CITY UNIVERSITY LONDON

Security-informed safety case approach to Analysing MILS Systems

Kateryna Netkachova, Kevin Müller, Michael Paulitsch, Robin Bloomfield

Collaboration: City University London, Adelard LLP,
Airbus Group Innovations, Thales

International Workshop on MILS:
Architecture and Assurance for Secure System

20 January 2015

CITY UNIVERSITY LONDON

EST 1894

Structure of the presentation

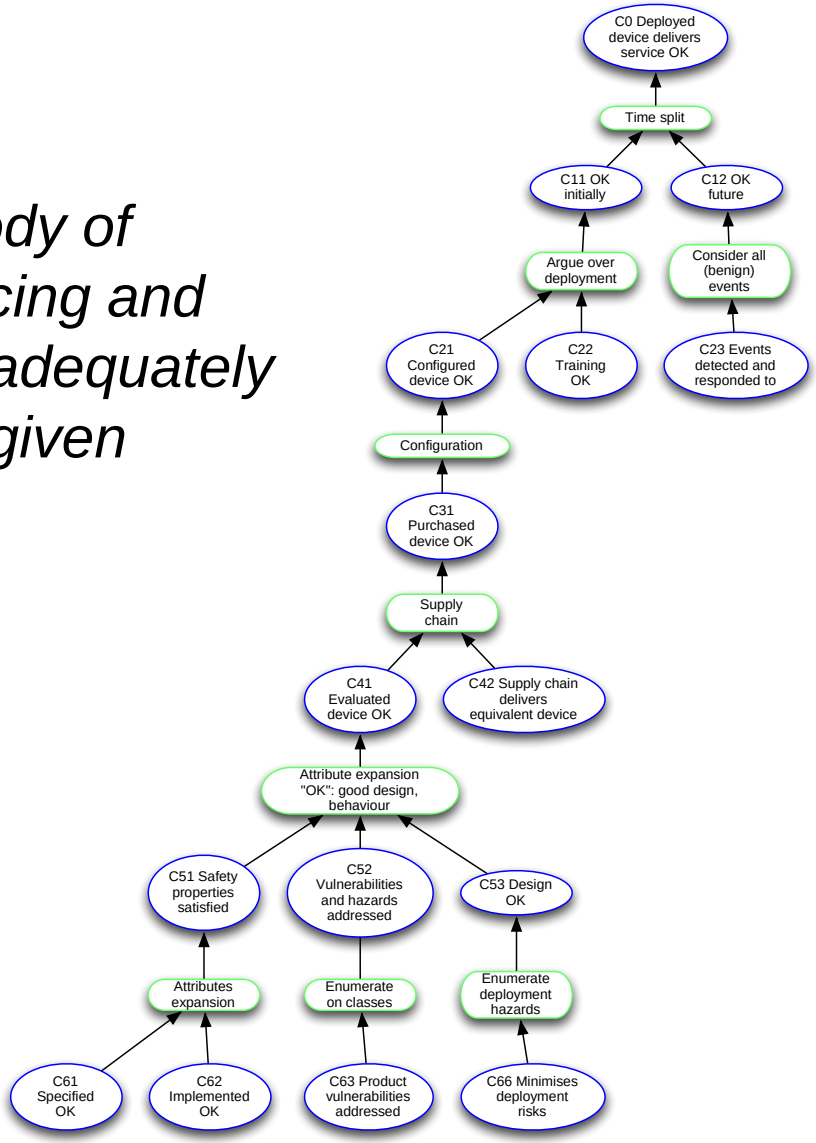
1. Introduction
   - Projects: SESAMO, EURO-MILS, CEDRICS
   - Integrated security and safety solution
2. Safety cases, security-informed safety cases
3. The layered assurance approach
4. Application to the MILS use case
5. Discussions and next steps

CITY UNIVERSITY LONDON

Safety Cases

Safety case *– a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment.*

- Overall approach
- Claims, Argument, Evidence
- Top claim
- Split into sub-claims
- Structure of argumentation



CITY UNIVERSITY LONDON

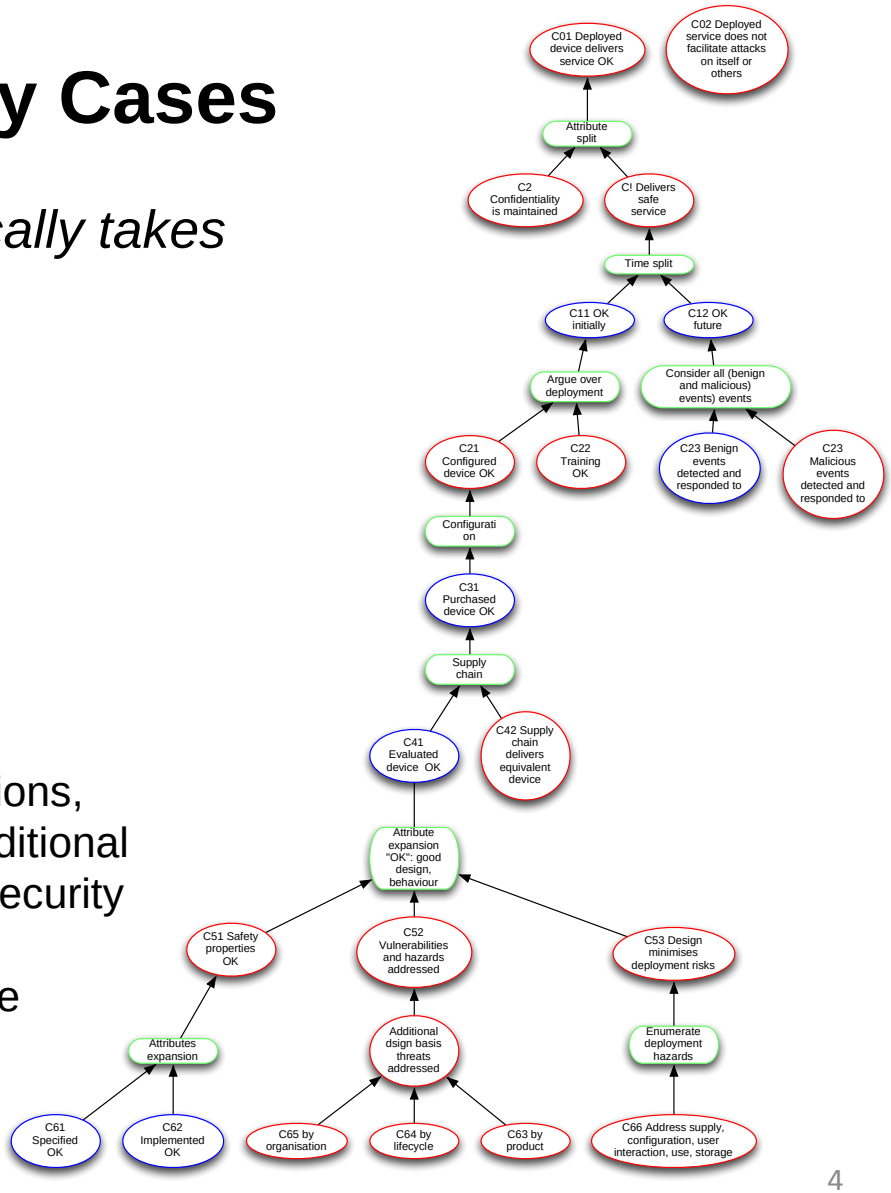
EST 1894

Security-informed Safety Cases

Justification of safety which specifically takes into account the impact of security.

- Security consideration
- Impact on the Case Structure
- Some observations

Supply chain integrity.
Malicious events post deployment.
Design changes to address user interactions, training, configuration, vulnerabilities. Additional functional requirements that implement security controls.
Possible exploitation of the device/service to attack itself or others.



CITY UNIVERSITY LONDON

Levels of abstraction

- **L0 Policy and requirements** – the highest level of abstraction where the system represents its requirements, and defines safety and security policies and their interaction;
- **L1 Architectural layer** – the intermediate level where the abstract system components and architecture are analysed;
- **L2 Implementation layer** – the detailed level where the implementation of specific components and their integration within the specific system architecture are scrutinised.

