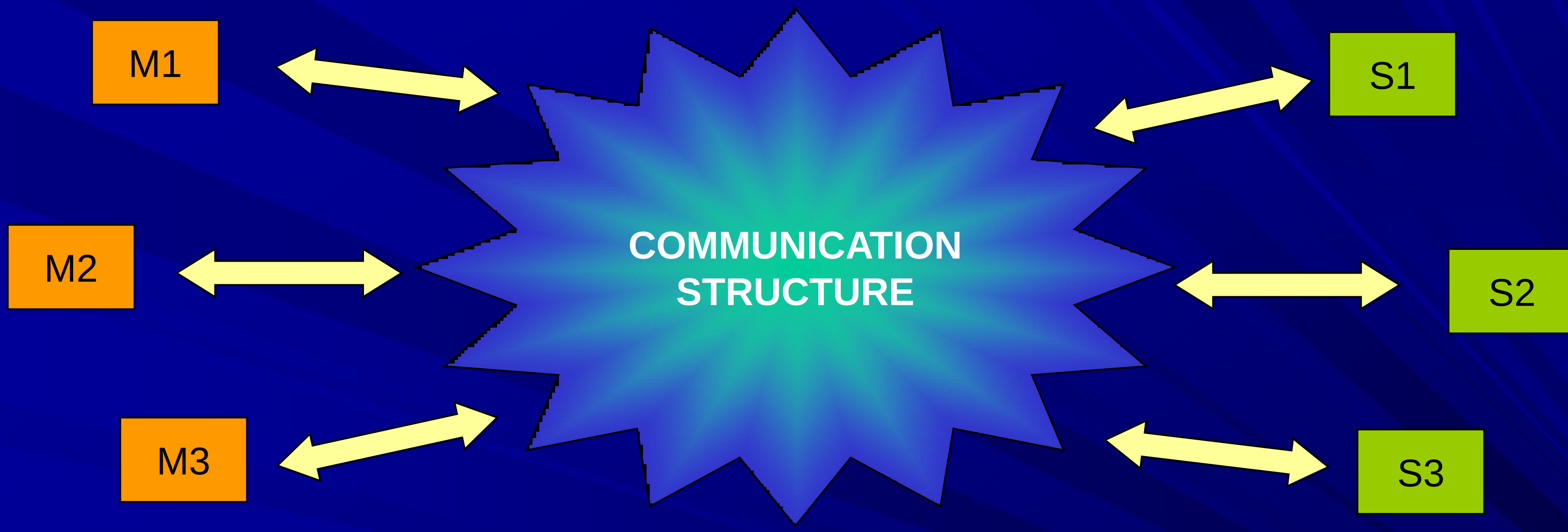
- ***COMPUTATION STRUCTURE:***
  - High level of integration: More IPs integrated to the 3D-MPSoC can be dedicated to security.
    - Cryptoprocessors
    - Security IPs.
- ***COMMUNICATION STRUCTURE:***
  - 3D-MPSoCs are foreseen as communication-centric systems.
  - All software attacks start with an abnormal communication.
  - Main role of the CS in the system operation can be used for detect an attack.

OUR WORK

Goal:

1. To integrate security mechanisms to the HoC in order to provide different levels of security (3D-QoCS), evaluate its efficiency and efficacy.

