SECURE SYSTEM ARCHITECTURES BY SPECIFICATION & ANALYSIS

HIBA HNAINI

DIRECTOR: RAÙL MAZO

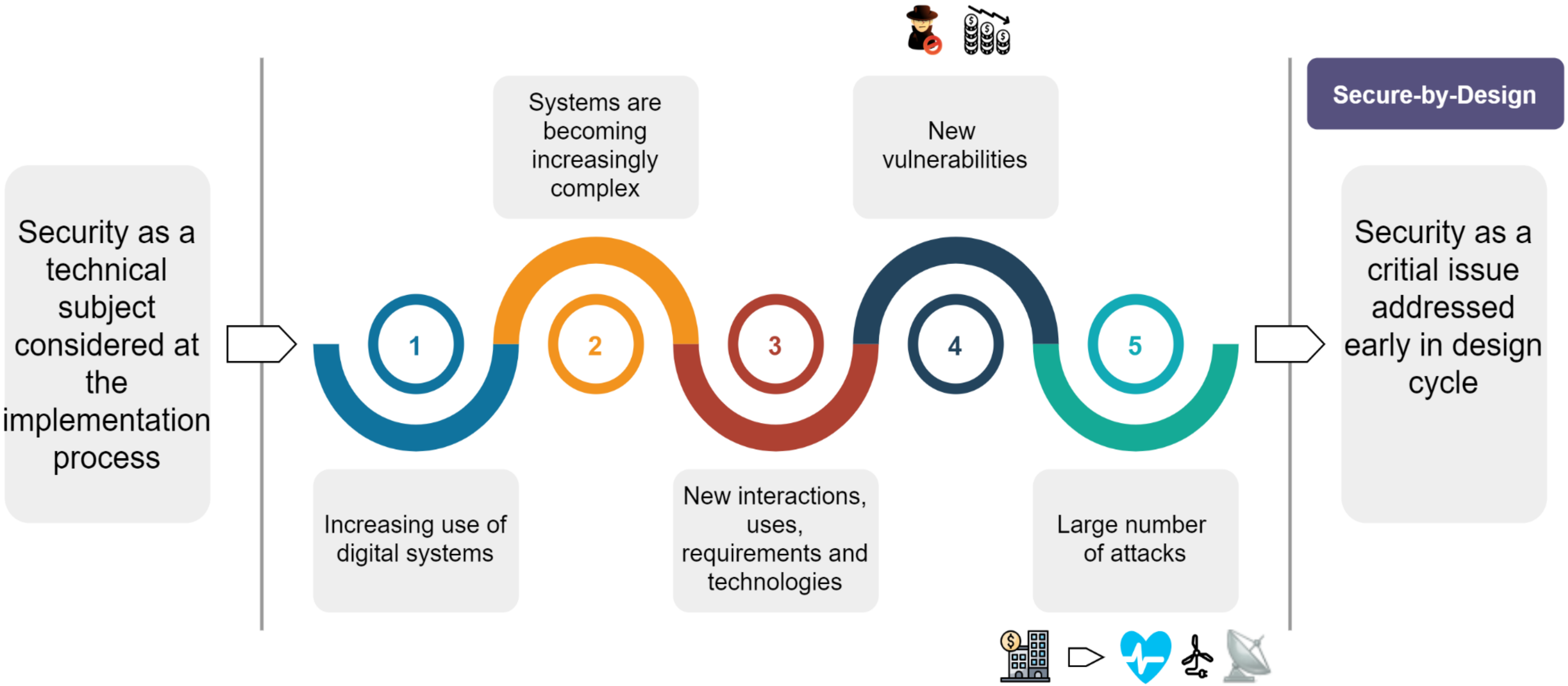
SUPERVISORS: PAOLA VALLEJO & JOËL CHAMPEAU

HIBA.HNAINI@ENSTA-BRETAGNE.ORG

OBJECTIVE

- Security modeling approach
  - **Requirements specification**, **formalization** and **analysis** of secure system architectures at **domain and application levels.**
  - **Define** and **evaluate** a new multi-paradigm approach
  - Provide an engineering framework (engineering process and tooling) **based on the VariaMos tool.**

CONTEXT



Security as a technical subject considered at the implementation process

1 Increasing use of digital systems

2 Systems are becoming increasingly complex

3 New interactions, uses, requirements and technologies

4 New vulnerabilities

5 Large number of attacks

Secure-by-Design

Security as a critial issue addressed early in design cycle

INNOVATIVE NATURE OF THE PROJECT

Design secure systems using a unified framework (Specification, Modeling, and Analysis), with quantitative analysis

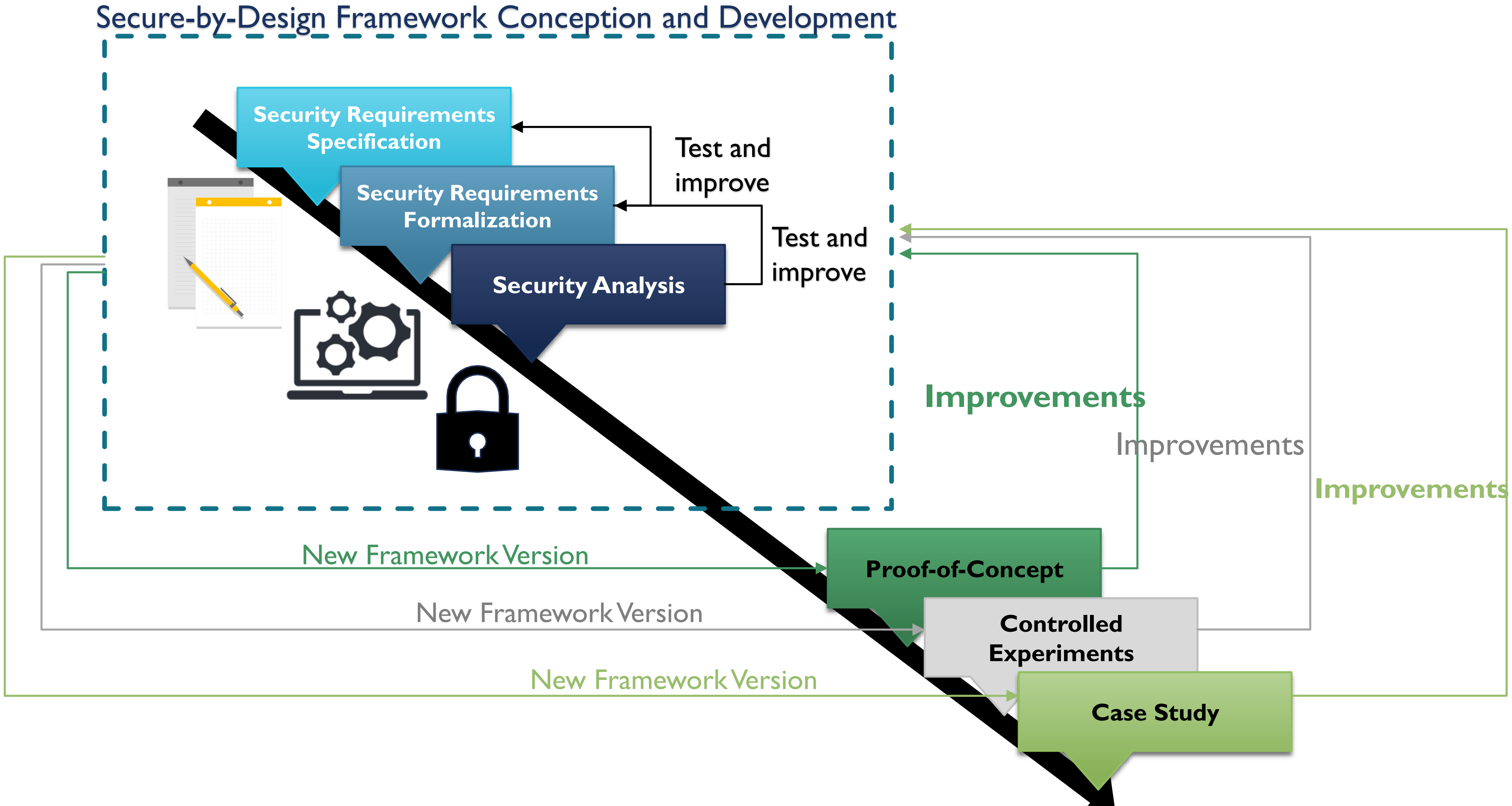
Problems

- The path to designing secure systems is long.
- Need for federated approach (Different levels of abstraction and viewpoints)
- No unifying framework for the multiple languages
- Technology transfer has a significantly lower efficiency outside limited test facilities

Solutions

- Using secure-by-design (early stages)
- Going beyond a simple mix of solutions & using different modeling and programming formalisms (Multiparadigm)
- Ensuring reusability of the approach (Separate between specification and analysis)
- Developing reference experiments to affirm the applicability and usefulness in real cases

METHODOLOGY - FRAMEWORK PRESENTATION



CHALLENGES ADDRESSED

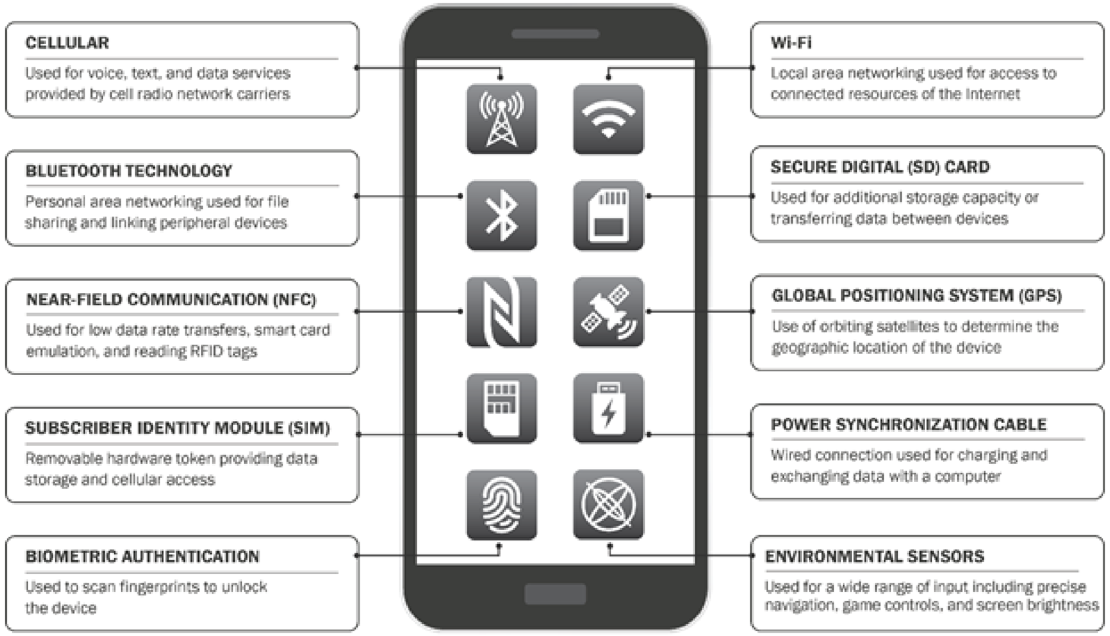
- How to express structured and non-complex security requirements while using natural language?
- What security requirements to specify and improve security coverage?
- How to formalize the security requirements with the lack of multiparadigm security modeling approaches?
- How to analyze the resulting formalized security requirements to reach the ultimate security level for the system?

OUTLINE

- Proof of Concept
- Background
  - Security Requirements Specification
  - Security Requirements Formalization
  - Security Analysis
- Our Approach
  - Security Requirements Specification
    - SECRET:Security Requirements Specification Template
    - SCORE: Security Criteria Ontology for REquiremenets Specification
    - SECRET & SCORE
  - Security Requirements Formalization
    - SERENA:SEcurity REquirements aNAlysis
  - Security Analysis
    - Constraint Programming
- Implementation
- Evaluation & Validation
- Conclusion
- Perspectives

PROOF OF CONCEPT – A SMART PHONE OR A FAMILY OF SMART PHONES

Security Criteria	Number of Requirements
Maintainability	2
Access Control	6
Integrity	2
Privacy	5
Authorization	1
Resilience to Attacks	3
Immunity	1
Availability	1
Confidentiality	4
Location Privacy	1



CELLULAR
Used for voice, text, and data services provided by cell radio network carriers

BLUETOOTH TECHNOLOGY
Personal area networking used for file sharing and linking peripheral devices

NEAR-FIELD COMMUNICATION (NFC)
Used for low data rate transfers, smart card emulation, and reading RFID tags

SUBSCRIBER IDENTITY MODULE (SIM)
Removable hardware token providing data storage and cellular access

BIOMETRIC AUTHENTICATION
Used to scan fingerprints to unlock the device

Wi-Fi
Local area networking used for access to connected resources of the Internet

SECURE DIGITAL (SD) CARD
Used for additional storage capacity or transferring data between devices

GLOBAL POSITIONING SYSTEM (GPS)
Use of orbiting satellites to determine the geographic location of the device

POWER SYNCHRONIZATION CABLE
Wired connection used for charging and exchanging data with a computer

ENVIRONMENTAL SENSORS
Used for a wide range of input including precise navigation, game controls, and screen brightness

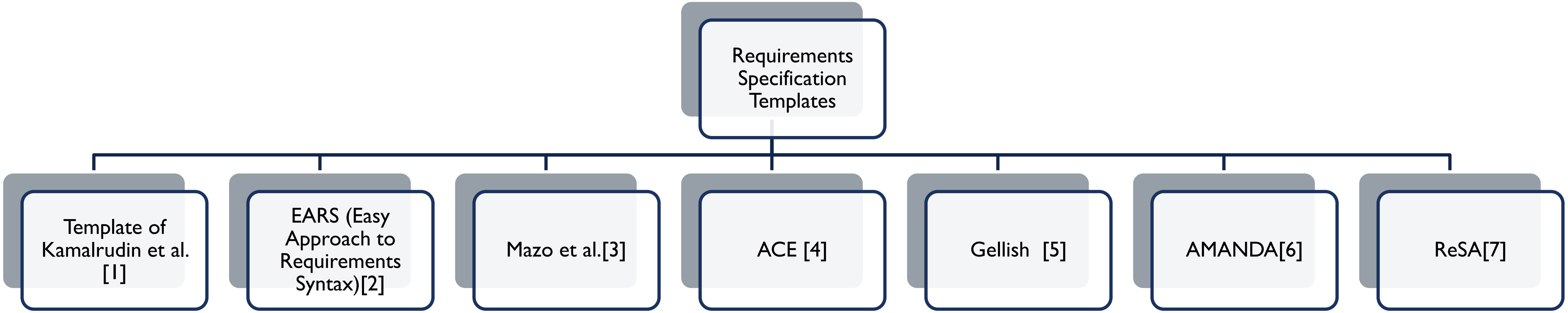
Requirements for OEM regarding Smartphone Security (bund.de):
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/requirements/Requirements-Smartphones.pdf?__blob=publicationFile&v=2

PROOF OF CONCEPT – A SMART PHONE OR A FAMILY OF SMART PHONES

The main security criteria	Confidentiality Integrity Privacy Availability
Requirements from the document	Req1: From the network perspective the use of the newest Radio Canal Ciphering Algorithms has very high priority Devices supporting these algorithms are better protected. Req2:The HSE must be used to store critical user data. Req3:All new devices must be provided with the latest OS available at release time.