CITY UNIVERSITY LONDON

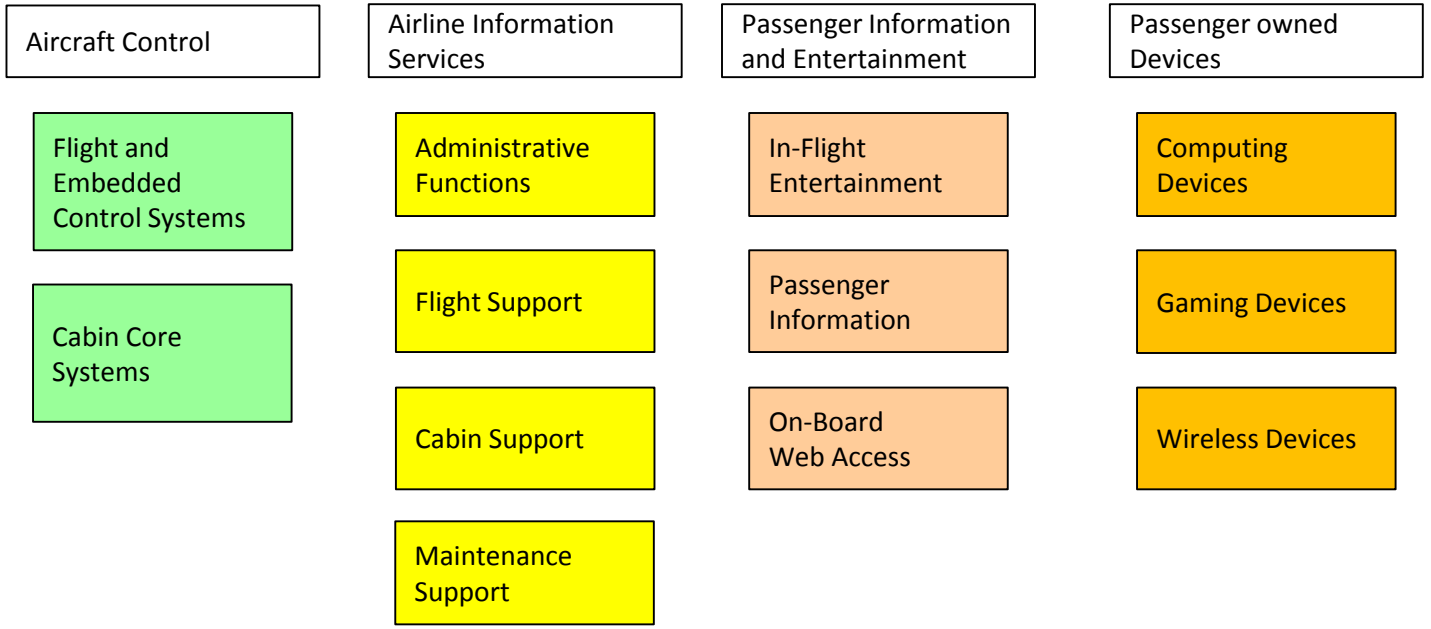
EST 1894

Application to the MILS Systems

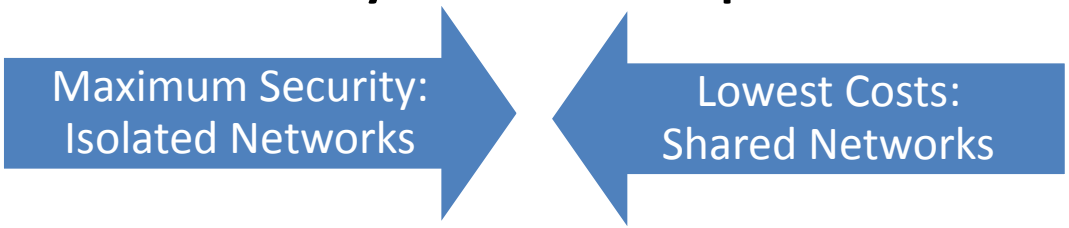
- Safety case perspective – not common using the CAE structure in avionics
- Case Study: MILS-based gateway controlling information flow between aircraft security domains
- Details of the approach
- Some observations from the Case Study
- Layered Assurance, Compositional Trustworthiness (LAW)
- Further directions and improvements

CITY UNIVERSITY LONDON

Use Case (ARINC 811)



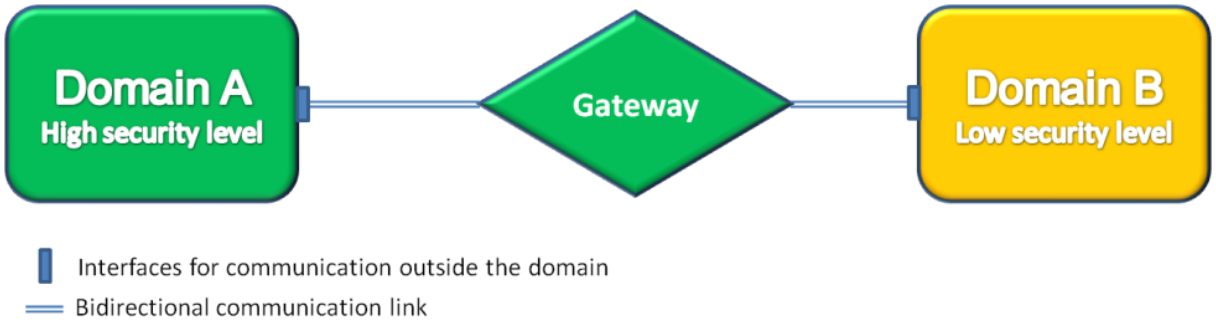
How to securely connect multiple domains?