Communication structure

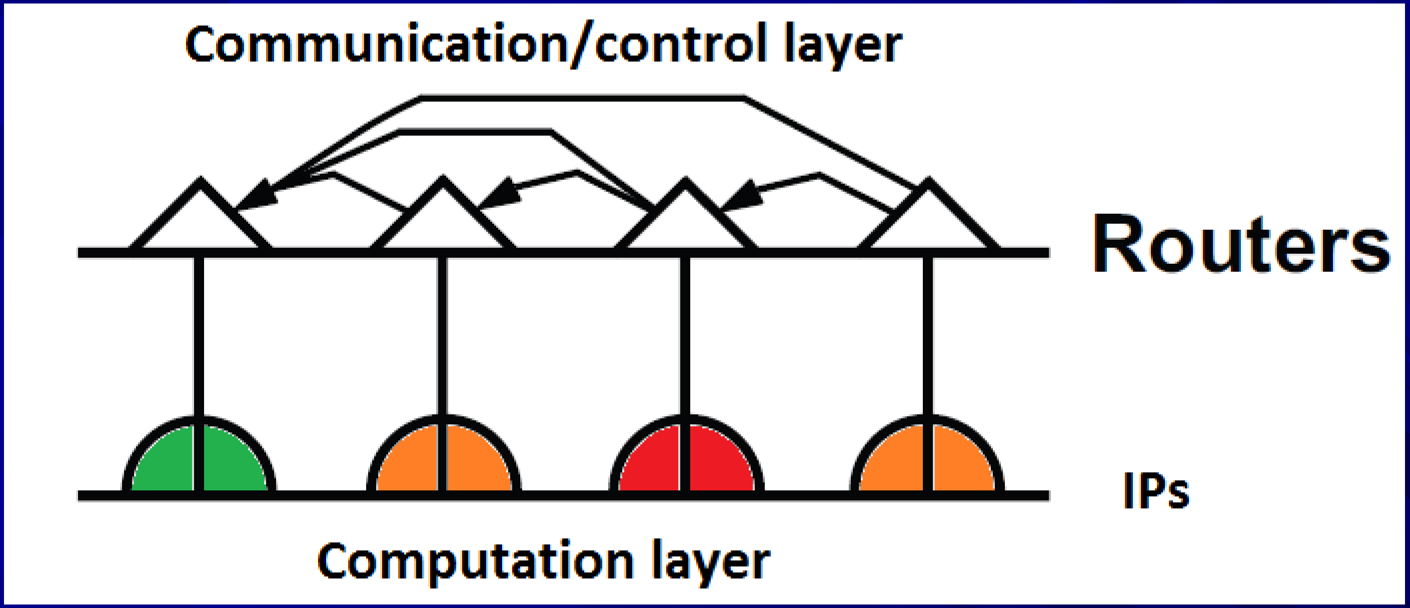


All software attack begins with an abnormal communication.