BACKGROUND

SECURITY REQUIREMENTS SPECIFICATION



Requirements Specification Templates

Template of Kamalrudin et al. [1]

EARS (Easy Approach to Requirements Syntax)[2]

Mazo et al.[3]

ACE [4]

Gellish [5]

AMANDA[6]

ReSA[7]

[1] Kamalrudin, Massila & Mustafa, Nuridawati & Sidek, Safiah. (2018). A Template for Writing Security Requirements. 10.1007/978-981-10-7796-8_6.

[2] A. Mavin, P. Wilkinson, A. Harwood and M. Novak, "Easy Approach to Requirements Syntax (EARS)," 2009 17th IEEE International Requirements Engineering Conference, 2009, pp. 317-322, doi: 10.1109/RE.2009.9.

[3]] Mazo, Raúl & Jaramillo, Carlos & Vallejo, Paola & Medina, Jhon. (2020). Towards a new template for the specification of requirements in semi-structured natural language. Journal of Software Engineering Research and Development. 8. 3. 10.5753/jserd.2020.473.

[4] Fuchs, Norbert E., et Rolf. Schwitter. « Attempto Controlled English (ACE).» CLAW 96: proceedings of the First International Workshop on Controlled Language Applications. 1996.

[5] van Renssen, Andries. (2011). Modeling of Textual Requirements in a Gellish Universal Database.. 102-115.

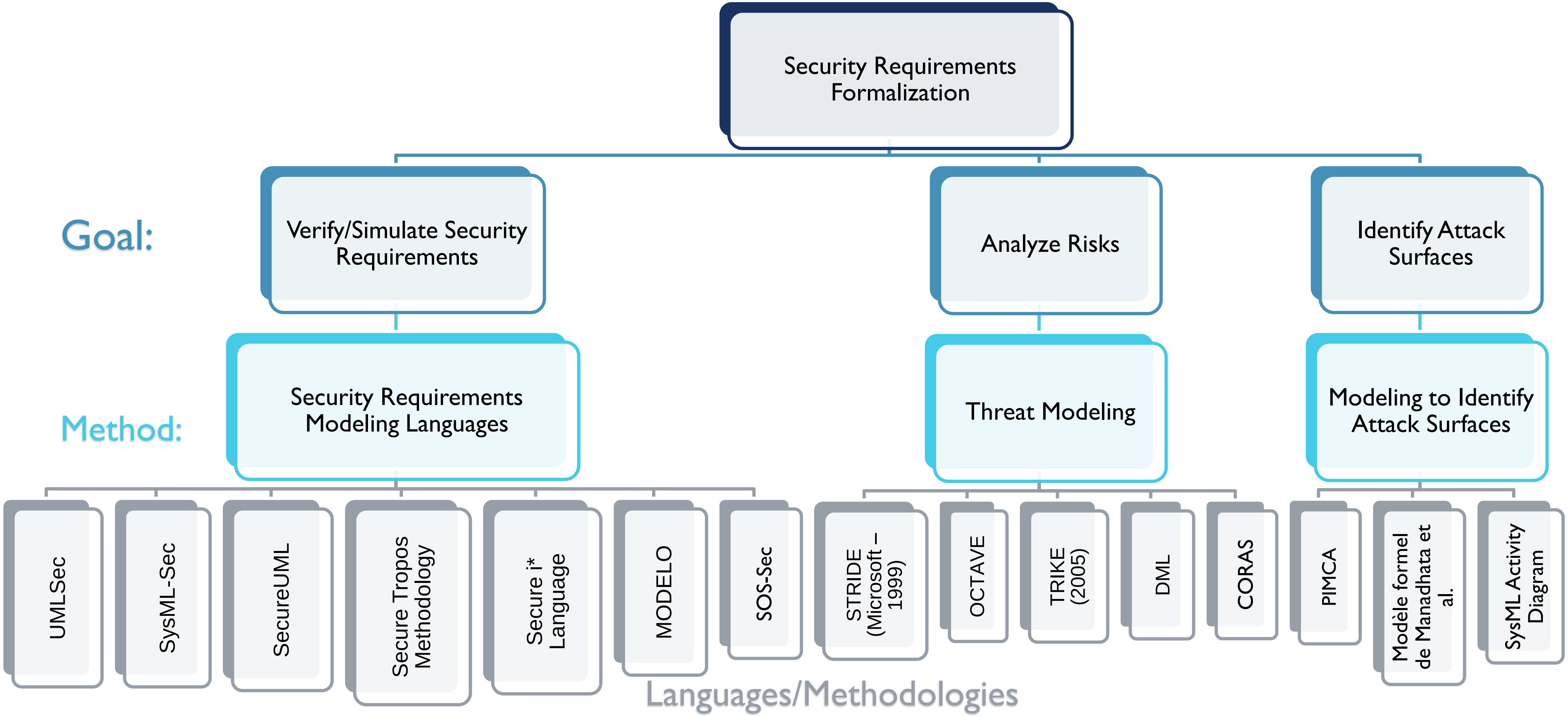
[6] Amina Souag. AMAN-DA: A knowledge reuse based approach for domain specific security requirements engineering. Other [cs.OH]. Université Paris 1 Panthéon Sorbonne, 2015. English. ⟨NNT : ⟩. ⟨tel-01302760⟩

[7] Mahmud, Nesredin & Seceleanu, Cristina & Ljungkrantz, Oscar. (2016). ReSA Tool: Structured Requirements Specification and SAT-based Consistency-checking. 1737-1746. 10.15439/2016F404.

SECURITY REQUIREMENTS SPECIFICATION

Template	Structured Natural Language	Security Criteria	Security Mechanism	Reduces Ambiguity, Complexity…	Applies To A Family Of Systems	Applies to auto adaptive systems
Template Of Kamalrudin Et Al.	x		x	x		
EARS (Easy Approach To Requirements Syntax)	x			x		
New Template For The Specification Of Requirements	x			x	x	x
ACE	x			x	x	
EARS	x			x		
AMANDA	x	x		x		
ReSA	x			x		

SECURITY REQUIREMENTS FORMALIZATION



Security Requirements Formalization

Goal:

Verify/Simulate Security Requirements

Analyze Risks

Identify Attack Surfaces

Method:

Security Requirements Modeling Languages

Threat Modeling

Modeling to Identify Attack Surfaces

UMLSec

SysML-Sec

SecureUML

Secure Tropos Methodology

Secure i* Language

MODELO

SOS-Sec

STRIDE (Microsoft – 1999)

OCTAVE

TRIKE (2005)

DML

CORAS

PIMCA

Modèle formel de Manadhata et al.

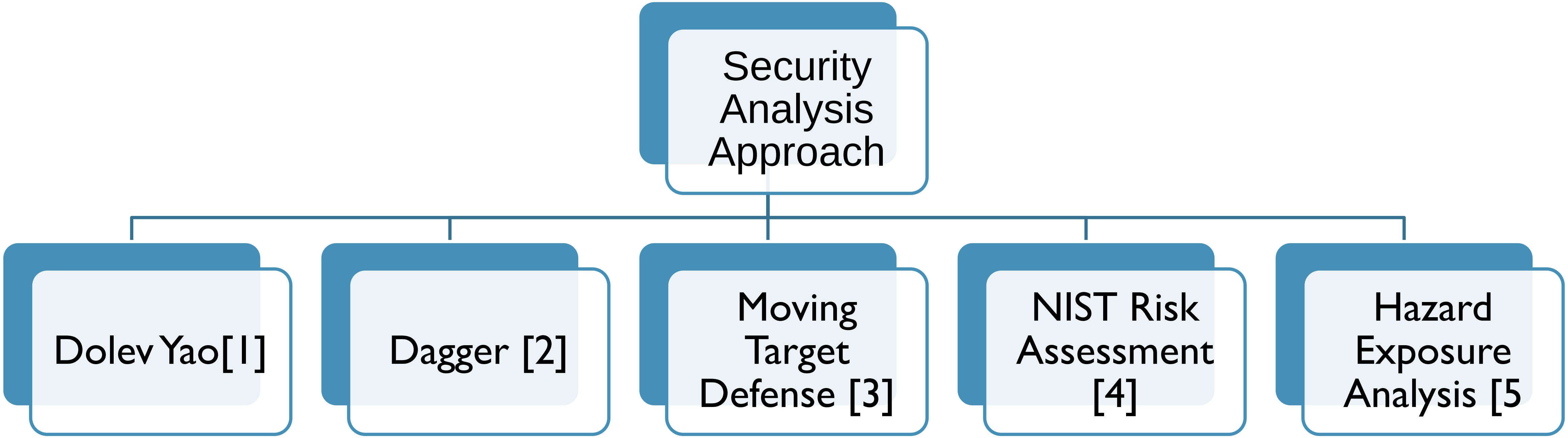
SysML Activity Diagram

Languages/Methodologies

SECURITY REQUIREMENTS FORMALIZATION

Language	Tool	Security Criteria	Security Mechanism	Enough to represent a requirement using the template	Applicable to a family of systems	Applicable to auto-adaptive systems
STRIDE	Microsoft Threat Modeling Tool	6 security criteria(Authentication, Integrity, Non-repudiation, Confidentiality, Availability, Authorization)	No	No	No	No
OCTAVE	-	Yes	Yes	Yes	No	No
TRIKE	Excel Sheet	No	No	No	No	No
DML	-	-	-	-	No	No
CORAS	Coras	No	Yes	No	No	No

SECURITY ANALYSIS



Security Analysis Approach

Dolev Yao[1]

Dagger [2]

Moving Target Defense [3]

NIST Risk Assessment [4]

Hazard Exposure Analysis [5

[1]Cervesato, Iliano. (2001). The Dolev-Yao Intruder is the Most Powerful Attacker
[2]Peterson, Elisha. (2016). Dagger: Modeling and visualization for mission impact situation awareness. 25-30. 10.1109/MILCOM.2016.7795296.
[3]Lei, Cheng & Zhang, Hong-Qi & Jinglei, Tan & Zhang, Yu-Chen & Liu, Xiao-Hu. (2018). Moving Target Defense Techniques: A Survey. Security and Communication Networks. 2018. 1-25. 10.1155/2018/3759626.
[4] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
[5] https://www.cisa.gov/sites/default/files/publications/Risk%2520Assessment%2520Methodologies.pdf

SECURITY ANALYSIS

Method	Tool	Targets	Can be applied
Dolev-Yao	ProVerif	Ciphering Protocols	Yes
Dagger	-	Network Security	-
MTD	-	Network Security	-
NIST	-	Systems	Yes
Hazard Exposure Analysis	-	Systems	Yes

BACKGROUND ANALYSIS

	Suitable approach
Requirements Specification	New Template For The Specification Of Requirements
Requirements Formalization	Secure Tropos, Secure i*, CORAS, (Soyer et al.)
Security Analysis	NIST Risk Assesment, Hazard Exposure Analysis