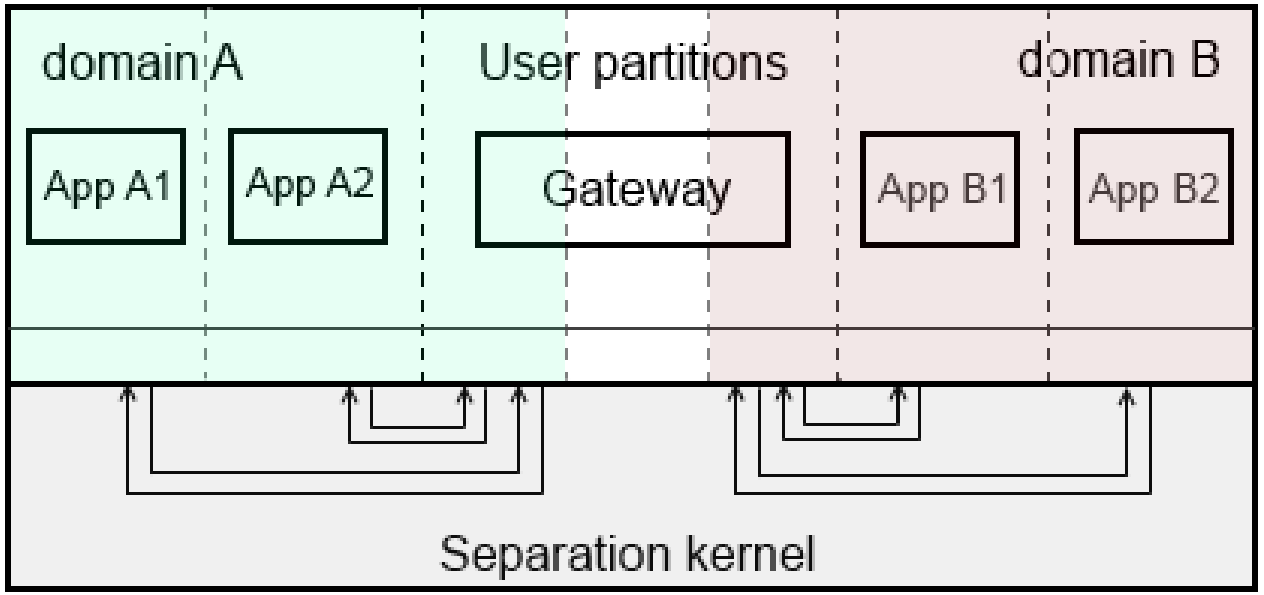


Solution: Gateway between domains

CITY UNIVERSITY LONDON

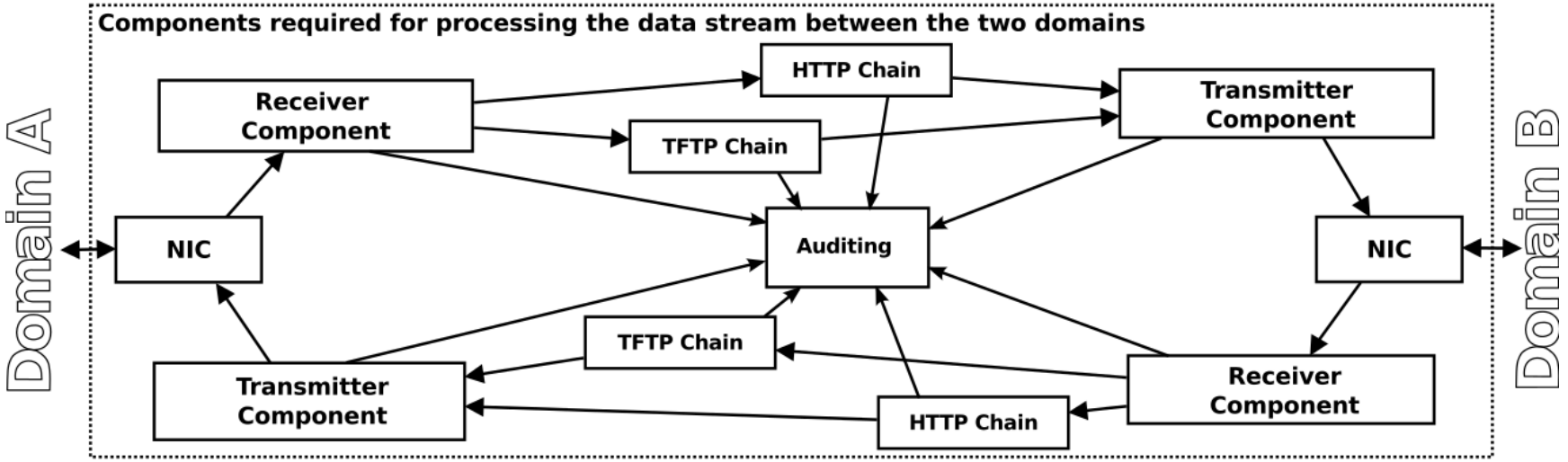
Logical scope





CITY UNIVERSITY LONDON

High-level View of Gateway Components



CITY UNIVERSITY LONDON

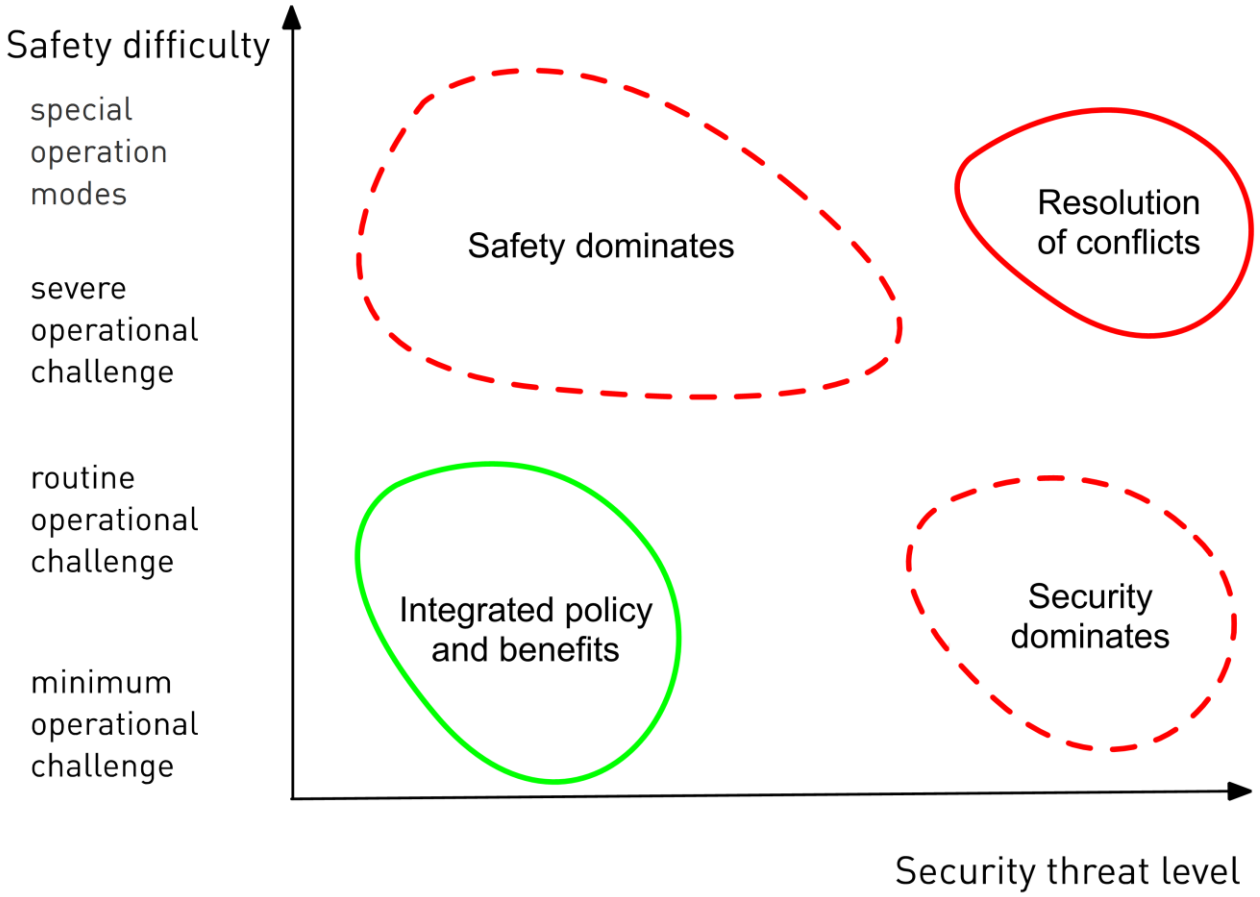
L0 Policy and requirements

At L0 we consider both security and safety and we wish to claim that the policies are adequate. We address this by considering two main aspects:

- The definition of the individual policies
- The interaction of the policies

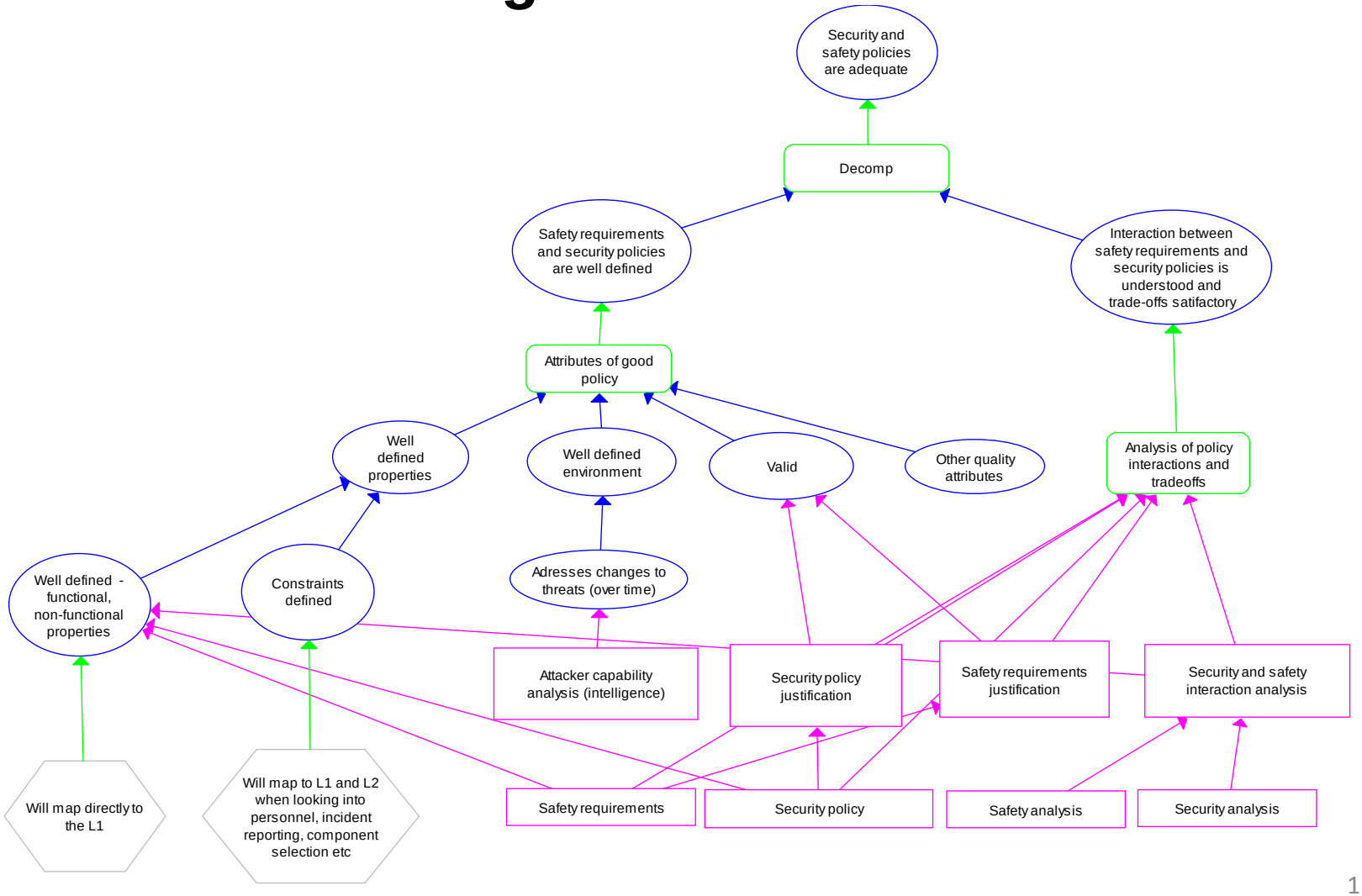
CITY UNIVERSITY LONDON

Defining integrated policy



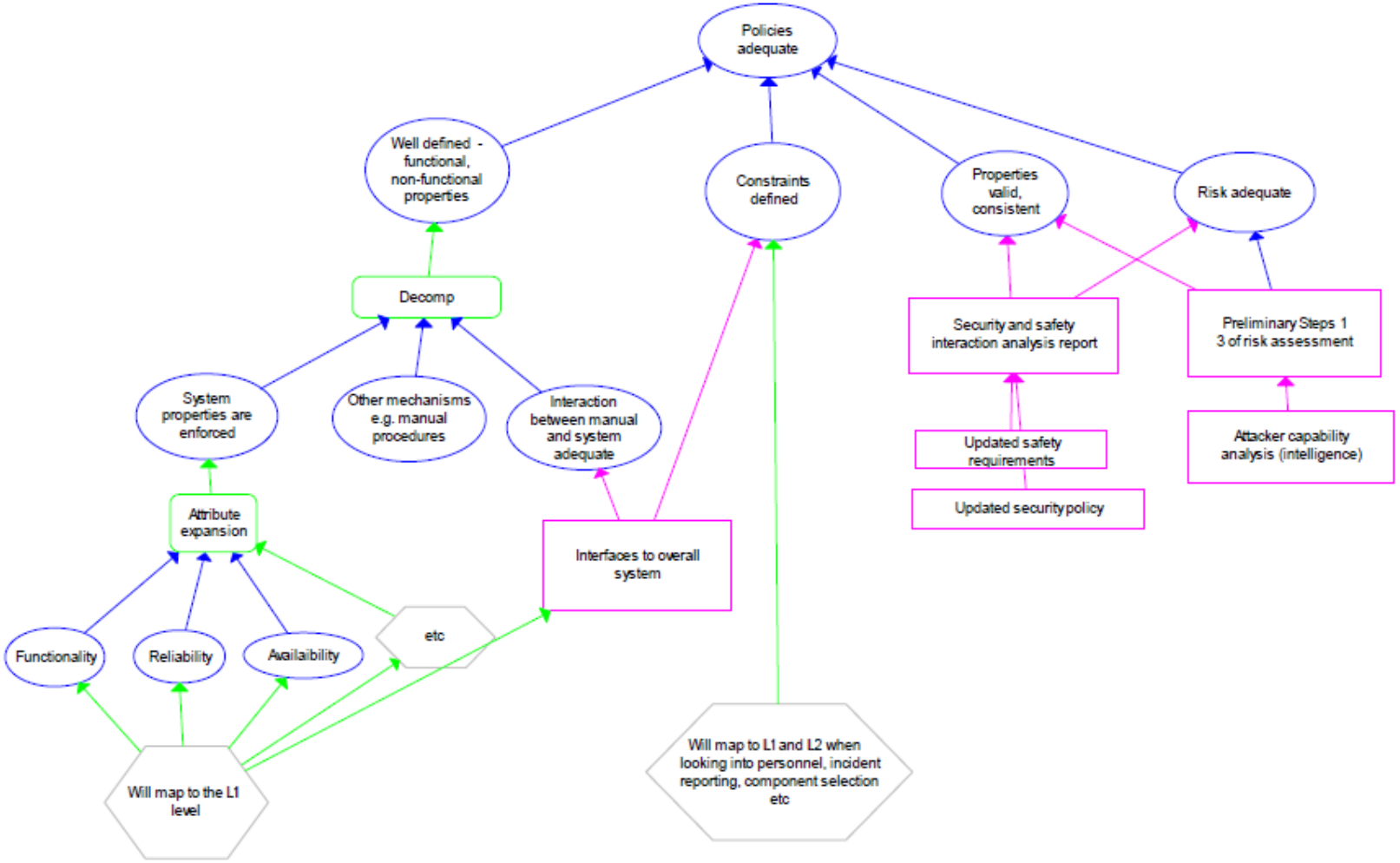
CITY UNIVERSITY LONDON

L0 – sketch of the general case



CITY UNIVERSITY LONDON

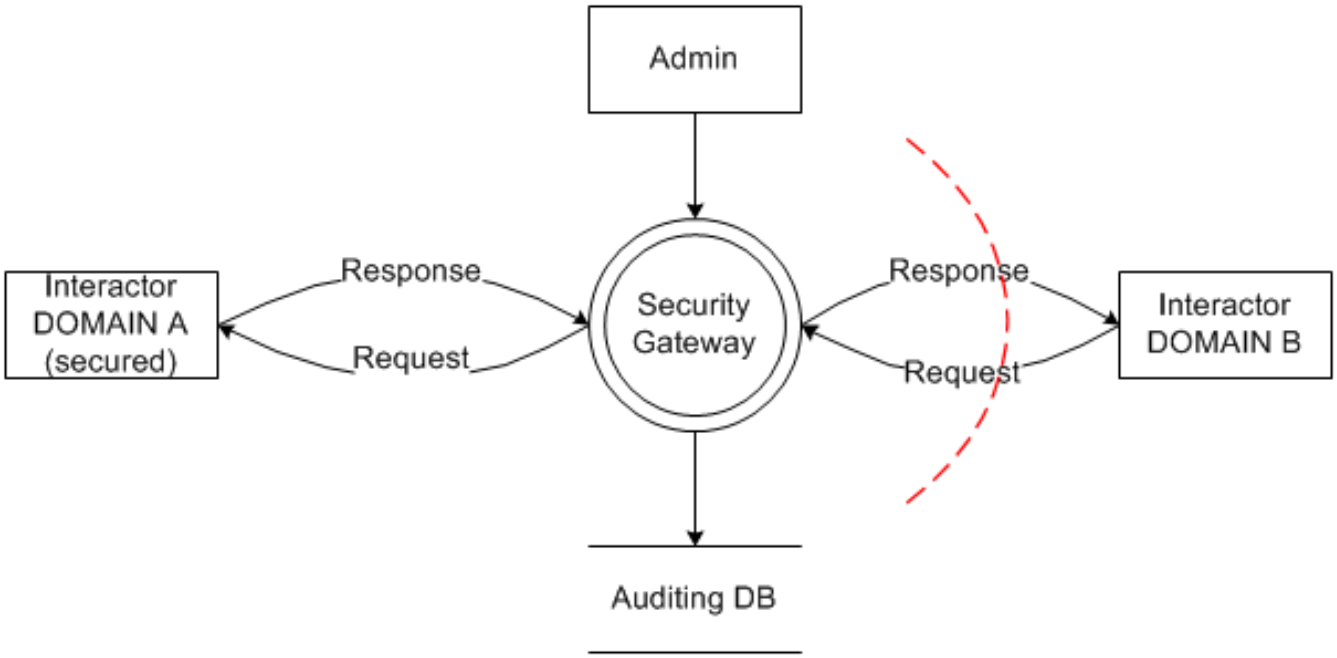
L0 – sketch of the gateway case



CITY UNIVERSITY LONDON

Scope of the system

Context DFD representing the highest level view of the system (SDL Threat Modelling Tool).



CITY UNIVERSITY LONDON

L1 – architectural level

At this level various methods are used to analyse the system:

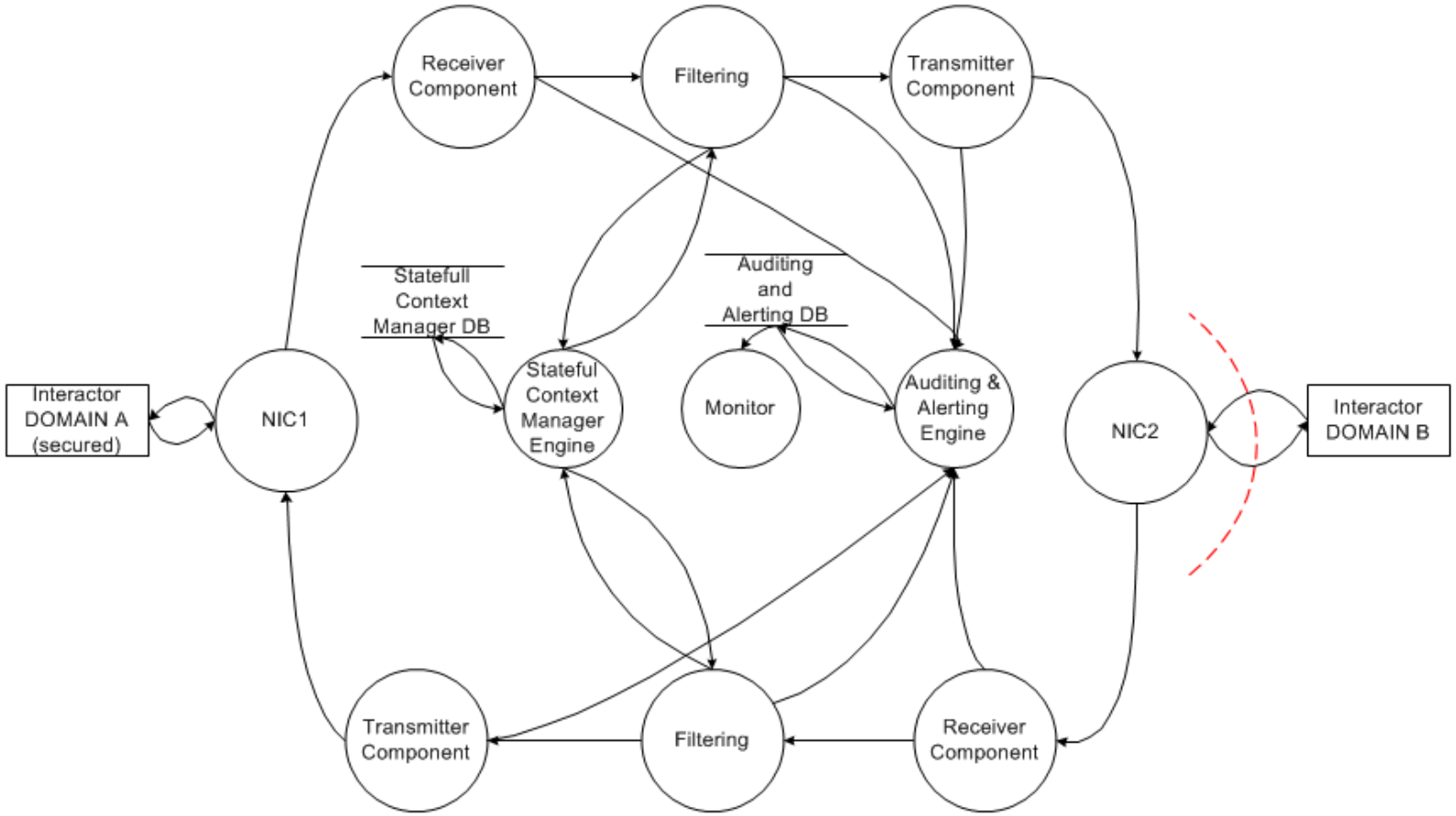
- A guideword based approach derived from the safety HAZOP analysis.
- An analysis of trust relationships
- Construction of attack scenarios and attack graphs
- STRIDE, the Microsoft threat modelling approach

In order to construct a case, at this level we need to take into account:

- The output from the L0 level of abstraction
- The identified and revised critical safety and security properties of the system
- Components that play essential roles in enforcing the critical properties
- A high-level architecture of the system representing components and their interaction
- Dynamic aspect to consider possible changes to the system in the future.