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

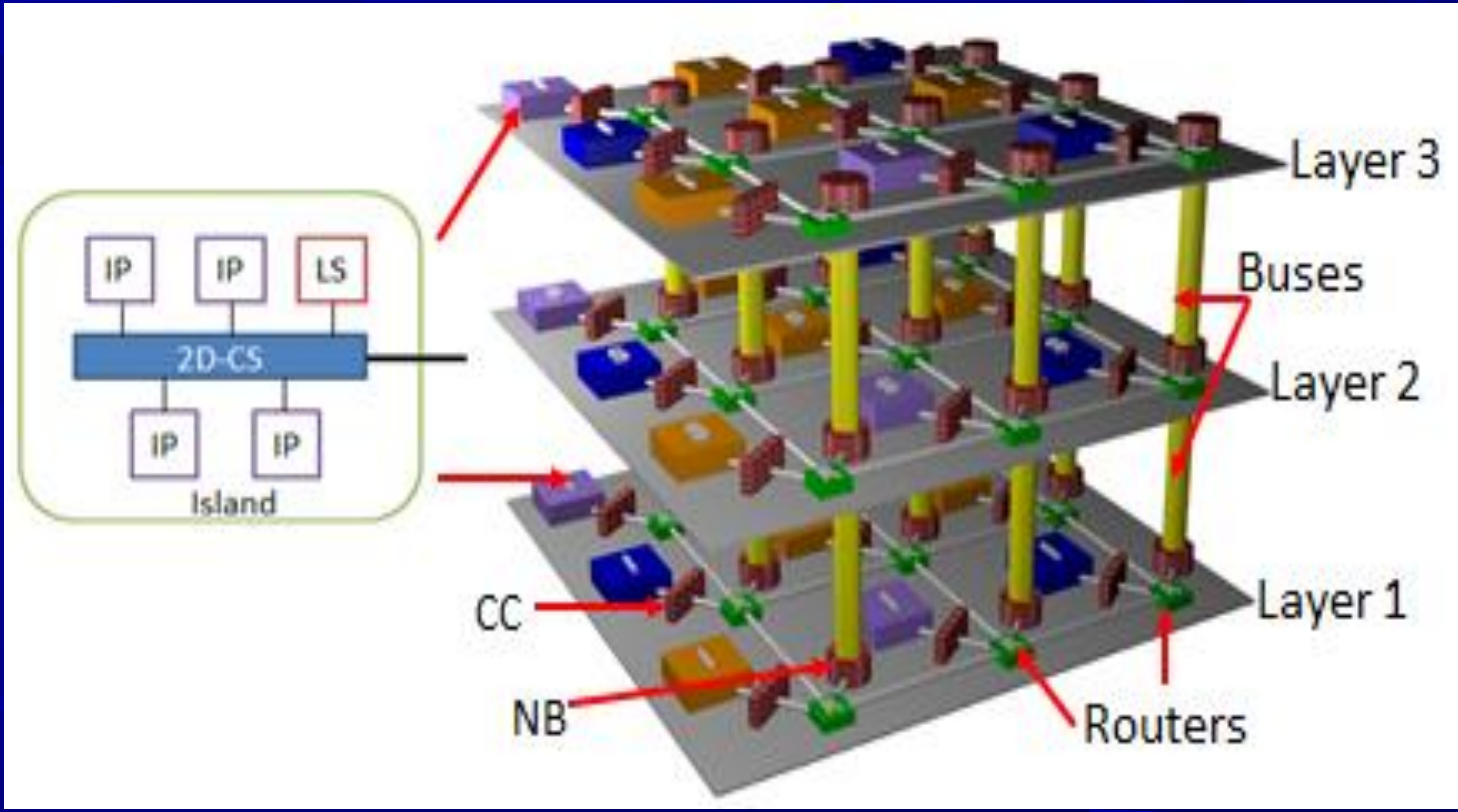
Security Implementation

1. Application specfic security layer



- Application specific security functionality
- Isolation
- Passive monitoring
- Layers can be fabricated at different foundries and integrated in a third trusty foundry.

2. Split security at all the layers



Islands: IPs or clusters of IPs.

2. Split security at all the layers

Characteristics:

We implement two security services at the 3D-HoC:

i) *authentication*: verifying the source integrity.

ii) *access control*: certifying the authorized use of the system.

- Different security choices (L0- L3):
  - Special configuration of the *security mechanism*.
  - Higher security may imply in higher costs.
  - Selection of a security level:
    - Security requirements of the system.
    - Resources availability and cost.

3D-SoC designer may select a lower protection level in order to fulfill the performance requirements (trade-off).

Access Control

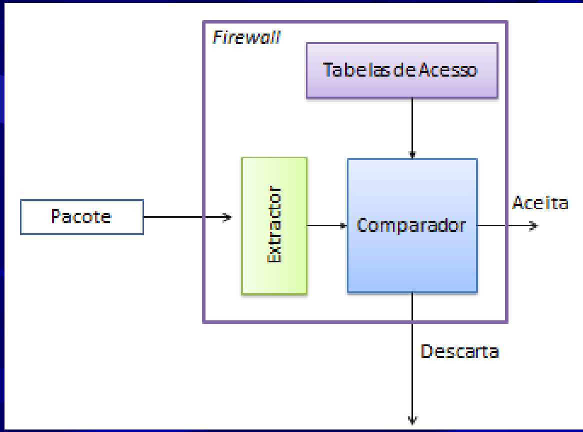
- Place of implementation: Interface, router.
- Security levels.
- Control information: Source, type, role.

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

SV: Source verification.
TV: Type verification.
RV: Role verification.

FILTER:

- *HoC firewall* : Allows or blocks a transaction.
- According to security policy.



Interface: * Before packet injection to the CS.
* Packet reception.

Authentication

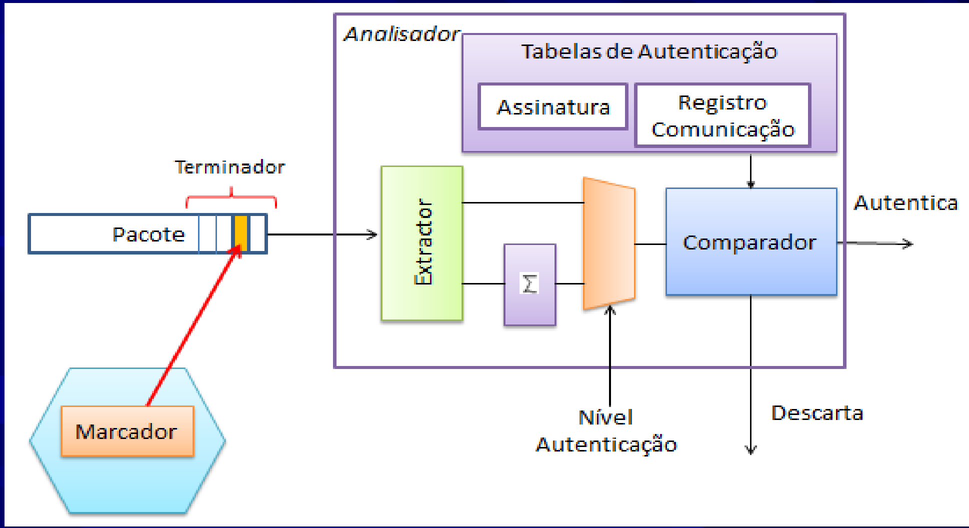
- Implementation place: Interface, router.
- No cryptographic mechanisms.
- Levels of security.