OUR APPROACH

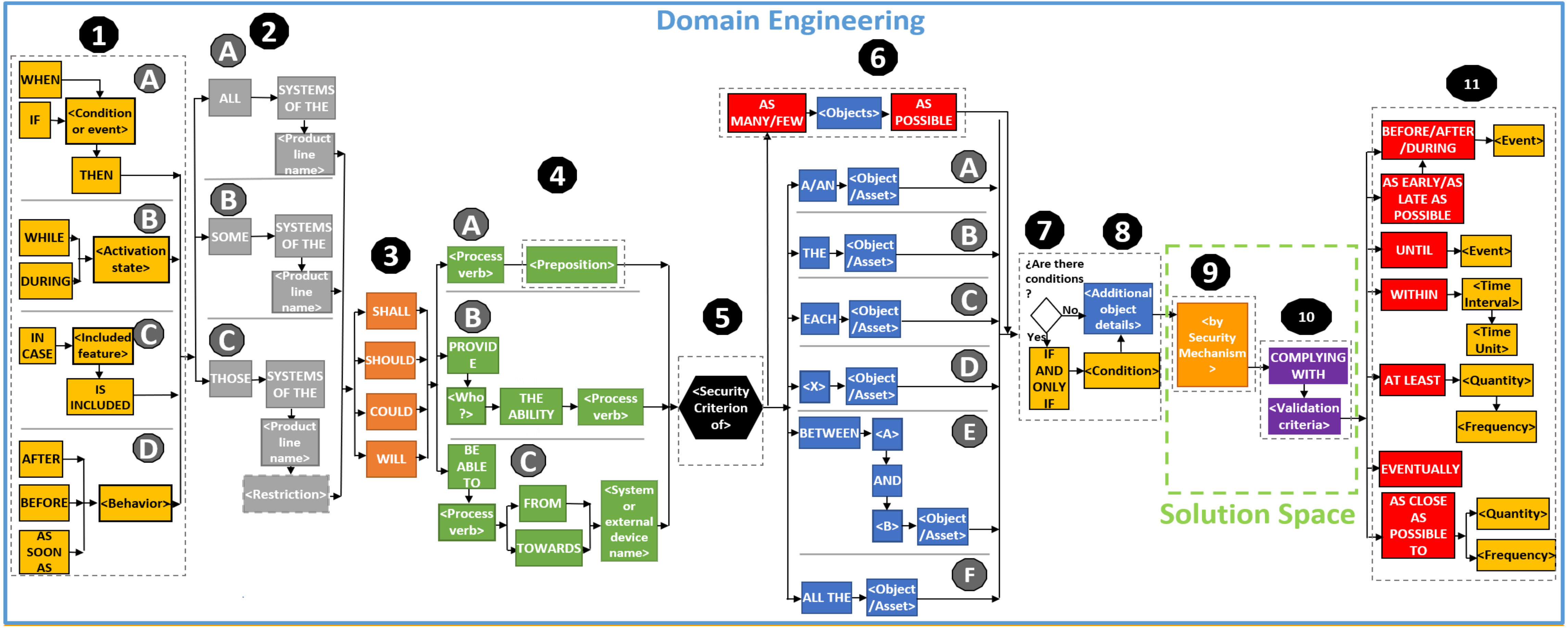
PROOF OF CONCEPT

HOW TO SPECIFY CLEAR AND NON-COMPLEX SECURITY REQUIREMENTS FOR SYSTEMS AND DOMAINS?

WHY USE A TEMPLATE (MAZO EL AL.)?

- Semi-structured natural language – No need to learn new specification languages
- Adapted for family of systems or product lines (domain level)
- Considers auto-adaptive systems
- Reduces ambiguity and complexity
- Easily adapted to security by adding security concepts (security criteria & security mechanisms)

SECRET: SECURITY REQUIREMENTS SPECIFICATION TEMPLATE



Domain Engineering

1
A
WHEN
IF
<Condition or event>
THEN
B
WHILE
DURING
<Activation state>
C
IN CASE
<Included feature>
IS INCLUDED
D
AFTER
BEFORE
AS SOON AS
<Behavior>

2
A
ALL
SYSTEMS OF THE
<Product line name>
B
SOME
SYSTEMS OF THE
<Product line name>
C
THOSE
SYSTEMS OF THE
<Product line name>
<Restriction>

3
SHALL
SHOULD
COULD
WILL

4
A
<Process verb>
<Preposition>
B
PROVIDE
<Who ?>
THE ABILITY
<Process verb>
C
BE ABLE TO
<Process verb>
FROM
TOWARDS
<System or external device name>

5
<Security Criterion of>

6
AS MANY/FEW
<Objects>
AS POSSIBLE
A
A/AN
<Object /Asset>
B
THE
<Object /Asset>
C
EACH
<Object /Asset>
D
<X>
<Object /Asset>
E
BETWEEN
<A>
AND
<B>
<Object /Asset>
F
ALL THE
<Object /Asset>

7
¿Are there conditions ?
No
Yes
IF AND ONLY IF

8
<Additional object details>
<Condition>

9
<by Security Mechanism >

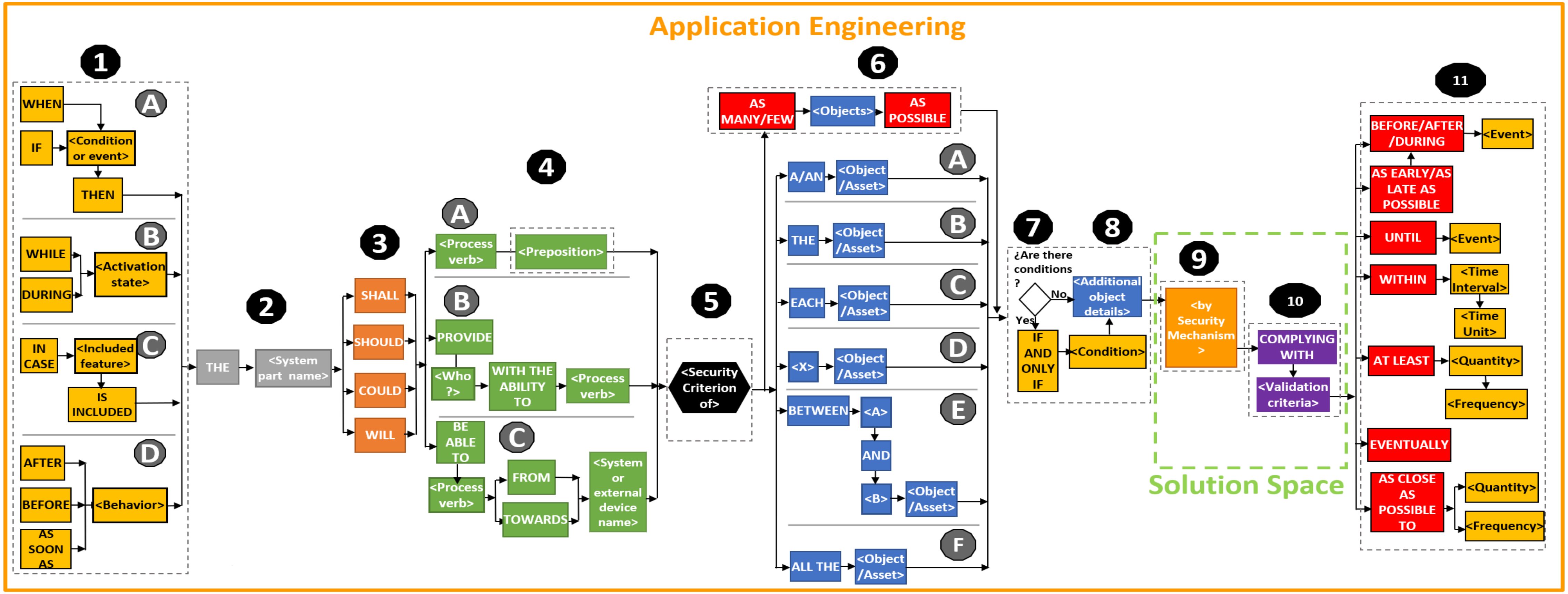
10
COMPLYING WITH
<Validation criteria>

Solution Space

11
BEFORE/AFTER /DURING
<Event>
AS EARLY/AS LATE AS POSSIBLE
UNTIL
<Event>
WITHIN
<Time Interval>
<Time Unit>
AT LEAST
<Quantity>
<Frequency>
EVENTUALLY
AS CLOSE AS POSSIBLE TO
<Quantity>
<Frequency>

Hnaini, H., Mazo, R., Vallejo, P., Lopez, A., Champeau, J., Galindo, J. (2024). SECRET: A New SECurity REquirements SpecificaTion Template. In: Rocha, Á., Ferrás, C., Hochstetter Diez, J., Diéguez Rebolledo, M. (eds) Information Technology and Systems. ICITS 2024. Lecture Notes in Networks and Systems, vol 933. Springer, Cham. https://doi.org/10.1007/978-3-031-54256-5_22

SECRET: SECURITY REQUIREMENTS SPECIFICATION TEMPLATE



Application Engineering

1

A
WHEN
IF
<Condition or event>
THEN

B
WHILE
DURING
<Activation state>

C
IN CASE
<Included feature>
IS INCLUDED

D
AFTER
BEFORE
AS SOON AS
<Behavior>

2
THE
<System part name>

3
SHALL
SHOULD
COULD
WILL

4

A
<Process verb>
<Preposition>

B
PROVIDE
<Who ?>
WITH THE ABILITY TO
<Process verb>

C
BE ABLE TO
<Process verb>
FROM
TOWARDS
<System or external device name>

5
<Security Criterion of>

6
AS MANY/FEW
<Objects>
AS POSSIBLE

A
A/AN
<Object /Asset>

B
THE
<Object /Asset>

C
EACH
<Object /Asset>

D
<X>
<Object /Asset>

E
BETWEEN
<A>
AND
<B>
<Object /Asset>

F
ALL THE
<Object /Asset>

7
¿Are there conditions ?
No
Yes
IF AND ONLY IF

8
<Additional object details>
<Condition>

9
<by Security Mechanism >

10
COMPLYING WITH
<Validation criteria>

Solution Space

11
BEFORE/AFTER /DURING
<Event>
AS EARLY/AS LATE AS POSSIBLE
UNTIL
<Event>
WITHIN
<Time Interval>
<Time Unit>
AT LEAST
<Quantity>
<Frequency>
EVENTUALLY
AS CLOSE AS POSSIBLE TO
<Quantity>
<Frequency>

Legend: Optional ● Section ● Sub-Section

SECRET: SECURITY REQUIREMENTS SPECIFICATION TEMPLATE

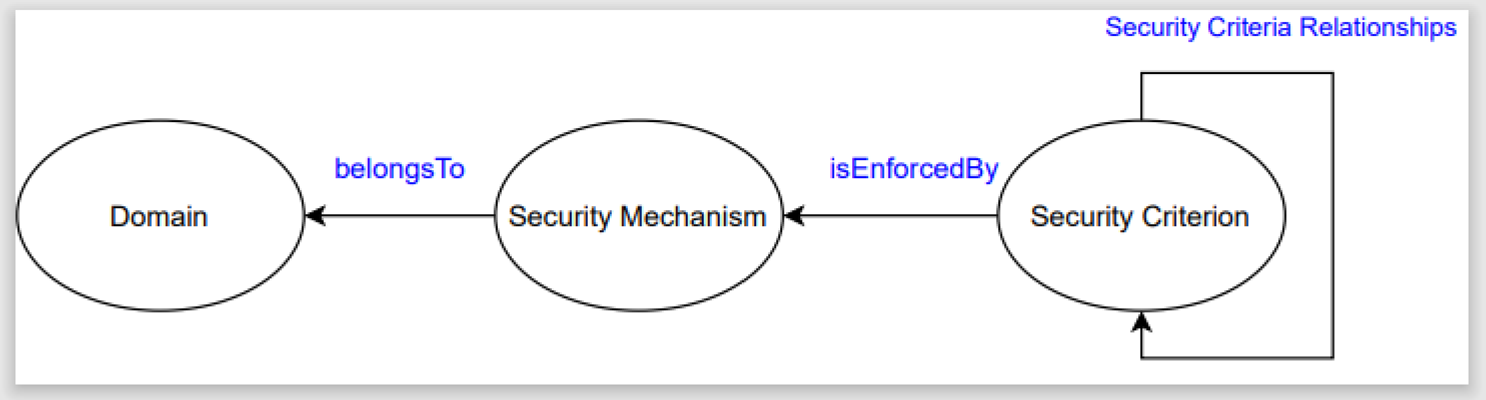
ID	DESCRIPTION
REQ1	The <Cellular Interface> system or system part <should> priority <ensure> process verb <confidentiality> security criteria of <the data> asset to protect <by Radio Canal Ciphering Algorithms> security mechanism
REQ3	All <new devices of the smartphones product line> system or system part <should> priority <ensure> process verb <integrity> security criteria of <the data> asset to protect <by storing security critical data> security mechanism

HOW TO IMPROVE THE SECURITY REQUIREMENTS COVERAGE IN THE SYSTEM(S)?