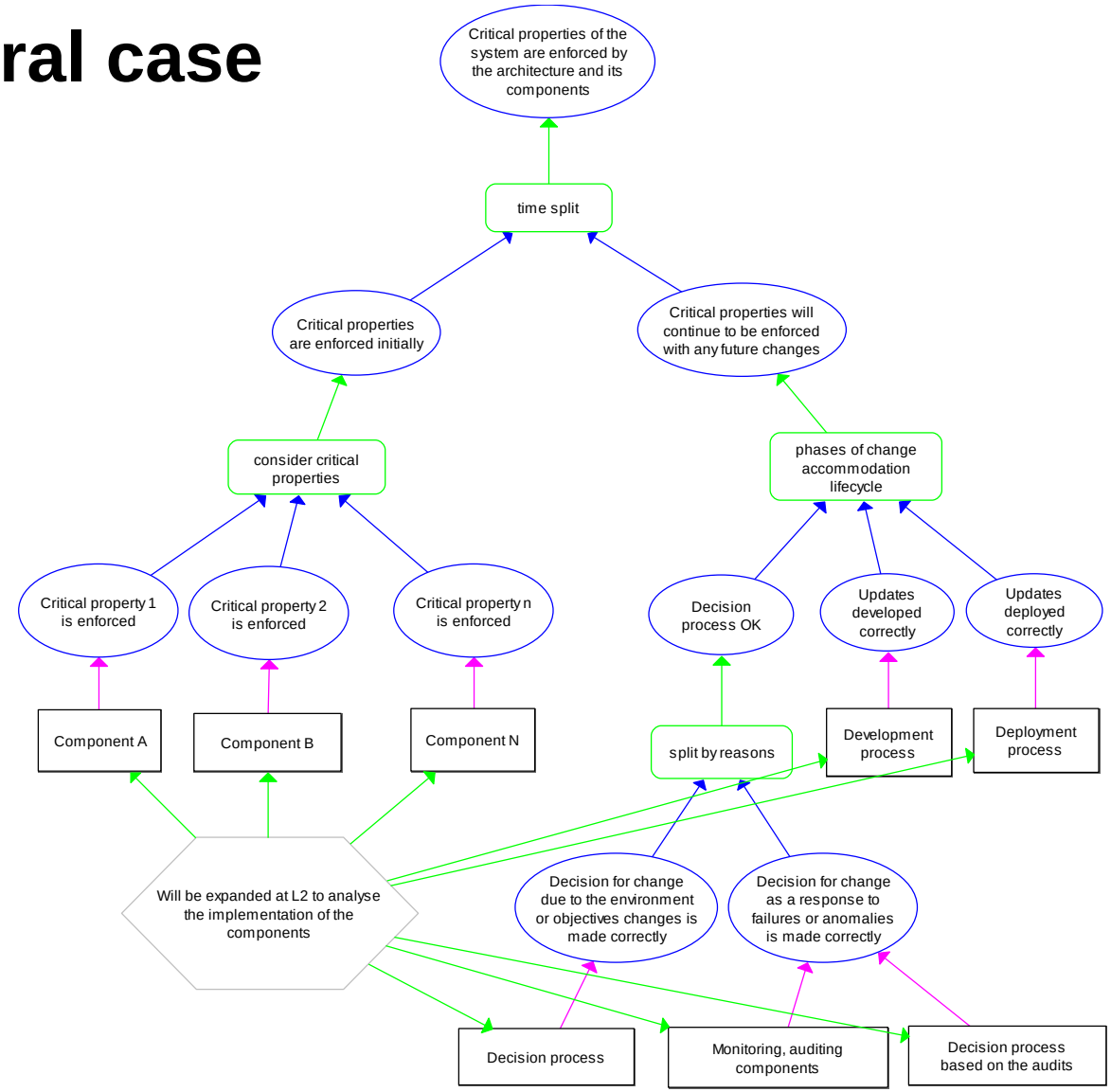
CITY UNIVERSITY LONDON

Level-n DFD model (SDL Threat Modelling Tool)



CITY UNIVERSITY LONDON

L1 general case



CITY UNIVERSITY LONDON

Hazop guidewords with respect to security

Example guidewords	Impact on security attributes		
	Confidentiality	Integrity	Availability
Late/too soon		Could cause downstream corruption.	Might impact protocols and availability
As well as	Additional info (of same class, of different class)		
Wrong	Classification (so inadvertent high to low)	Wrong message	
More/less/intermittent		Corrupted info "less" or "more" than needed	Could cause denial of service., loss of availability depending on how handled

CITY UNIVERSITY LONDON

Identifications of hazards

Service interface hazards:

- Denial of service:
  - Are channels isolated from each other?
  - Are there any application limits on resource consumption?
- Service guarantees:
  - What service level guarantees does the gateway provide?
  - Are there any end-to-end checks at the application level?
- Man-in-middle attacks:
  - How does the application know that it's talking to the gateway?
  - How does an application know that a message has come from a different security domain?

System operational hazards:

- The gateway is configurable, so there are hazards relating to incorrect maintenance or configuration of the system
- The audit log might contain sensitive information and therefore needs to be protected
- Physical access to the gateway during flight is considered impracticable, so the main threats come during maintenance when the plane is on the ground

CITY UNIVERSITY LONDON

Example of Hazop applied to the case study

No.	Element	Guide word	Deviation	Possible causes	Consequences
Function considered:			Connecting to the gateway		
1	Connect to channels	OTHER THAN	Application connects to a channel other than gateways.	Another application from the same domain pretends to be and acts like a gateway.	Man-in-middle attacks.
2	Connect to channels	MORE	Too many messages are sent to gateway channels.	Broken or compromised application is sending too many requests.	Denial of service.
Function considered:			Gateway filtering		
12	Filter messages going through the gateway	AS WELL AS	Additional messages are allowed to pass through the gateway.	Error in filter specification or implementation.	Leakage of confidential data.

CITY UNIVERSITY LONDON

EST 1894

Analysis of trust relationships

- Identify trust relationships:
  - Gateway trusts Administrator
  - Auditing system trusts Gateway
  - Applications trust separation kernel
  - Applications in the same domain trust each other
- Identify consequences of breach of trust
- Assess risk
- Design mitigations as appropriate

CITY UNIVERSITY LONDON

Example of analysis

Breach of Trust	Consequences	Mitigation
Gateway – Administrator	High Denial of service, loss of data integrity and confidentiality, man in the middle attack.	All security policies have to be operating and have to be identified by some authority. The gateway will only accept these security policies.
Gateway – Audit logs	Medium Loss of accountability and nonrepudiation, possible impact on confidentiality	Applications located in the domains can have their own logs documenting what they sent. No confidential data or data that can help facilitate an attack should be stored in logs.

CITY UNIVERSITY LONDON

STRIDE threat modelling (Microsoft)

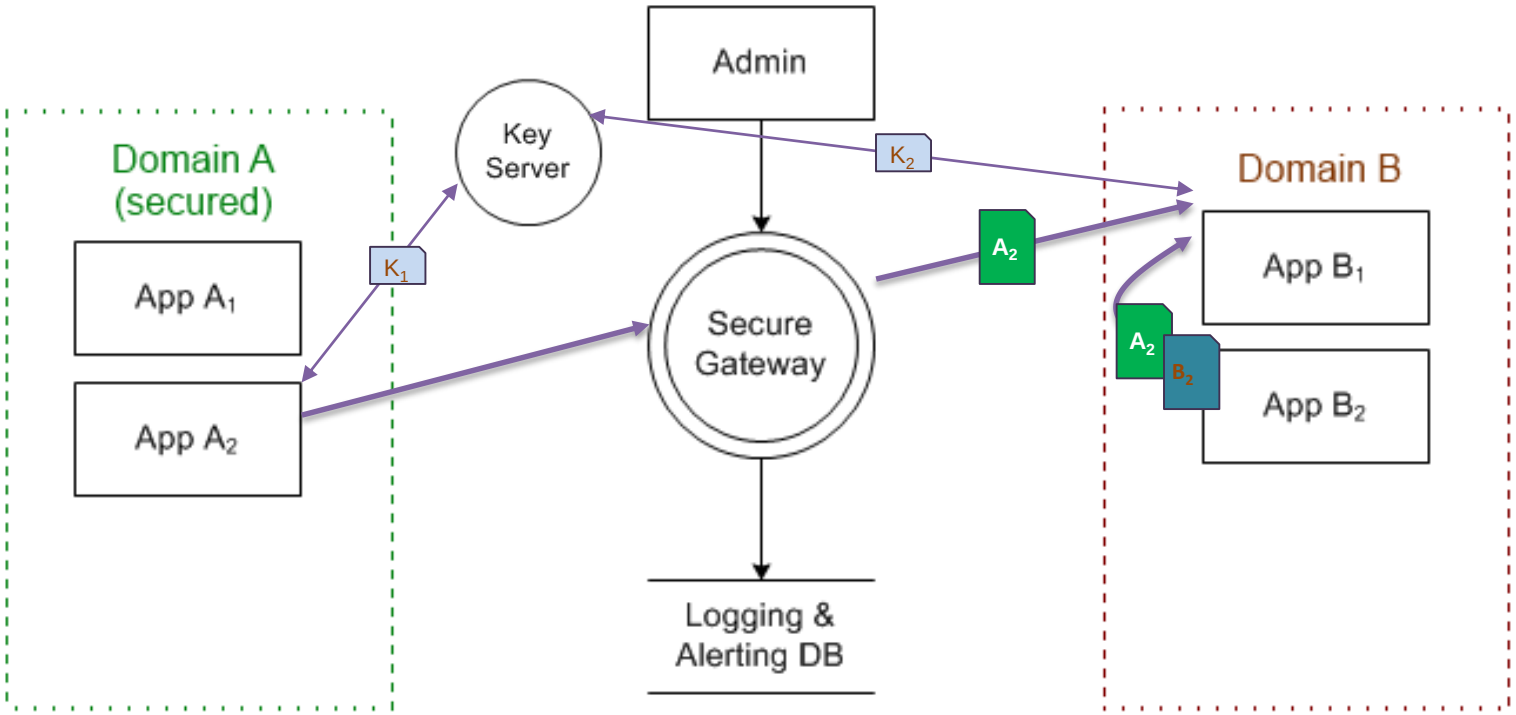
STRIDE stands for:

- Spoofing (impersonating someone else)
- Tampering (modifying data)
- Repudiation (claiming not to have performed an action)
- Information disclosure (loss of confidentiality)
- Denial of service (deny or degrade service to valid users)
- Elevation of privilege (gain privileged access)