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

NR: Router number.
RP: Set Routers ID.
CC: Communication code.

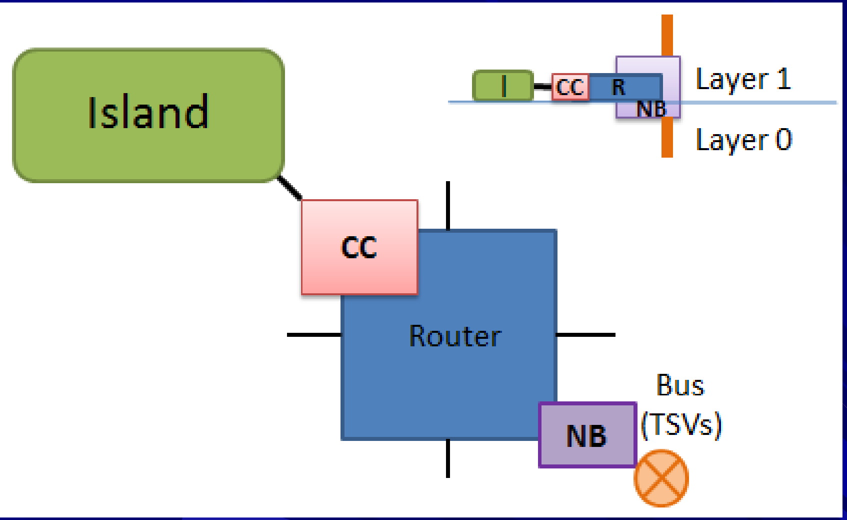
ANALIZER:

Number of routers through the communication path.
Routers ID.
Communication code.



2. Split security at all the layers

- Firewalls in the 3D-HoC interfaces: Allow or block a transaction according to the matching or mismatch between the content of the packet and the security policy.
- Firewalls store the security policy information in a *security table*.
- 3D-HoCs integrates two types of interfaces:
  - Computation-Communication (**CC**).
  - NoC-Bus (**NB**).



SECURITY MECHANISMS

Service	*Mechanism*	*CC*	*NB*	*L0*	*L1*	*L2*	*L3*
AC	Destination	Island	Memory	x	x		x
	Operation	read, read-linked, write and broadcast	read, read-exclusive, write.		x	x	x
	Size	No checking	Checking		x	x	x
	Deadline/ role	cycles/root-user	cycles/root -user			x	x
AU	Source	Island	Island	x	x		x
	Path	No checking	Checking		x	x	x
	ID Code	Checking	Checking			x	x

CC: rules the intra-layer communication (same layer).

NB: rules the inter-layer communication (different layers).

2. Architecture

Policy keeper:

- It stores the information of the 3D-SoC task mapping and the security policy.
- The security policy set the protection level (from L0 to L3) of each service.
- The size of the table stored by the policy keeper component depends on the number of applications, tasks and IPs integrated at the 3D-MPSoC.

Reconfiguration manager:

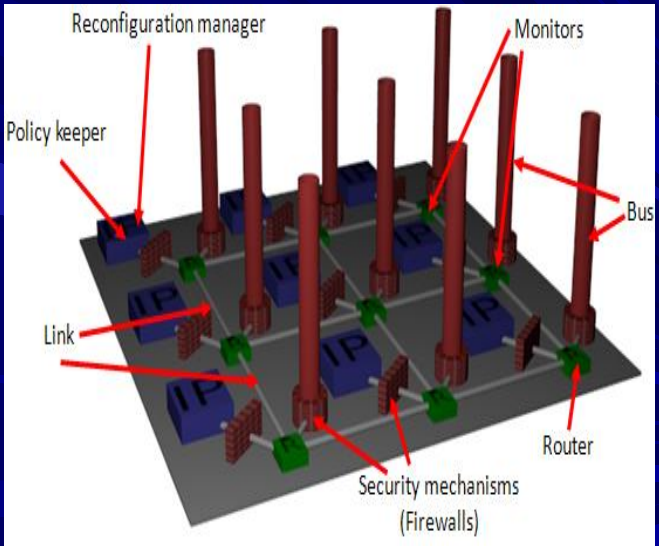
- Coordinates the upgrading of the security table of all the firewalls.