HOW TO IMPROVE SECURITY

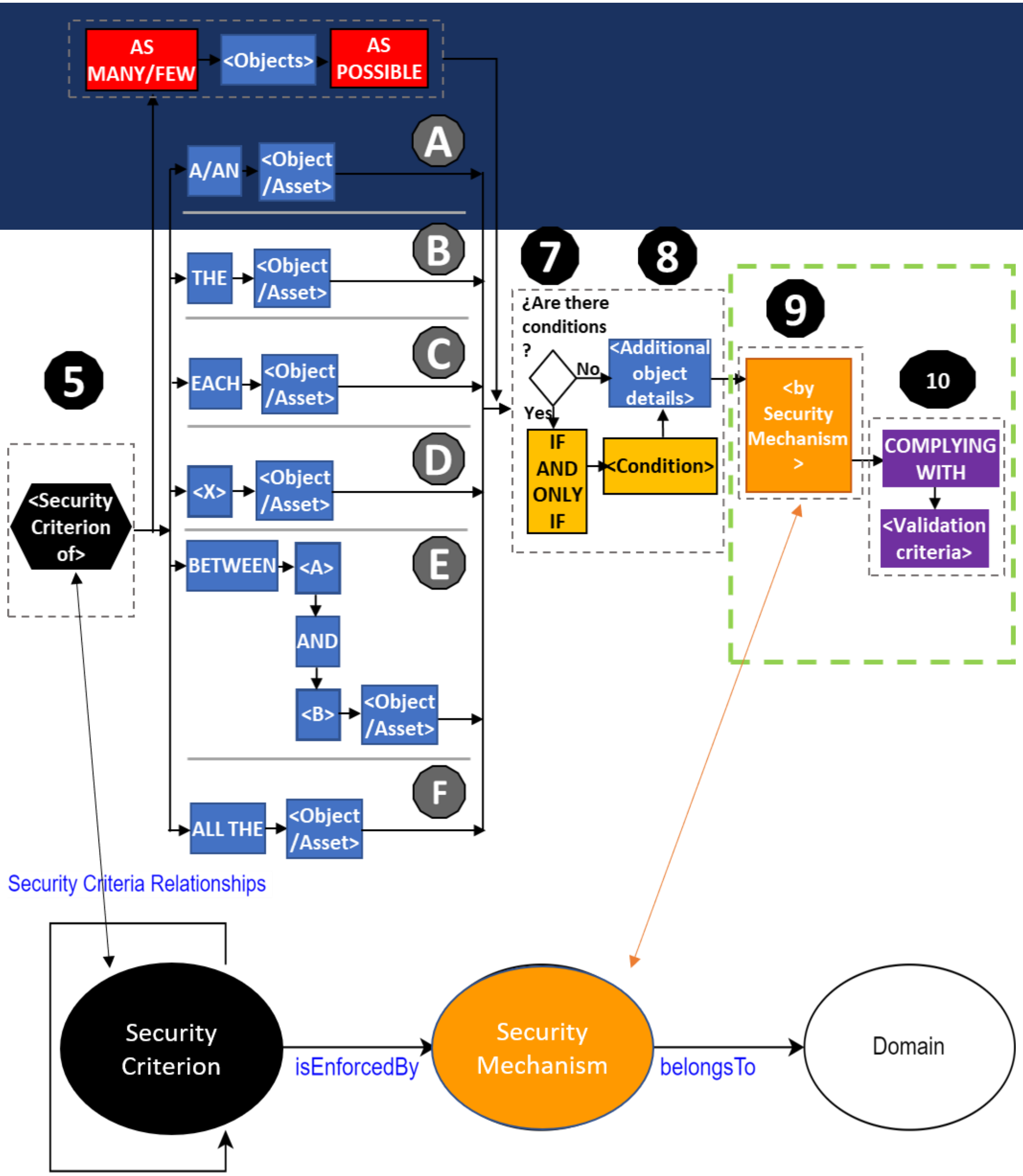
- Use an ontology that links the security criterion, security mechanism, and domain concepts.

- Suggest security mechanisms and security criteria according to a chosen domain
- Use the relationships between security criteria to suggest additional security criteria to improve security coverage

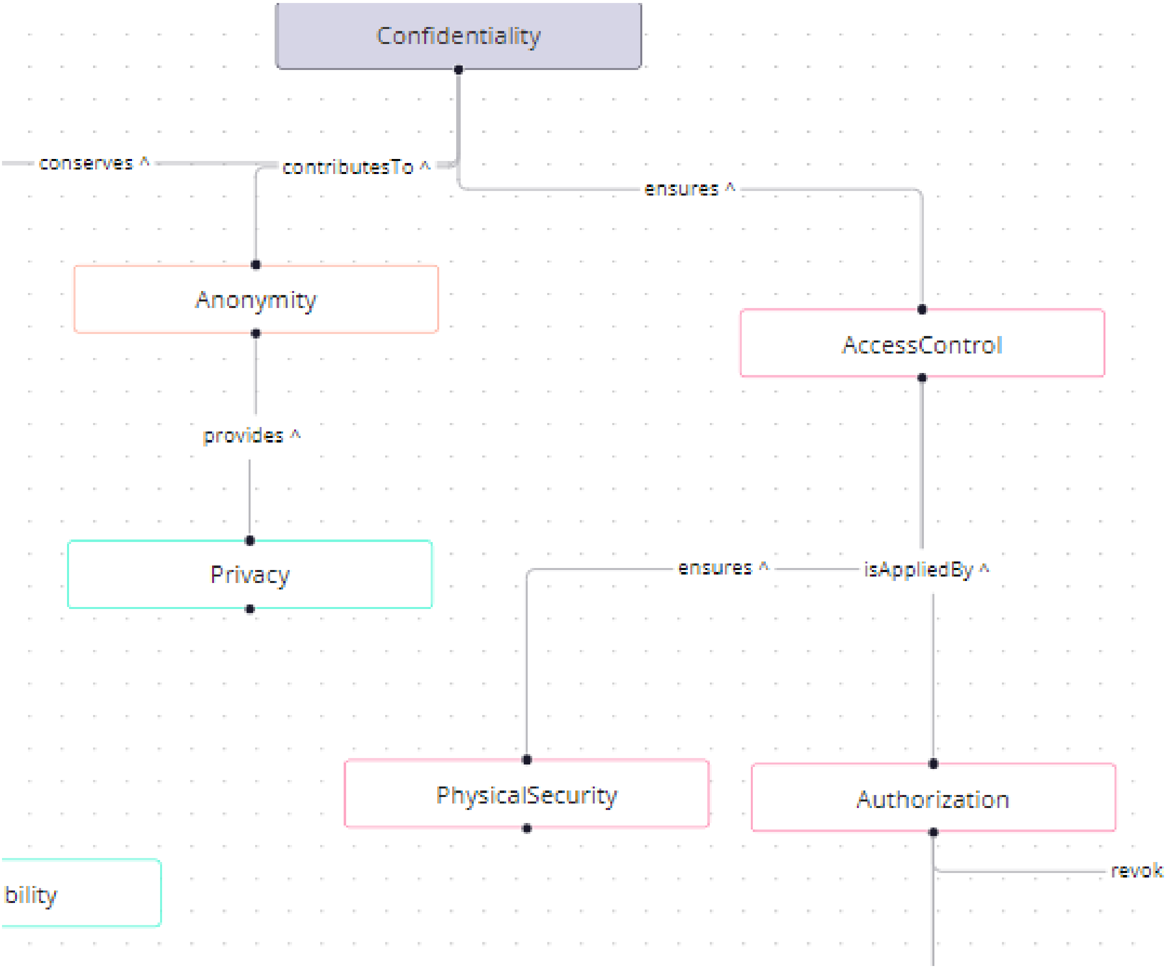


SECRET – SCORE (I)

REQ1 .The <Cellular Interface>system or system part <should>priority <ensure>process verb <confidentiality>security criteria of <the data> asset to protect <by Radio Canal Ciphering Algorithms>security mechanism



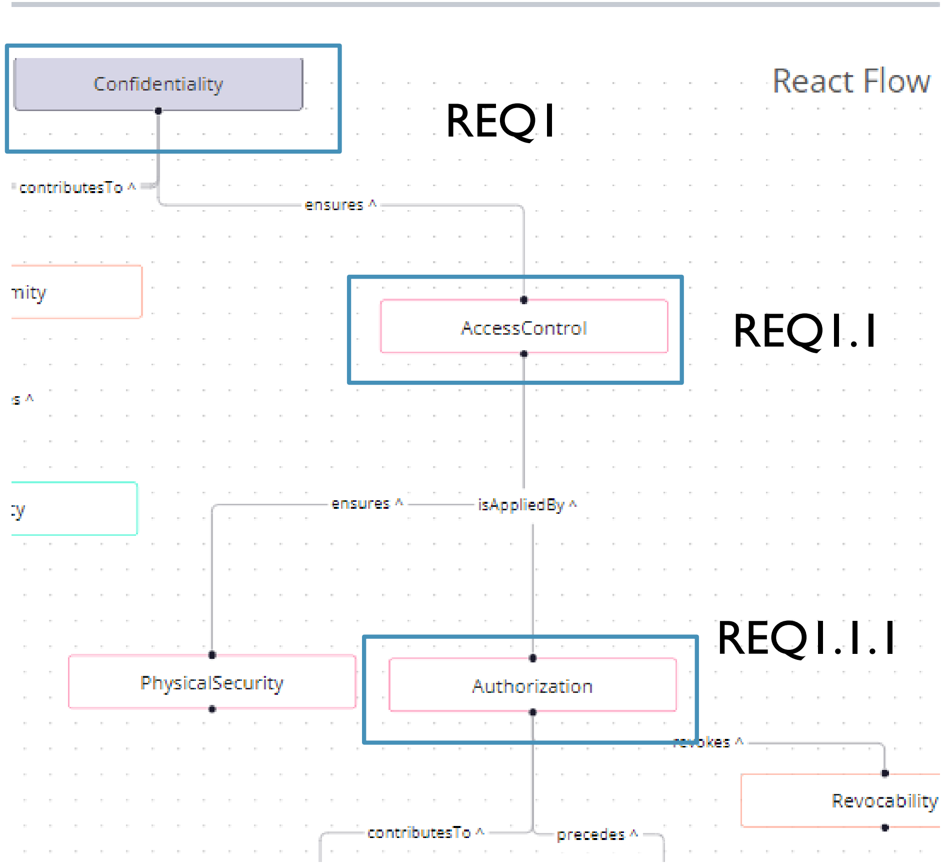
SCORE: SECURITY CRITERIA ONTOLOGY FOR REQUIREMENETS SPECIFICATION



- Additional security criteria for confidentiality in the smartphones domain

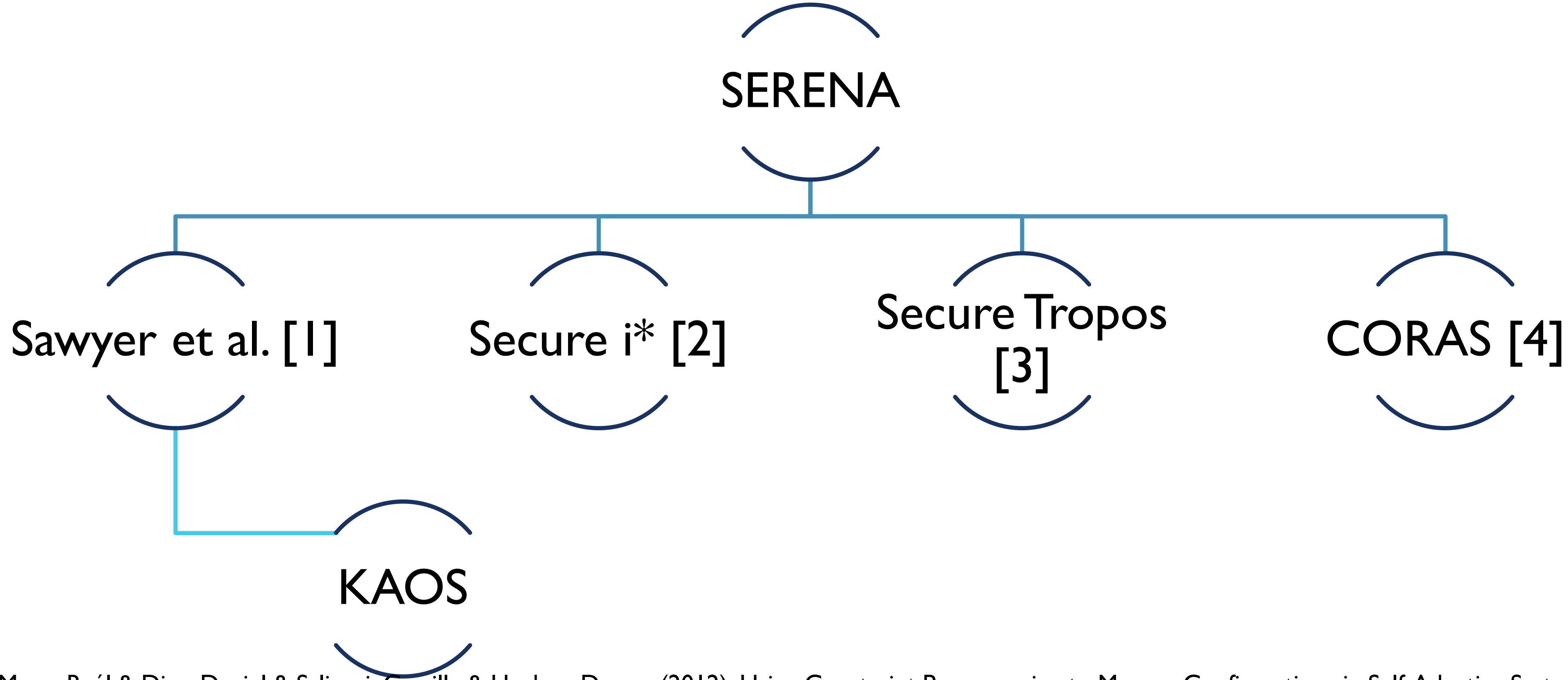
SECRET – SCORE (2)

ID	DESCRIPTION
REQ 1	The <Cellular Interface>$_{\text{system or system part}}$ <should>$_{\text{priority}}$ <ensure>$_{\text{process verb}}$ **<confidentiality>**$_{\text{security criteria}}$ of <the data> $_{\text{asset to protect}}$ <by Radio Canal Ciphering Algorithms>$_{\text{security mechanism}}$
REQ 1.1	The <Cellular Interface>$_{\text{system or system part}}$ <should>$_{\text{priority}}$ <ensure>$_{\text{process verb}}$ **<access control>**$_{\text{security criteria}}$ of <the data> $_{\text{asset to protect}}$ <…..>$_{\text{security mechanism}}$
REQ 1.1.1	Req1.2:The <Cellular Interface>$_{\text{system or system part}}$ <should>$_{\text{priority}}$ <ensure>$_{\text{process verb}}$ **<authorization>**$_{\text{security criteria}}$ of <the users> $_{\text{asset to protect}}$ <…..>$_{\text{security mechanism}}$



HOW TO FORMALIZE THE REQUIREMENTS FOR ANALYSIS?