CITY UNIVERSITY LONDON

Attack scenarios – example 1

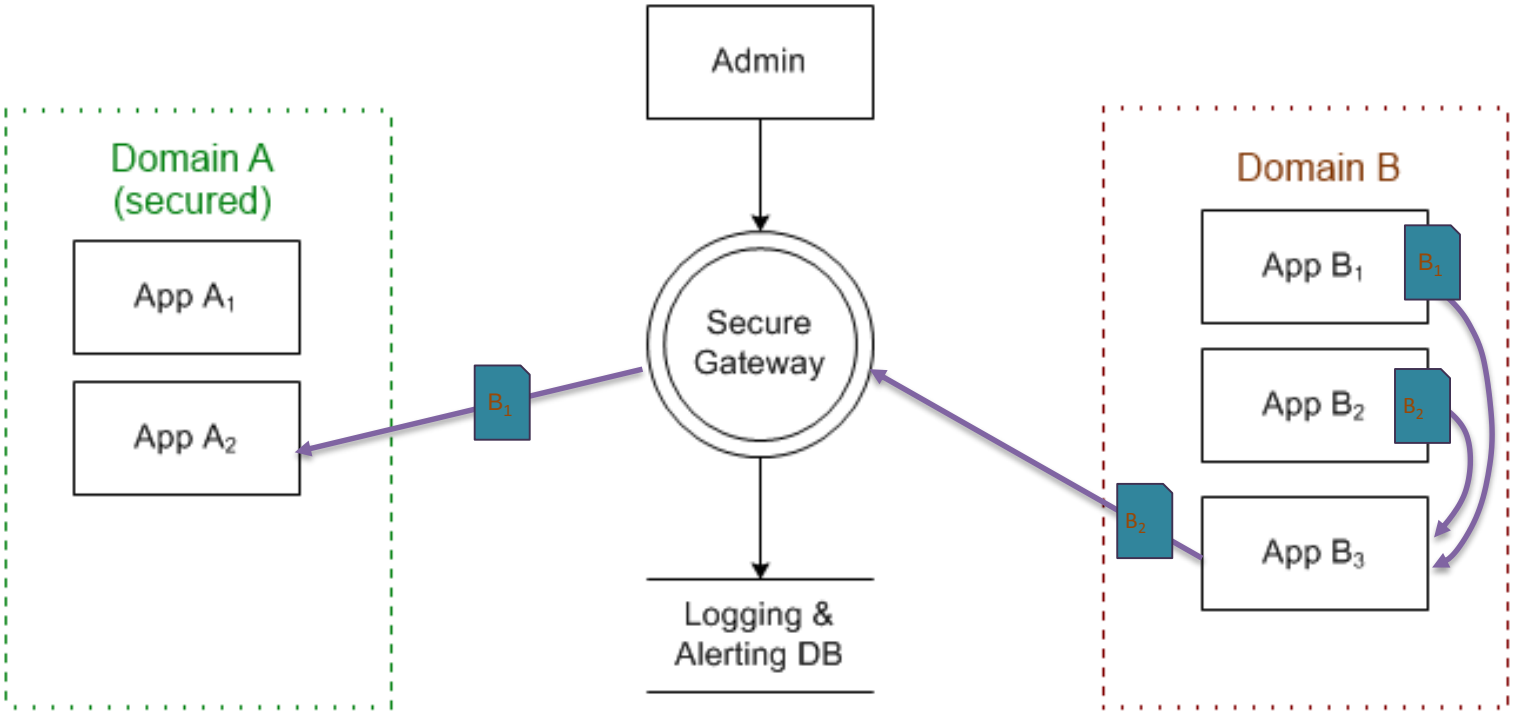
- Spoofing



CITY UNIVERSITY LONDON

Attack scenarios – example 2

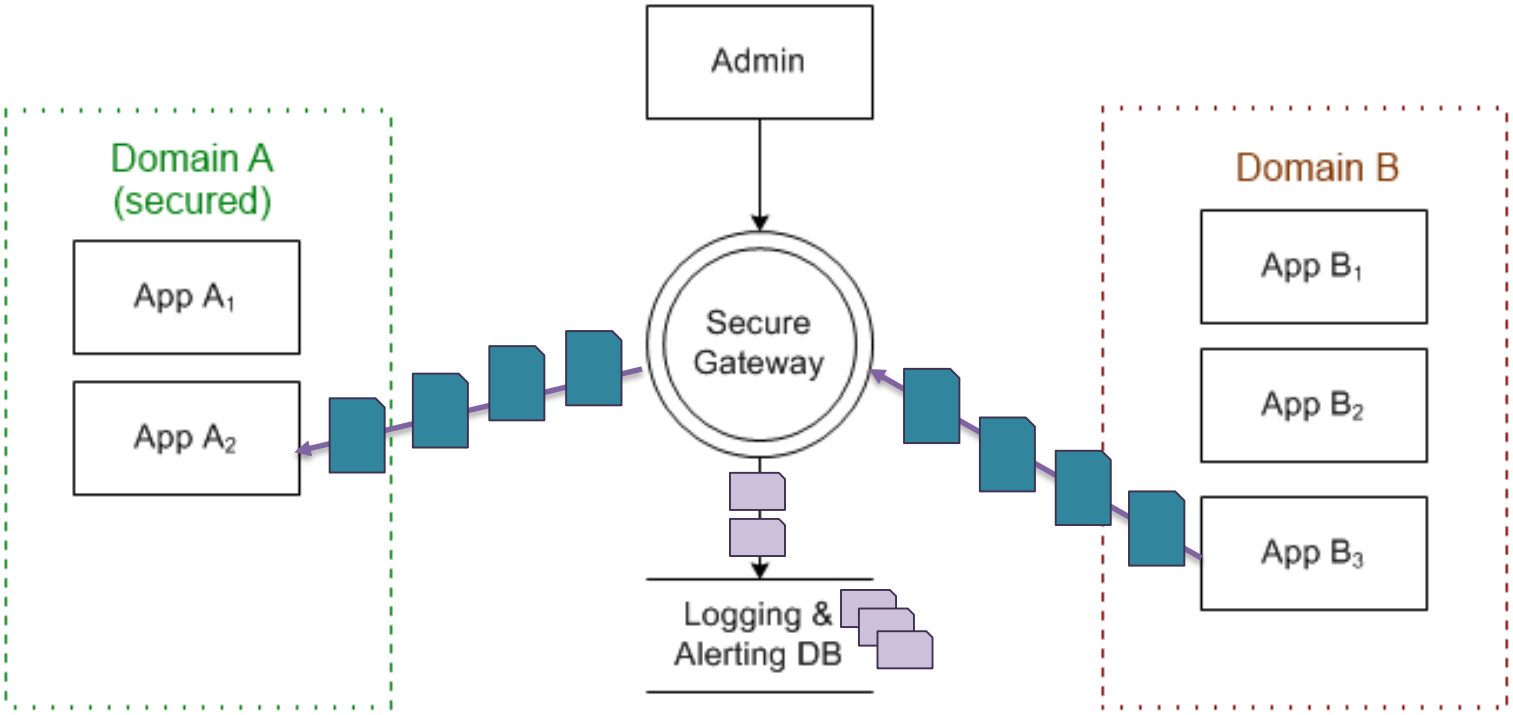
- Spoofing, tampering



CITY UNIVERSITY LONDON

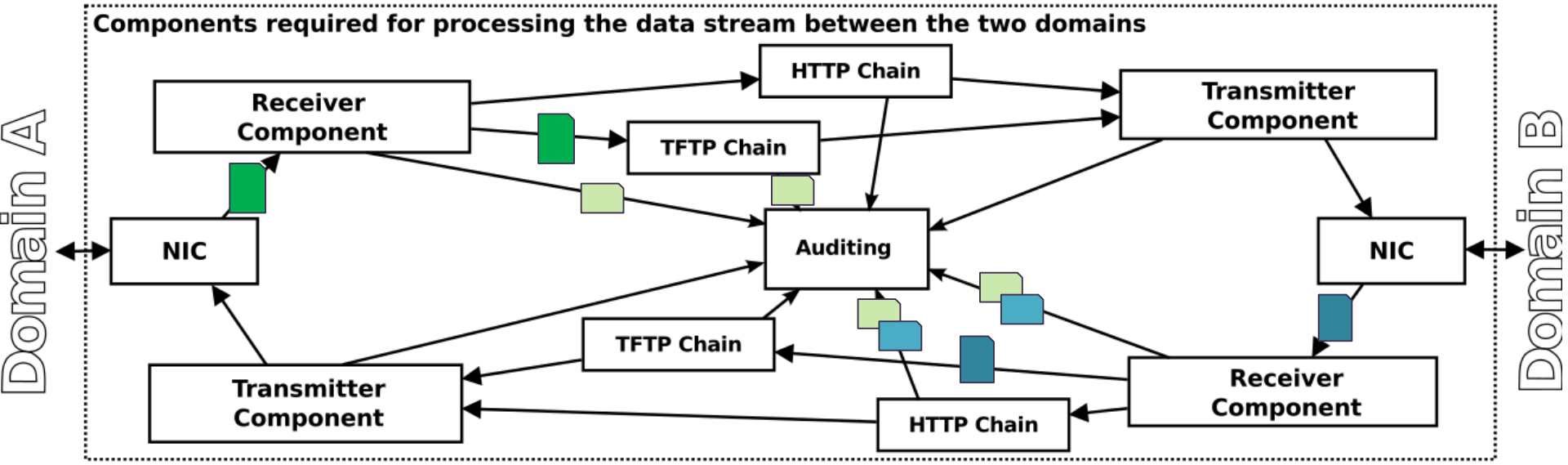
Attack scenarios – example 3

- Denial of service



CITY UNIVERSITY LONDON

Attack scenarios – example 4



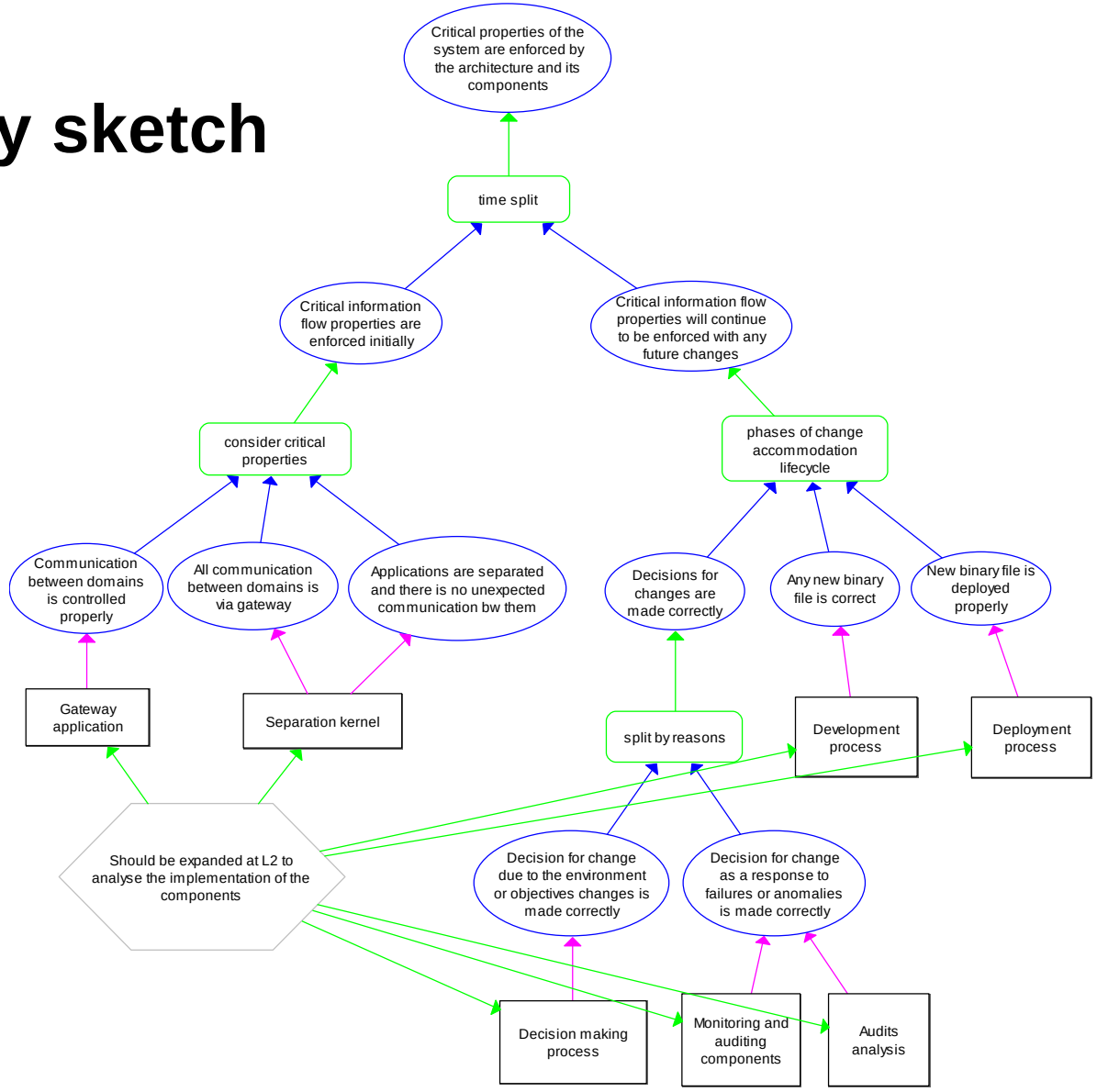
CITY UNIVERSITY LONDON

Example of STRIDE applied to the gateway

Threat type	Security property	Brief explanation	Use case examples	Mitigation
Spoofing	Authenticity	Impersonating someone else.	1) Application from domain B pretends to be a gateway or an application from domain A and sends something to domain B users. 2) One application from domain B pretends to be another application from domain B and requests something from the gateway.	The inter-domain communication is controlled by a MILS separation kernel. The entire system is assembled and configured by a knowledgeable and highly trusted system integrator.