Security mechanisms:

- Defends the 3D-MPSoC against possible attacks.
- Uses the information embodied in the packets.
- Able to be upgraded.

***Monitor**:*

- Audits the communication behavior of the 3D-SoC.
- Determine the completion of the transaction.
- Embodied at the routers of the 3D-HoC.

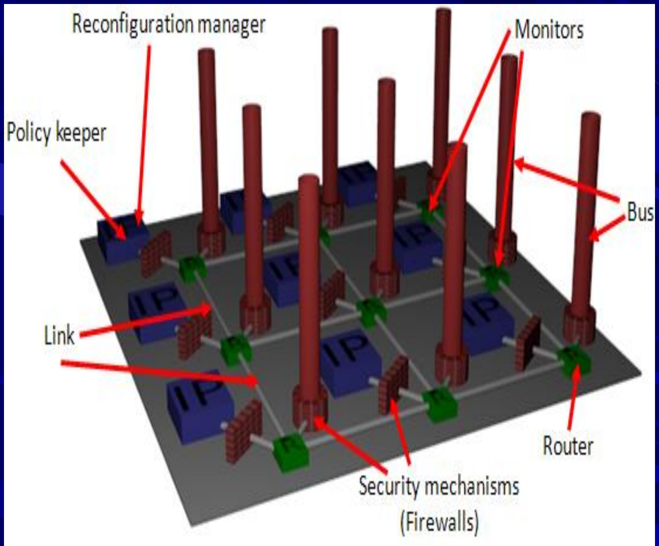


2. Functionality

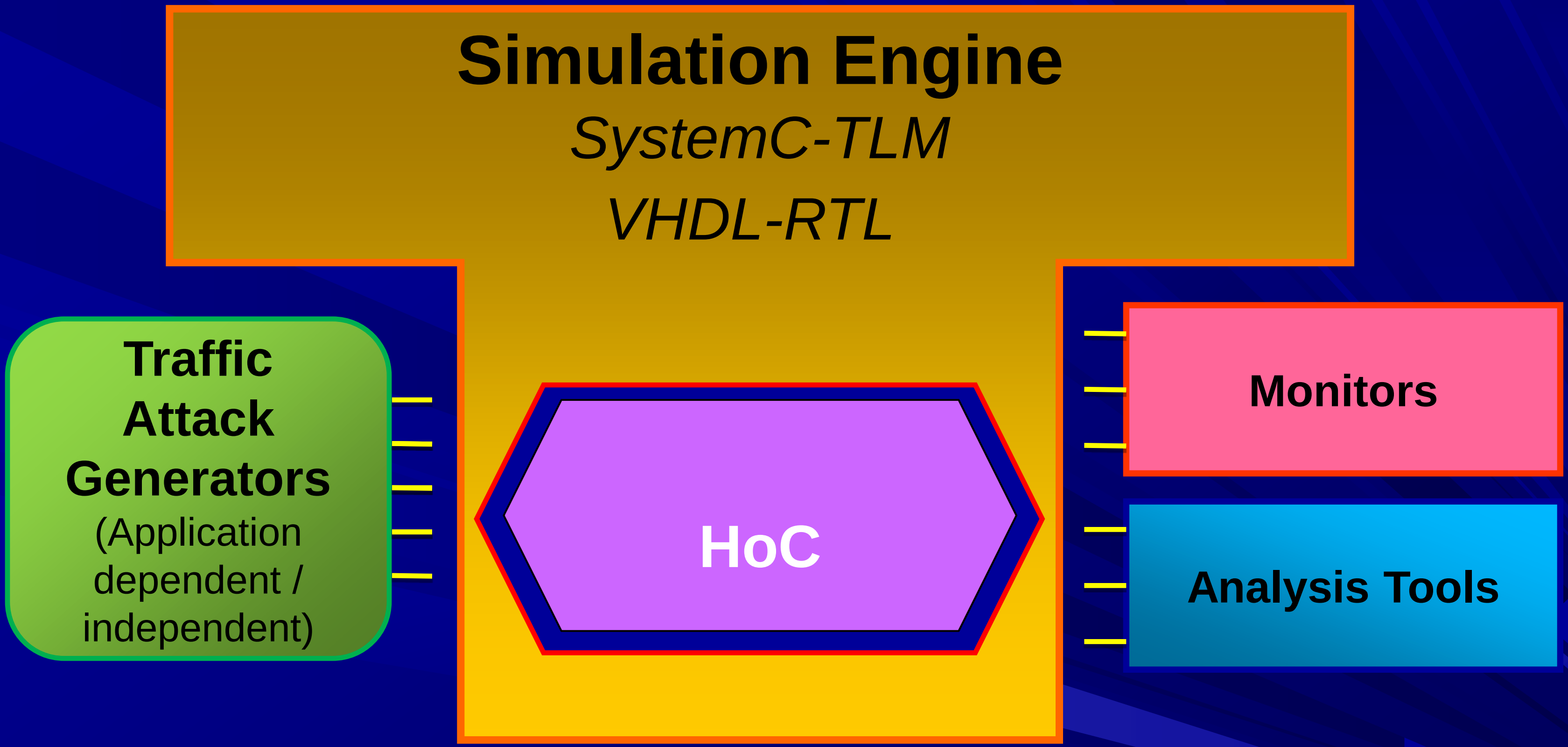
1. ***Analysis the security policy***
   - Identify the firewalls that must be configured (target firewall).
   - Which, where, new data.