SERENA: SECURITY REQUIREMENTS ANALYSIS



[1] Sawyer, Peter & Mazo, Raúl & Diaz, Daniel & Salinesi, Camille & Hughes, Danny. (2012). Using Constraint Programming to Manage Configurations in Self-Adaptive Systems. IEEE Computer Journal (cover feature). 45. 10.1109/MC.2012.286.

[2] Liu L, Yu E, Mylopoulos J (2002) Analyzing security requirements as relationships among strategic actors. In: Proceedings of the 2nd symposium on requirements engineering for information security

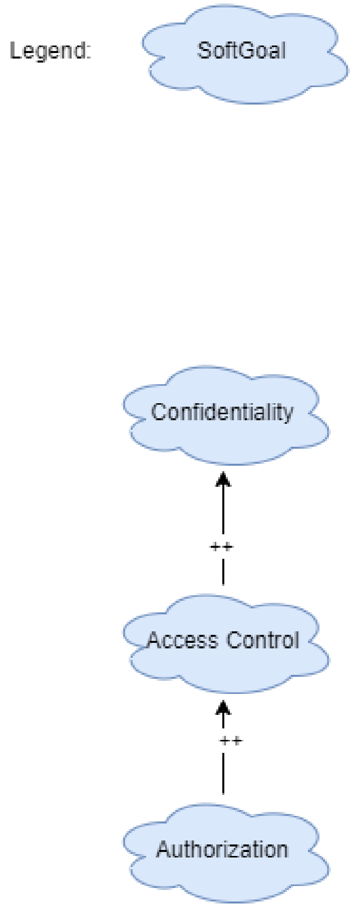
[3] Mouratidis, H. and Giorgini, P., 2007. Secure tropos: a security-oriented extension of the tropos methodology. International Journal of Software Engineering and Knowledge Engineering, 17(02), pp.285-309.

[4] Fredriksen, Rune & Kristiansen, Monica & Gran, Bjørn & Stølen, Ketil & Opperud, Tom & Dimitrakos, Theo. (2002). The CORAS Framework for a Model-Based Risk Management Process. 94-105. 10.1007/3-540-45732-1_11. [5] van Renssen, Andries. (2011). Modeling of Textual Requirements in a Gellish Universal Database.. 102-115.

SERENA: SECURITY REQUIREMENTS ANALYSIS

- Created based on Sawyer et al. (based on KAOS) with security concepts from Secure i* and SecureTropos
- Objectives:
  - Formal Representation of Security Requirements
  - Semantic Analysis of Security Requirements
  - Support for Security by Design Principles
- Multi-paradigm: Five views with different objectives

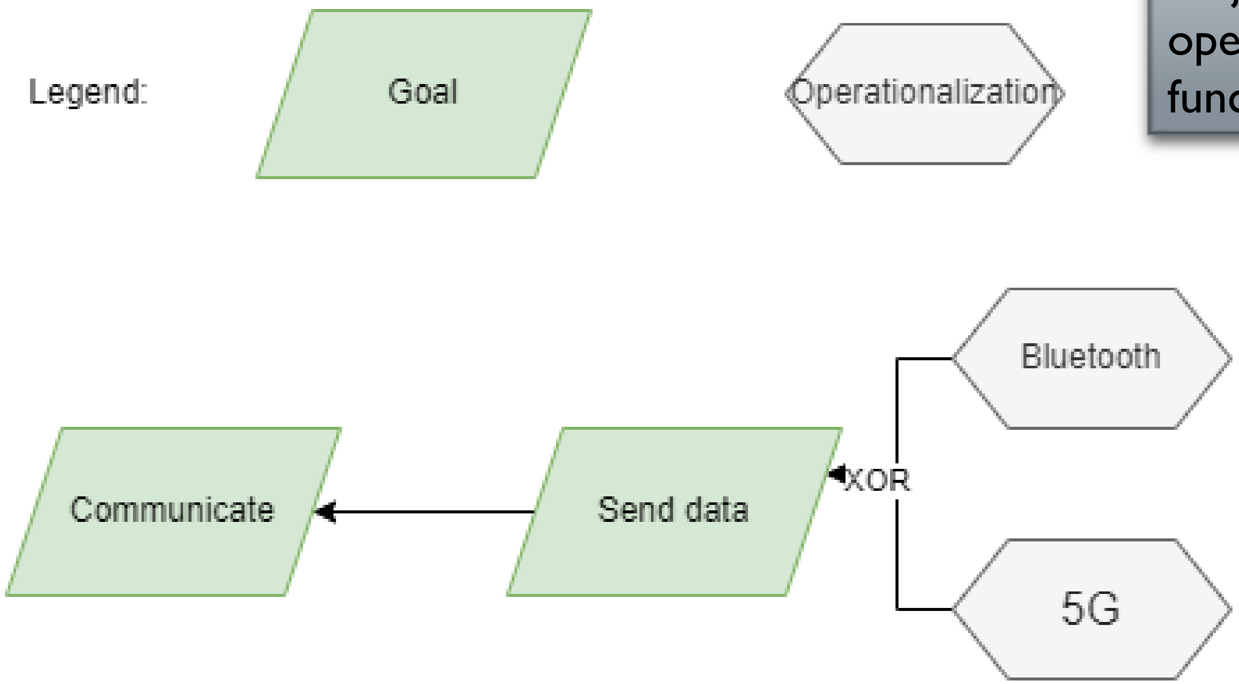
SERENA: SECURITY REQUIREMENTS ANALYSIS SECURITY CRITERIA MODEL



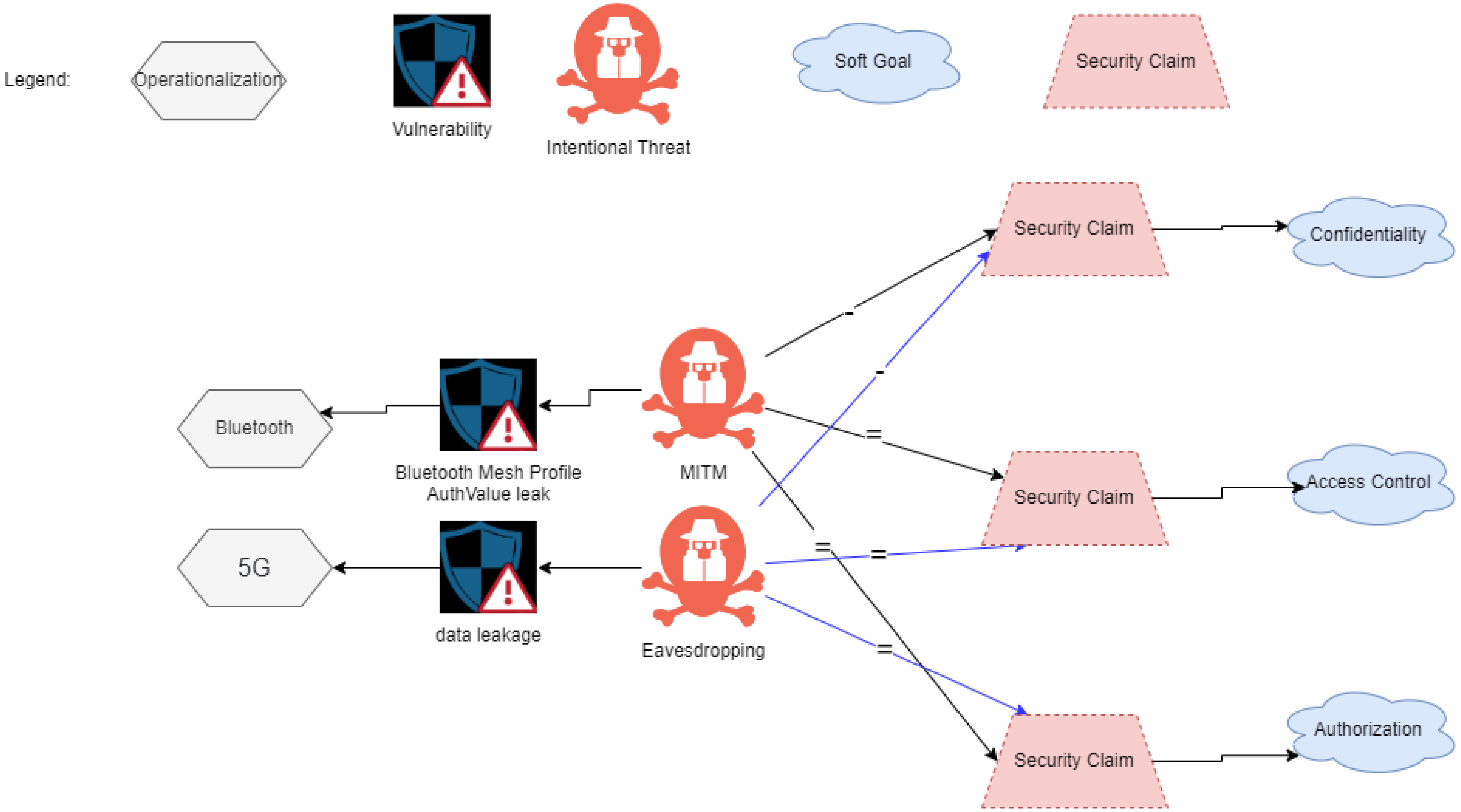
Objective: Security criteria analysis against the SCORE ontology

SERENA: SECURITY REQUIREMENTS ANALYSIS GOAL MODEL

Objective: Specify the operationalizations for each functional goal



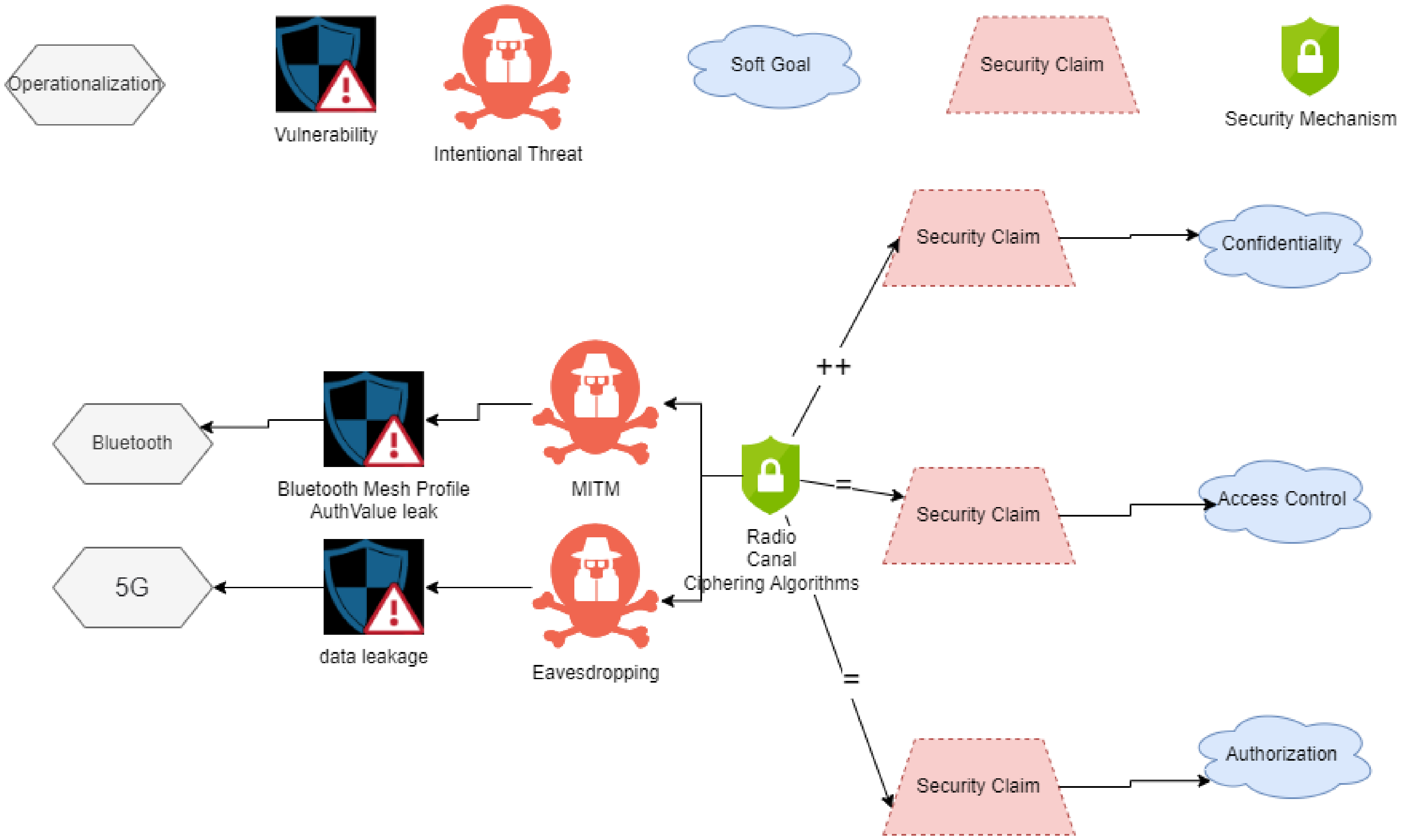
SERENA: SECURITY REQUIREMENTS ANALYSIS RISK MODEL



Objective: Risk Assessment between the operationlizations and the security criteria