Tampering	Integrity	Modifying data	One application from domain B intercepts and modifies the data sent to or from another application. (Man in the middle attack)	The inter-domain communication is controlled by a MILS separation kernel which prevents any interceptions and ensures the integrity of the messages.

CITY UNIVERSITY LONDON

L1 gateway sketch



CITY UNIVERSITY LONDON

L2 – implementation level

At this level we develop a detailed CAE structure to explain the behaviour of the specific components. This involves:

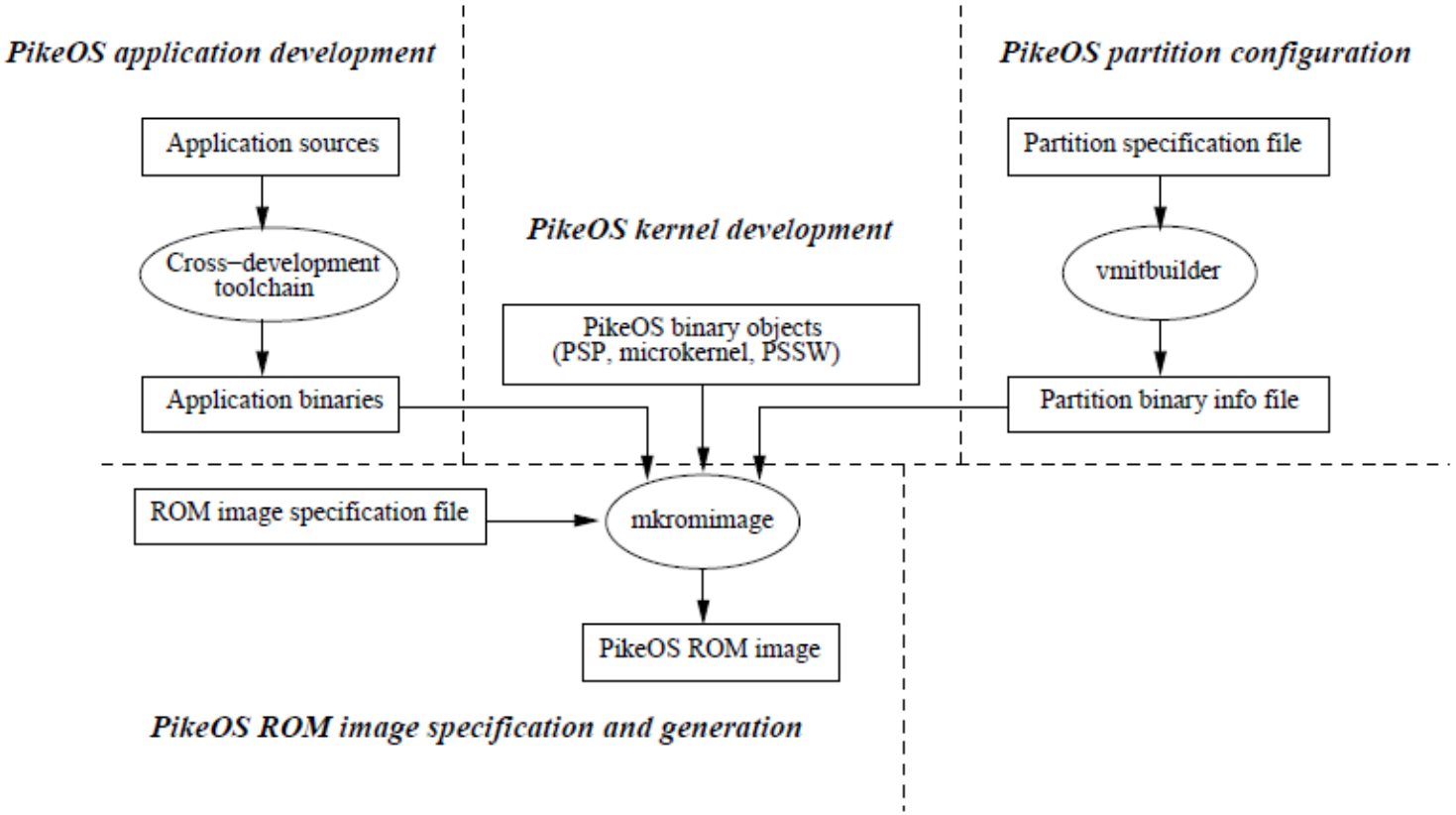
- Using the output from the L1 level of abstraction;
- Analysing the implementation details of every critical component;
- Creating an argument structure and elaborating the evidence to show that all the critical properties of the system are enforced;
- Documenting the results and providing traceability to the appropriate L0 and L1 security-informed safety case elements;

The case created at L2 level of abstraction is based on two types of technical information:

- General technical information produced and supplied with the components as part of the normal development process;
- Context-specific technical details derived from the analysis of the specific system implementation