2. ***Configuration of security mechanisms***
   - Block injection od new data whose destination is linked to the target firewall.
   - Send new data (local and global configuration).

3. ***Recovery***
   - Unblock communication.
   - Resume operation.



Evaluation



HoC simulation and evaluation framework.
Supports different traffic conditions.

Experimental Setup

CS: *2D-NoC (application specific layer)*

HoCs (security in all the layers)

HoC Configuration

- Stacked, single, ciliated and **3D-HoC** **3(5x5)/25/32)**
- XYZ routing algorithm
- 75 IP cores 3D-MPSoC
- Round-Robin
- Simple/QoS arbiter
- FIFO memory organization

Simulation Conditions

- *5 flits Payload.*
- *900.000 simulated cycles.*

Experimental Setup

- 3 characteristics of the traffic: Nature, topology and type.
- **Topology**
    - Hot-spot
    - Transpose
    - Uniform

- Real application (3 Applications, different security policies)

- **Nature**
    - Poisson + % LRD .

- **Type of traffic**
    - Best effort
    - Priority (L M H)
    - Guarantee

- Dynamicity (0, 20, 40, 50, 60 ,80)

Results

Efficiency:

* 3 different kind of attacks (Modification, extraction, *DoS*).

SECURITY EFFICACY

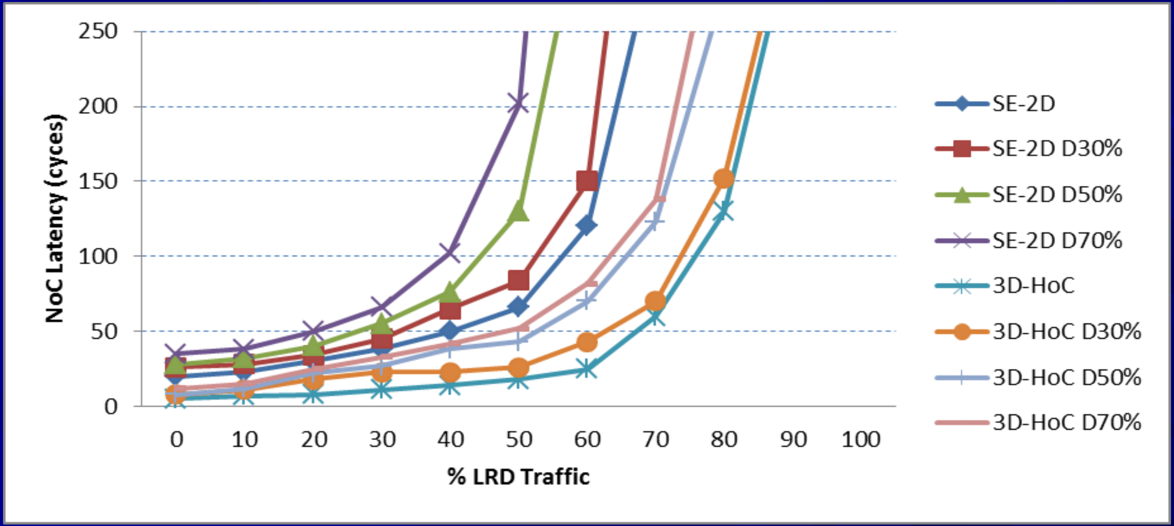
Attack scenario	*2D-NoC*	*3D-HoC*
Write critical data	97%	97%
Read critical data	100%	100%
Malicious task migration	100%	100%
Nonexisting target /Repeated data	89%	89%
Communication target = source	100%	100%