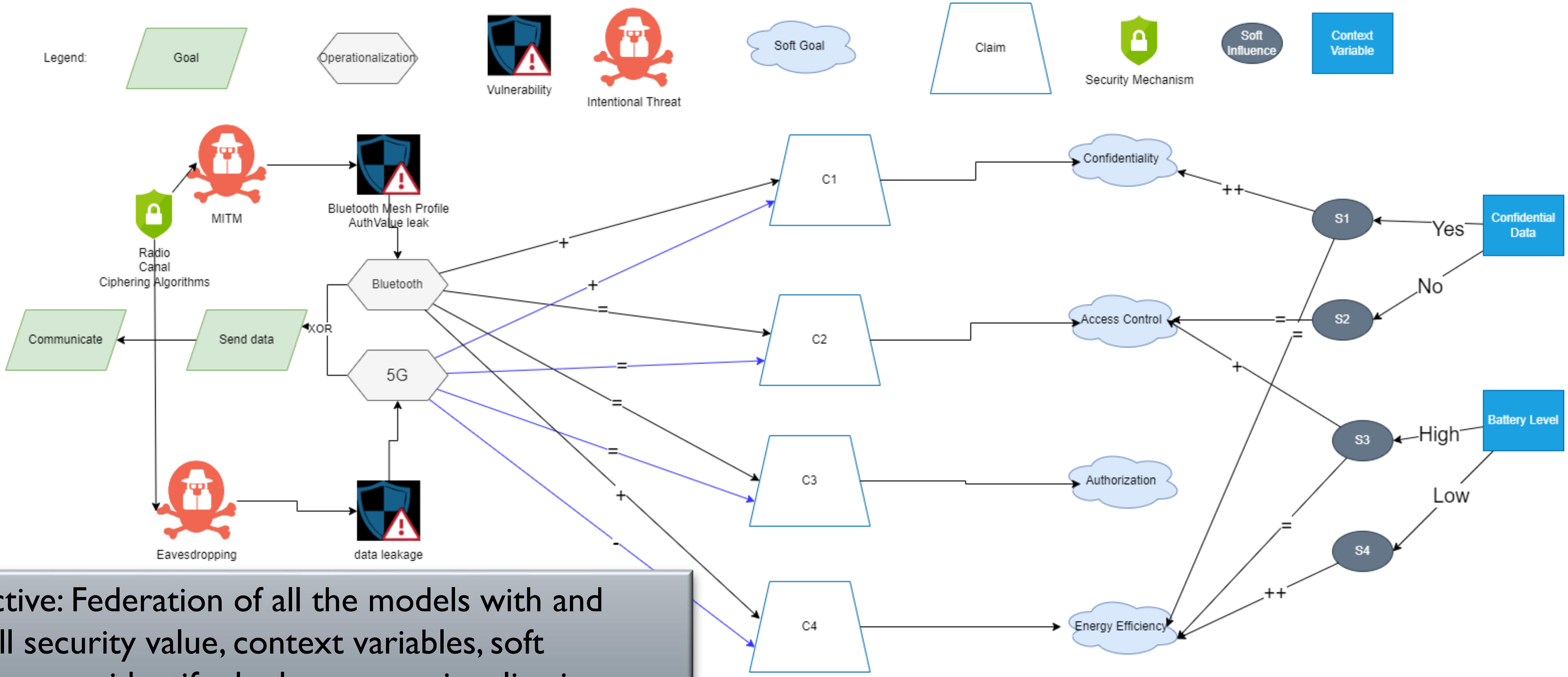
The extent to which a softgoal is satisfied is modeled on an ordinal scale in which the set of values is {--, -, =, +, ++}, ranging from complete denial (--) through neutral or undefined (=) to complete satisfaction (++).

SERENA: SECURITY REQUIREMENTS ANALYSIS TREATMENT MODEL



Objective: Link or add the treatments (security mechanisms) to the threats and security criteria

SERENA: SECURITY REQUIREMENTS ANALYSIS OVERALL MODEL



Objective: Federation of all the models with and overall security value, context variables, soft influences to identify the best operationalizations w.r.t. context variables values

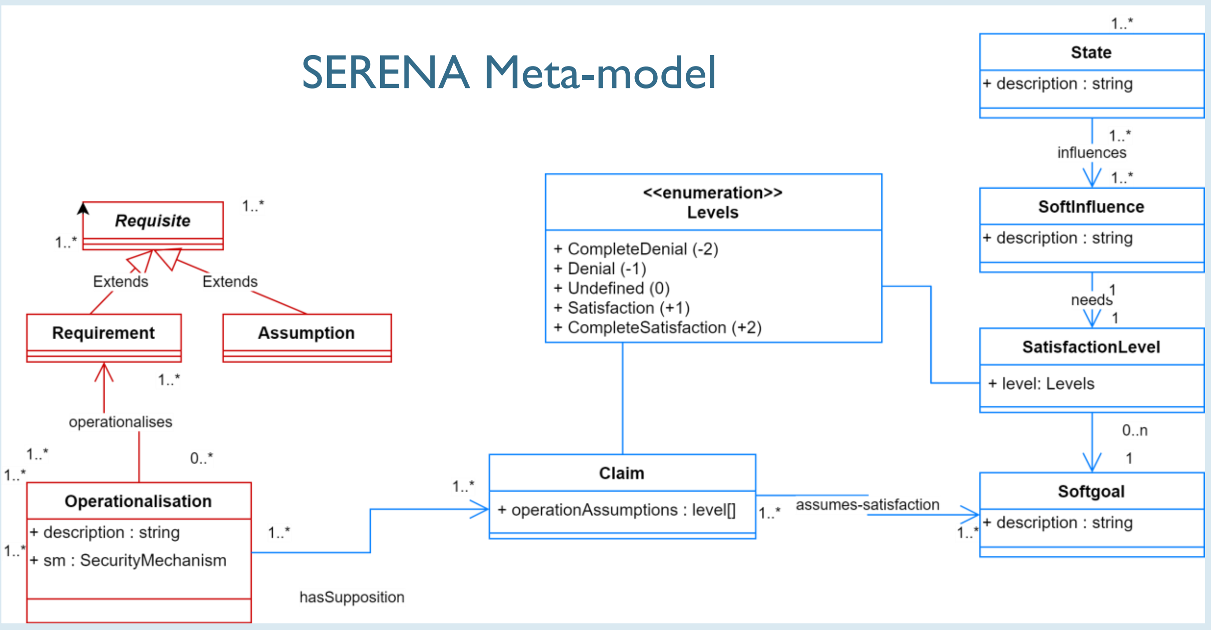
HOW TO ANALYZE THE SECURITY MODEL?

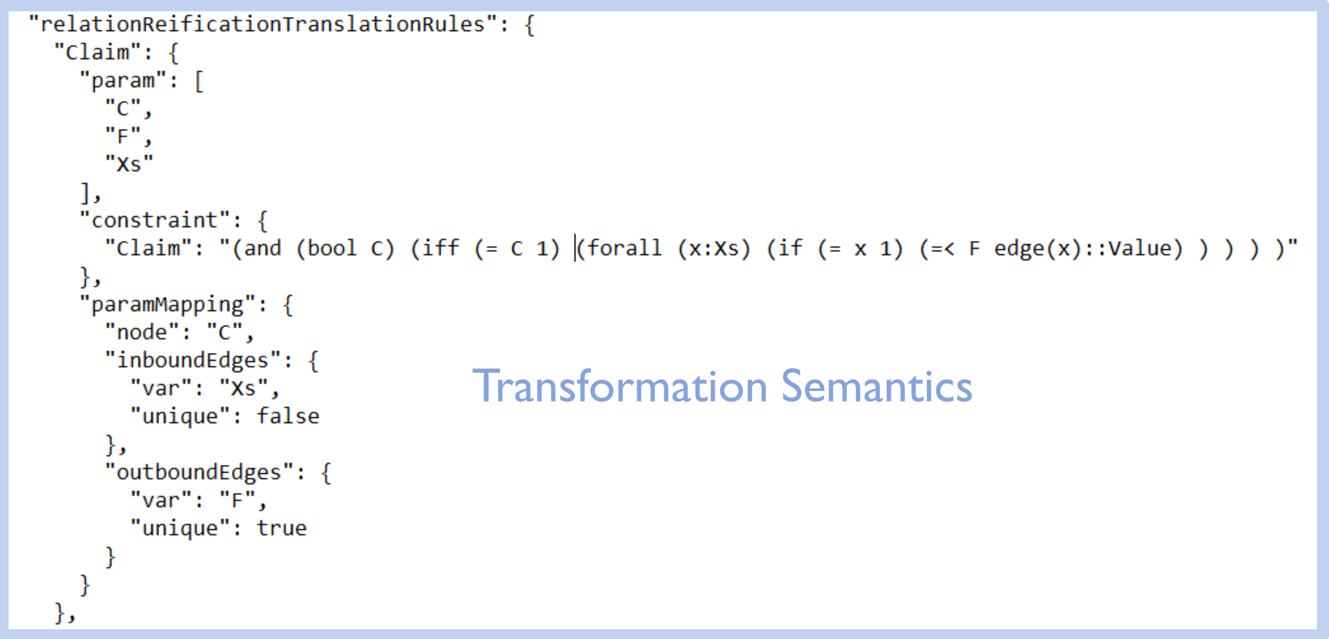
SECURITY ANALYSIS BY CONSTRAINT PROGRAMMING

- Objective : choose the best operationalisation with the best level of security according to the values of the context variables
- Minizinc: constraint modeling language.
- Why use constraint programming?
  - Objective security score
  - Previously used by Soyer et al.

https://www.minizinc.org/

META-MODEL TO CODE


SERENA Meta-model



```
"relationReificationTranslationRules": {
  "Claim": {
    "param": [
      "C",
      "F",
      "Xs"
    ],
    "constraint": {
      "Claim": "(and (bool C) (iff (= C 1) (forall (x:Xs) (if (= x 1) (=< F edge(x)::Value) ) ) ) )"
    },
    "paramMapping": {
      "node": "C",
      "inboundEdges": {
        "var": "Xs",
        "unique": false
      },
      "outboundEdges": {
        "var": "F",
        "unique": true
      }
    }
  },
```

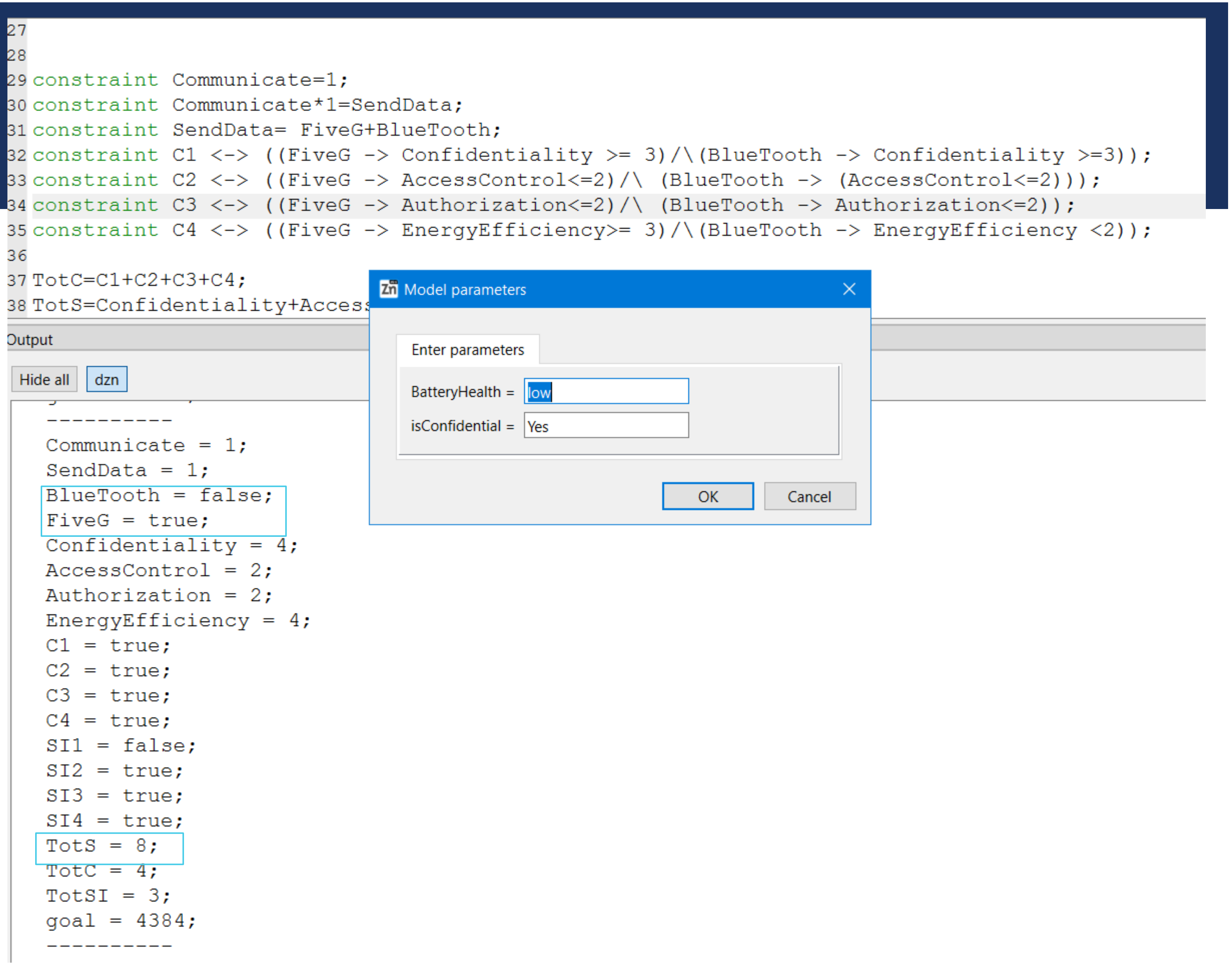
Transformation Semantics

```
constraint C1 <-> ((FiveG -> Confidentiality >= 3)/\(BlueTooth ->
Confidentiality >=3));
constraint C2 <-> ((FiveG -> AccessControl<=2)/\ (BlueTooth ->
(AccessControl<=2)));
```