CITY UNIVERSITY LONDON

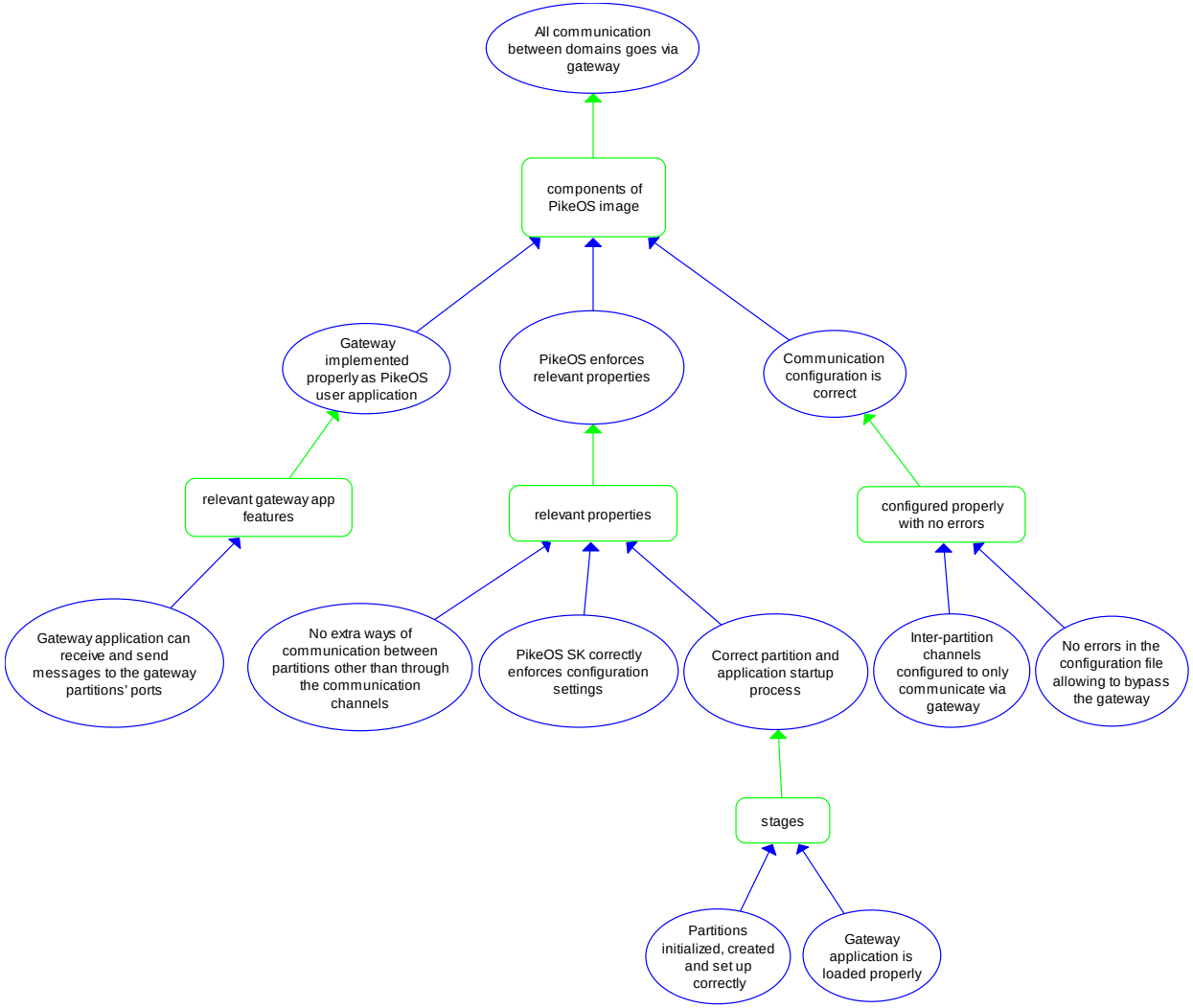
PikeOS development & configuration *



* SYSGO AG, Using PikeOS, v3.4, 2014

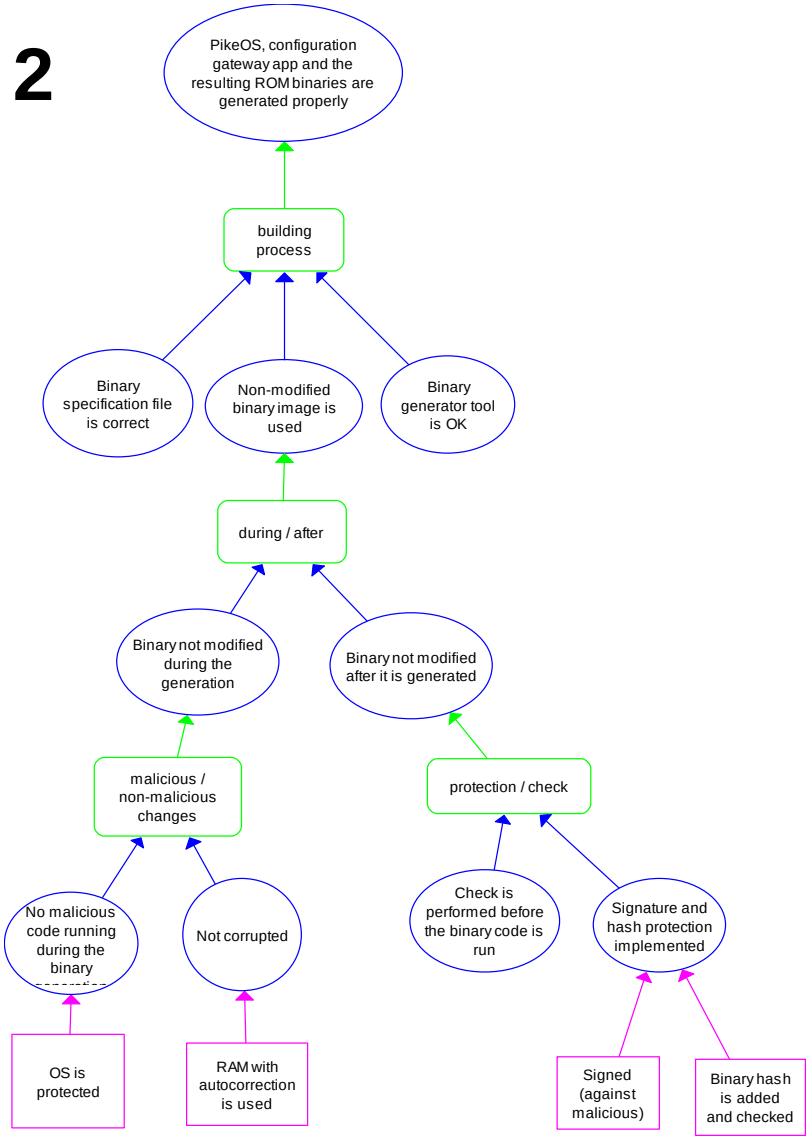
CITY UNIVERSITY LONDON

L2 gateway fragment 1



CITY UNIVERSITY LONDON

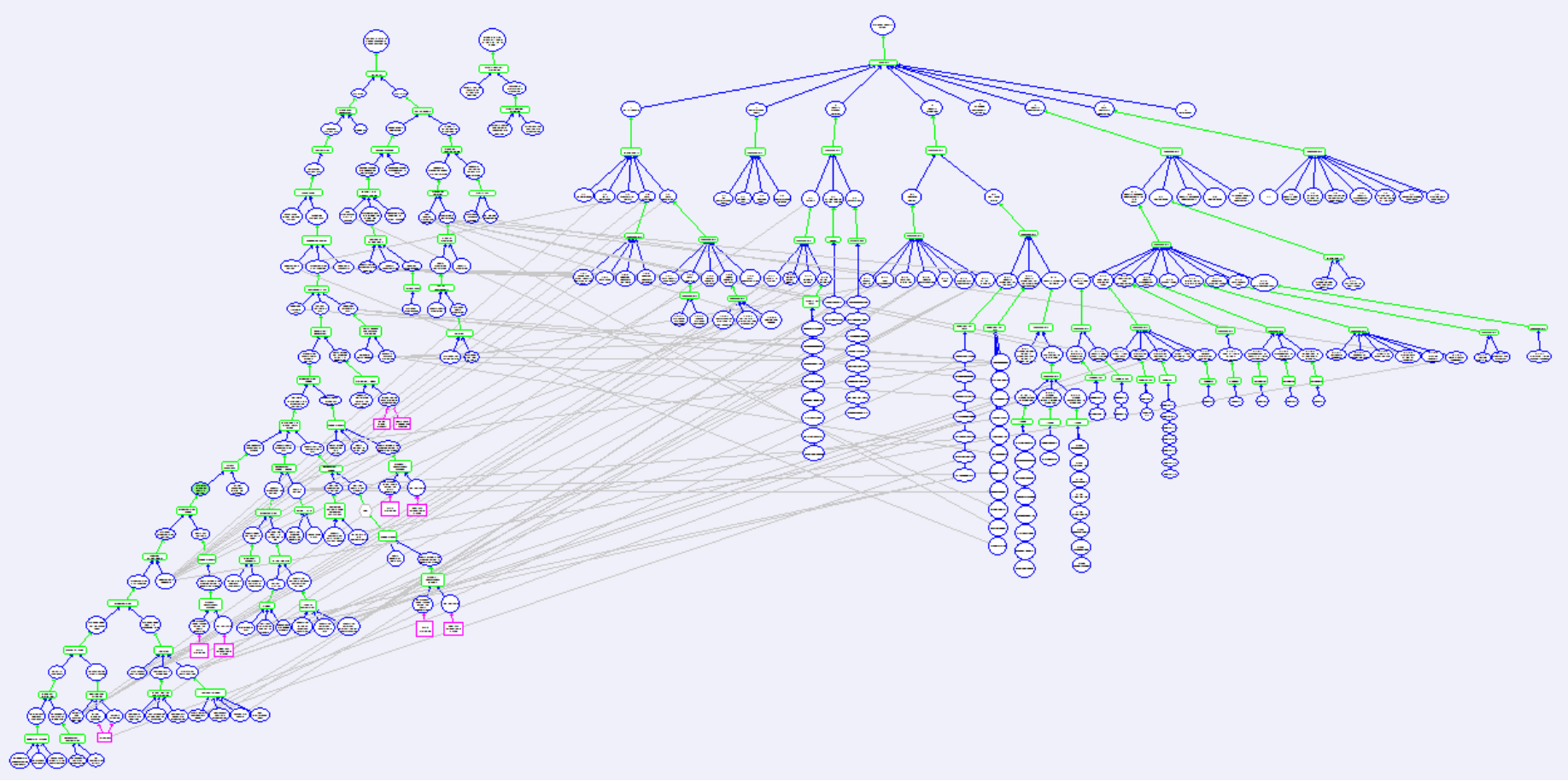
L2 gateway fragment 2



CITY UNIVERSITY LONDON

EST 1894

L2 gateway sketch linked to Security Target



CITY UNIVERSITY LONDON

Discussions and next steps

General directions:

- Integrated security and safety process
- Impact of security on safety cases
- Safety case perspective in avionics

Some issues of Layered Assurance:

- Compositionality and composability
  - Topology, CAE structure
  - CAE Building Blocks
- Incremental certification and polymorphism
  - Impact analysis of changes on the assurance: revisiting aspects of CAE, change cases
- Abstraction layers
  - Three levels of abstraction, can be deployed recursively
  - Divide and conquer approach with different focus, lower risks

Additional research:

- Formalisation of reasoning within cases, linkage to formal models
- CAE building blocks tool support
- Further mapping to Common Criteria, other approaches

Anything else? Suggestions welcome!

CITY UNIVERSITY LONDON

EST 1894

Thank you for your attention! ☺