- They show identical security efficacy (percentage of detected attacks).
- It was expected because the values of the security values at both alternatives were the same.
- The difference is the implementation (centralized, spread).
- 97% of efficacy mean that the security designer should increase the protection level in order to achieve a 100% of protection.

Results

Efficacy:

Latency results for CS L3 AC and AU security level and different dynamicity.



- 3D-HoC achieves a better performance when compared to 2DNoC.
- 3D-HoC is less sensible to the dynamicity of the system.

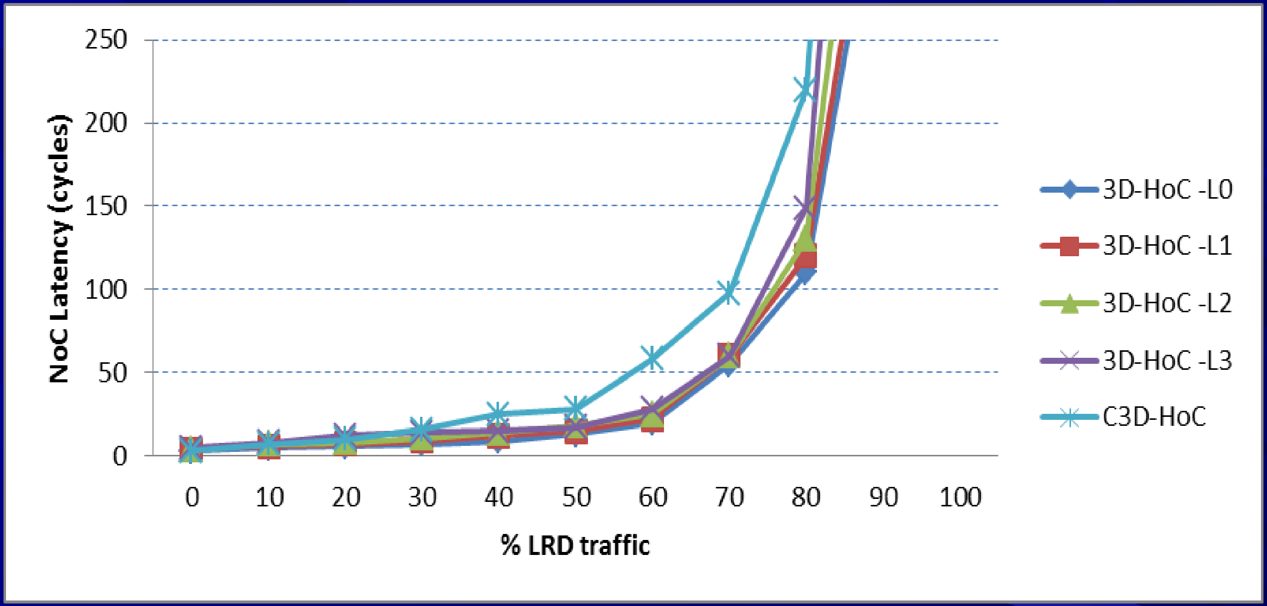
  i) 3D technology characteristics (smaller initiator/destination paths).

  ii) At the reconfiguration phase, only some small areas of 3D-HoC where blocked.

Results

Efficacy:

3D-HoC latency results for different levels of protection.



There is a trade-off security/performance to be explored!

Conclusions and future work

•We propose a dynamic security enhanced 3D-HoC for 3D-SoC protection.

•We show that 3D-HoC can be an efficient structure to guarantee the protection in the system.

•3D technology not only presents new challenges, but new opportunities to achieve a secure and efficient system.

•Three techniques are employed in order to achieve an efficient configuration:

- Only some firewalls are upgraded, so the communication in the remaining of the system is not interrupted
- Security customization
- Intrinsic low latency of 3D technology.

Conclusions and future work

- We compare our distributed architecture with a centralized one. As dynamicity increases, the distributed alternative becomes more efficient.

- As future work we plan to implement integrity and confidentiality security services.