Constraint rules

MODEL TO CODE

- Operationalization chosen with the highest security score (8) with a low battery level and confidential data is 5G
- **Advantage: objective security score**



```
constraint Communicate=1;
constraint Communicate*1=SendData;
constraint SendData= FiveG+BlueTooth;
constraint C1 <-> ((FiveG -> Confidentiality >= 3)/\(BlueTooth -> Confidentiality >=3));
constraint C2 <-> ((FiveG -> AccessControl<=2)/\ (BlueTooth -> (AccessControl<=2)));
constraint C3 <-> ((FiveG -> Authorization<=2)/\ (BlueTooth -> Authorization<=2));
constraint C4 <-> ((FiveG -> EnergyEfficiency>= 3)/\(BlueTooth -> EnergyEfficiency <2));

TotC=C1+C2+C3+C4;
TotS=Confidentiality+Access
```

```
----------
Communicate = 1;
SendData = 1;
BlueTooth = false;
FiveG = true;
Confidentiality = 4;
AccessControl = 2;
Authorization = 2;
EnergyEfficiency = 4;
C1 = true;
C2 = true;
C3 = true;
C4 = true;
SI1 = false;
SI2 = true;
SI3 = true;
SI4 = true;
TotS = 8;
TotC = 4;
TotSI = 3;
goal = 4384;
----------
```

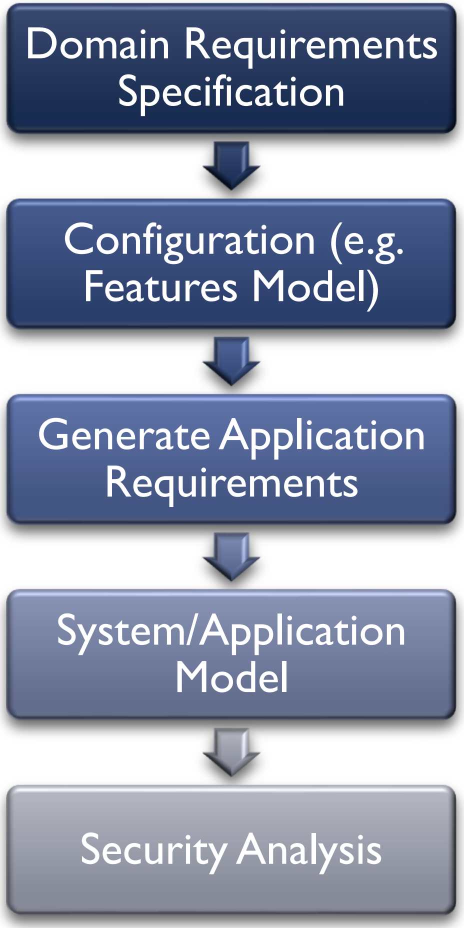
Model parameters

Enter parameters

BatteryHealth = low

isConfidential = Yes

SECURITY ANALYSIS METHODOLOGY



Domain Requirements Specification

Configuration (e.g. Features Model)

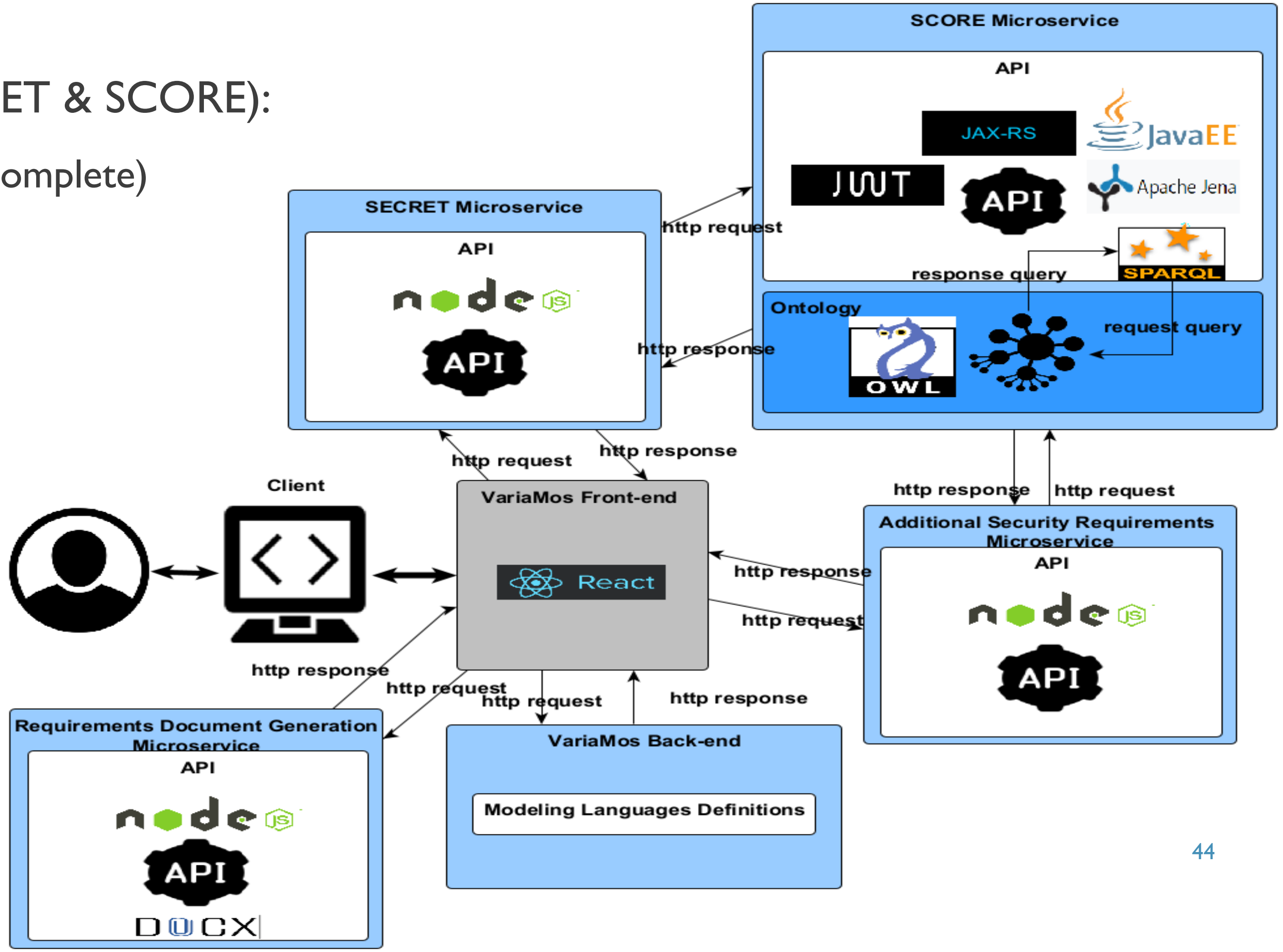
Generate Application Requirements

System/Application Model

Security Analysis

IMPLEMENTATION
REQUIREMENTS SPECIFICATION MODULE - VARIAMOS

- Two requirements specification languages (SECRET & SCORE):
  - Domain Requirements Specification – AC (Auto Complete)
  - Application Requirements Specification – AC
- Related security requirements (SCORE)
- Generate requirements document



SCORE Microservice

API

JAX-RS

JavaEE

JWT

API

Apache Jena

SPARQL

response query

Ontology

OWL

request query

SECRET Microservice

API

node JS

API

http request

http response

http request

http response

Client

VariaMos Front-end

React

http response

http request

Additional Security Requirements Microservice

API

node JS

API

http response

http request

http response

http request

http request

http response

Requirements Document Generation Microservice

API

node JS

API

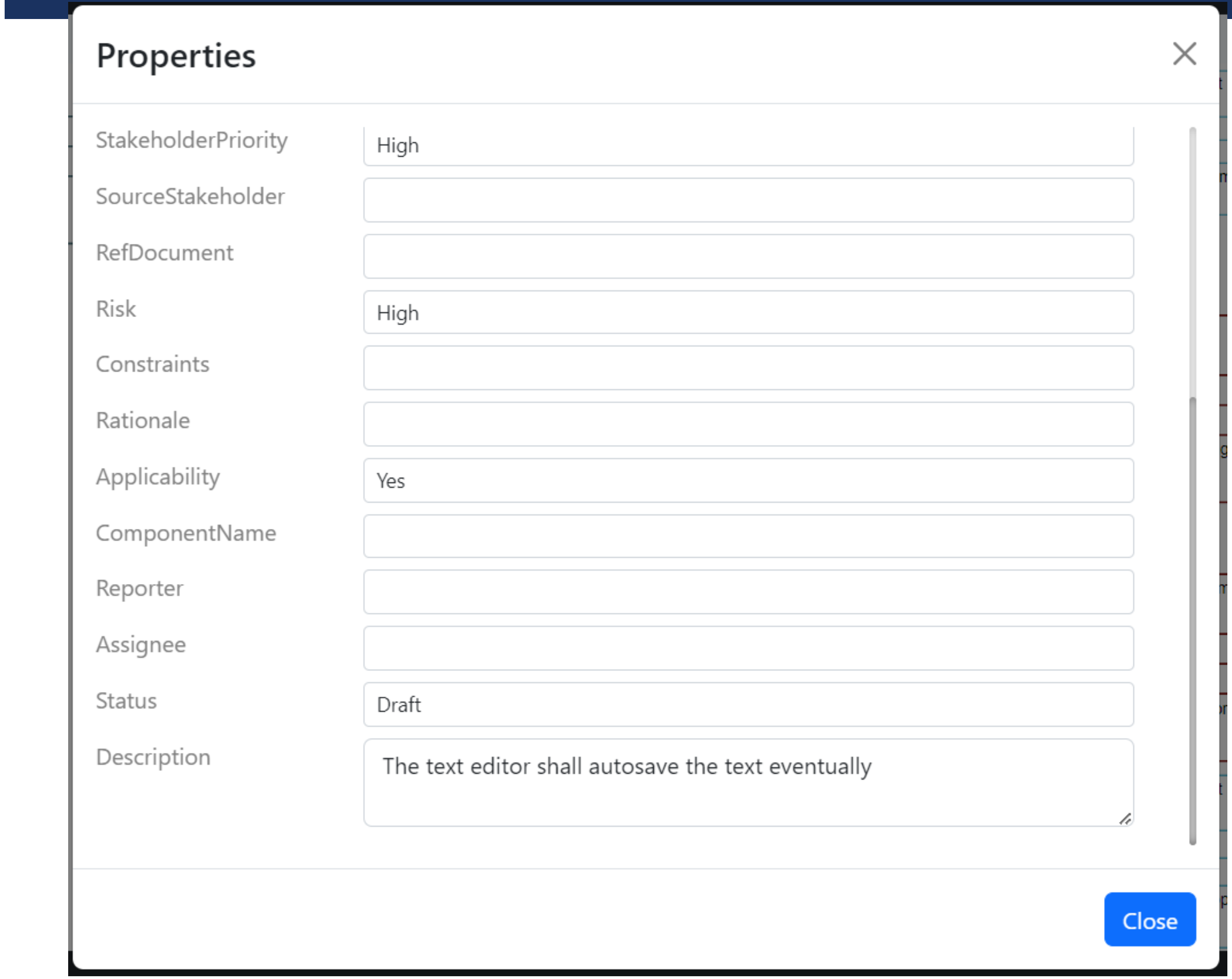
DOCX

VariaMos Back-end

Modeling Languages Definitions

https://app.variamos.com/dashboard

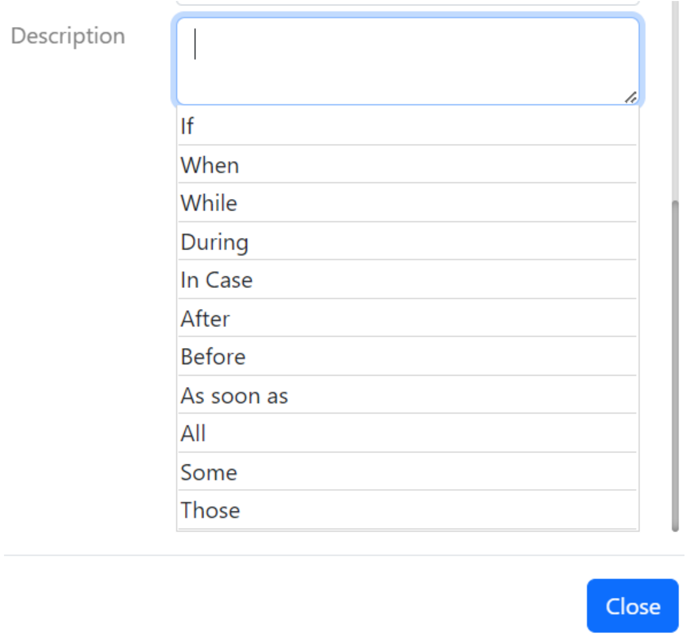
IMPLEMENTATION
REQUIREMENTS SPECIFICATION MODULE - VARIAMOS



Properties

StakeholderPriority	High
SourceStakeholder	
RefDocument	
Risk	High
Constraints	
Rationale	
Applicability	Yes
ComponentName	
Reporter	
Assignee	
Status	Draft
Description	The text editor shall autosave the text eventually

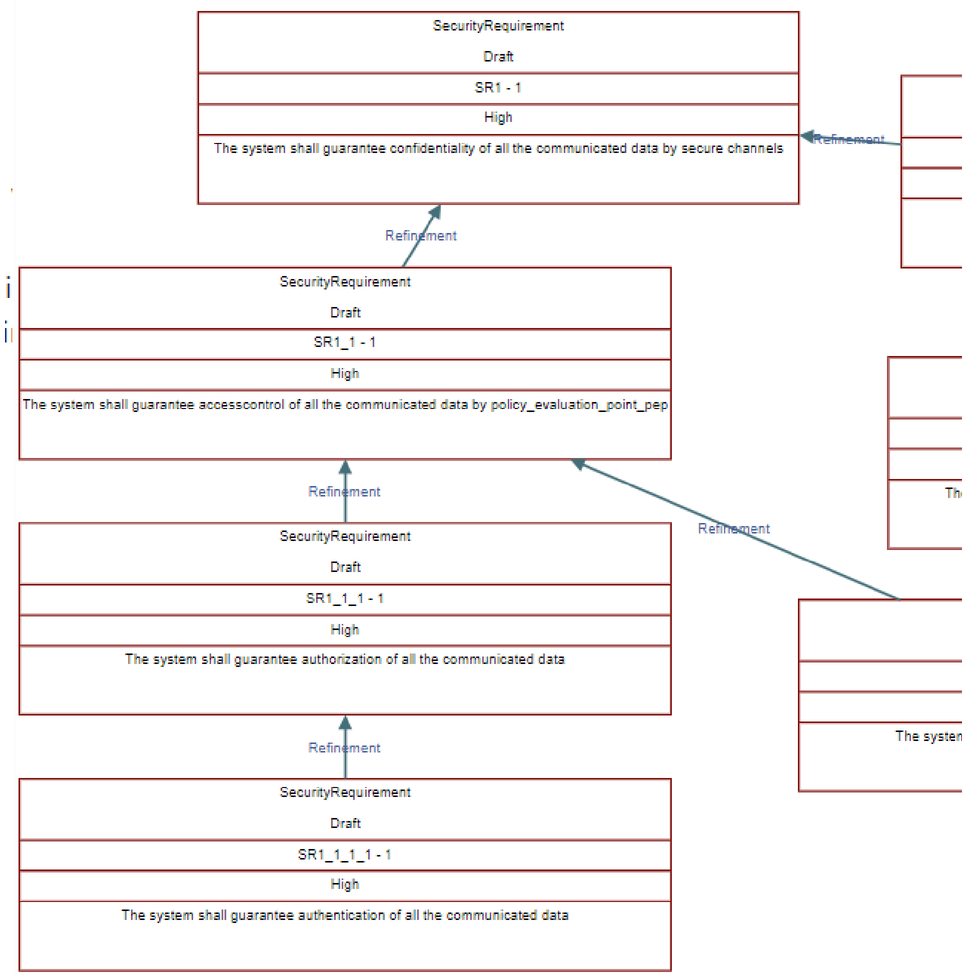
Define the metadata and the requirement decription (SECRET template)



Description

- If
- When
- While
- During
- In Case
- After
- Before
- As soon as
- All
- Some
- Those

IMPLEMENTATION
REQUIREMENTS SPECIFICATION MODULE - VARIAMOS

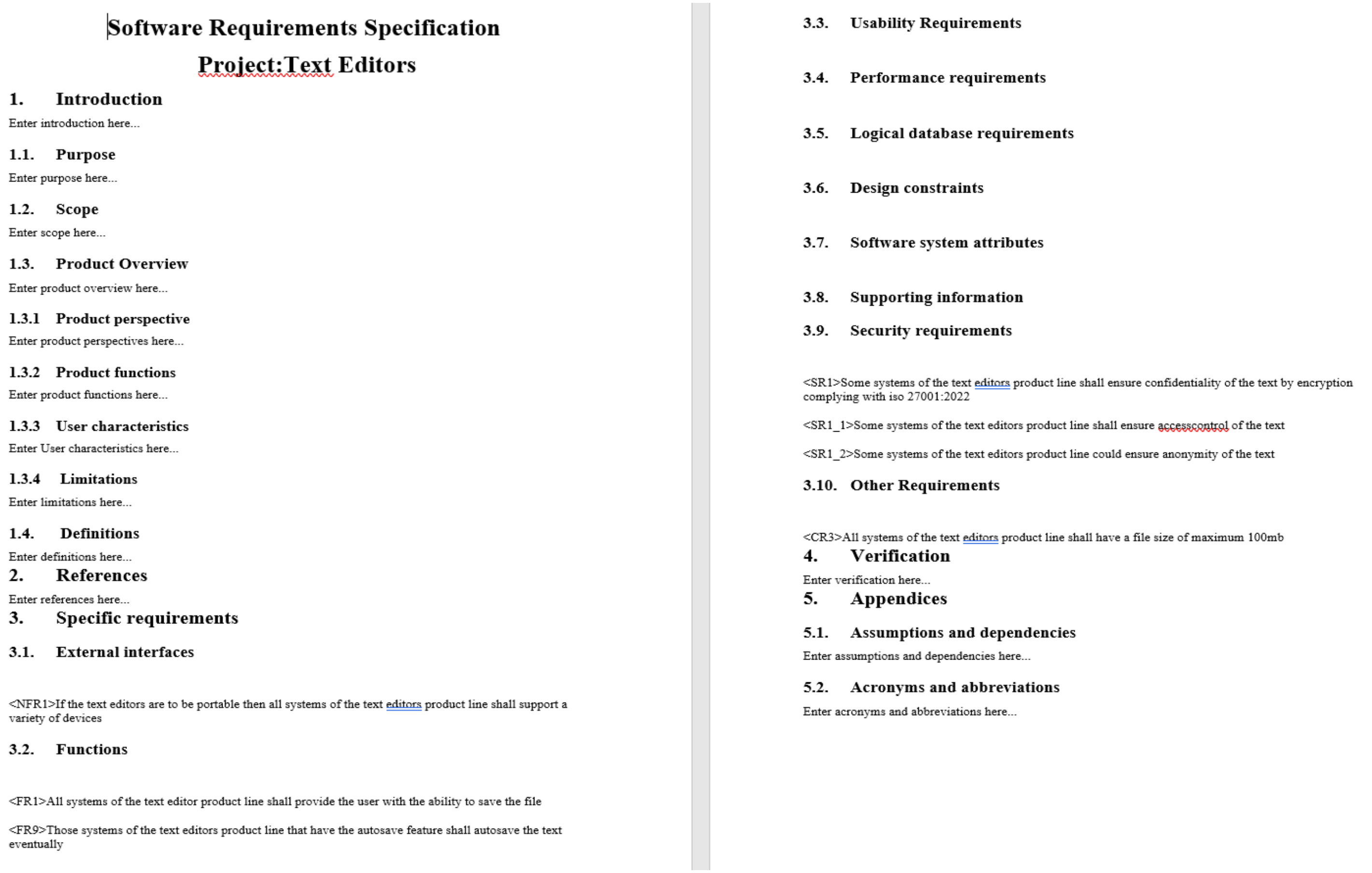


SecurityRequirement
Draft
SR1 - 1
High
The system shall guarantee confidentiality of all the communicated data by secure channels

SecurityRequirement
Draft
SR1_1 - 1
High
The system shall guarantee accesscontrol of all the communicated data by policy_evaluation_point_pep

SecurityRequirement
Draft
SR1_1_1 - 1
High
The system shall guarantee authorization of all the communicated data

SecurityRequirement
Draft
SR1_1_1_1 - 1
High
The system shall guarantee authentication of all the communicated data



Software Requirements Specification

Project:Text Editors

1. Introduction

Enter introduction here...

1.1. Purpose

Enter purpose here...

1.2. Scope

Enter scope here...

1.3. Product Overview

Enter product overview here...

1.3.1 Product perspective

Enter product perspectives here...

1.3.2 Product functions

Enter product functions here...

1.3.3 User characteristics

Enter User characteristics here...

1.3.4 Limitations

Enter limitations here...

1.4. Definitions

Enter definitions here...

2. References

Enter references here...

3. Specific requirements

3.1. External interfaces

<NFR1>If the text editors are to be portable then all systems of the text editors product line shall support a variety of devices

3.2. Functions

<FR1>All systems of the text editor product line shall provide the user with the ability to save the file

<FR9>Those systems of the text editors product line that have the autosave feature shall autosave the text eventually

3.3. Usability Requirements

3.4. Performance requirements

3.5. Logical database requirements

3.6. Design constraints

3.7. Software system attributes

3.8. Supporting information

3.9. Security requirements

<SR1>Some systems of the text editors product line shall ensure confidentiality of the text by encryption complying with iso 27001:2022

<SR1_1>Some systems of the text editors product line shall ensure accesscontrol of the text

<SR1_2>Some systems of the text editors product line could ensure anonymity of the text

3.10. Other Requirements

<CR3>All systems of the text editors product line shall have a file size of maximum 100mb

4. Verification

Enter verification here...

5. Appendices

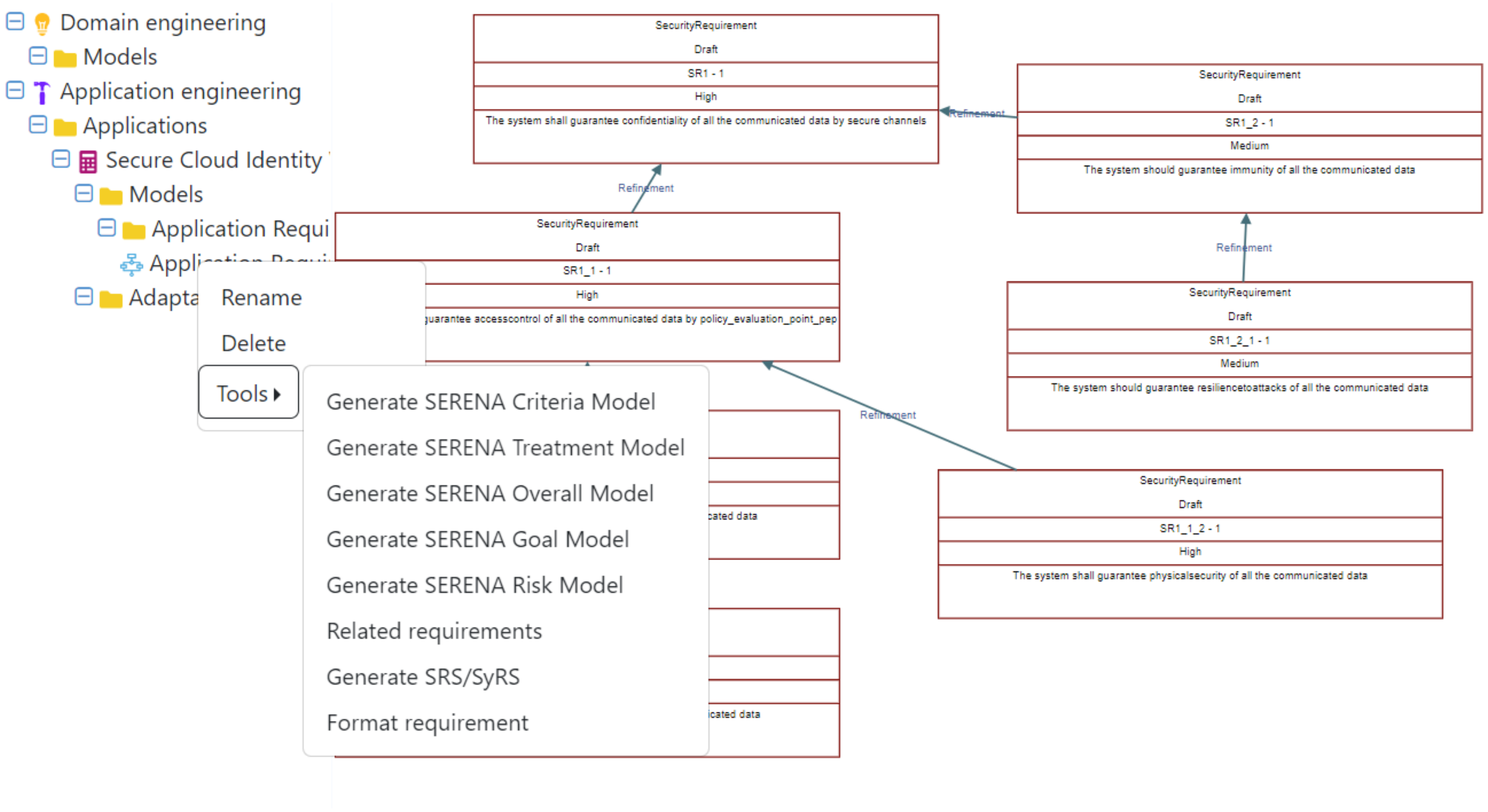
5.1. Assumptions and dependencies

Enter assumptions and dependencies here...

5.2. Acronyms and abbreviations

Enter acronyms and abbreviations here...

IMPLEMENTATION
SERENA TRANSFORMATIONS - VARIAMOS



SecurityRequirement
Draft
SR1 - 1
High
The system shall guarantee confidentiality of all the communicated data by secure channels

SecurityRequirement
Draft
SR1_2 - 1
Medium
The system should guarantee immunity of all the communicated data

SecurityRequirement
Draft
SR1_1 - 1
High
uarantee accesscontrol of all the communicated data by policy_evaluation_point_pep

SecurityRequirement
Draft
SR1_2_1 - 1
Medium
The system should guarantee resiliencetoattacks of all the communicated data

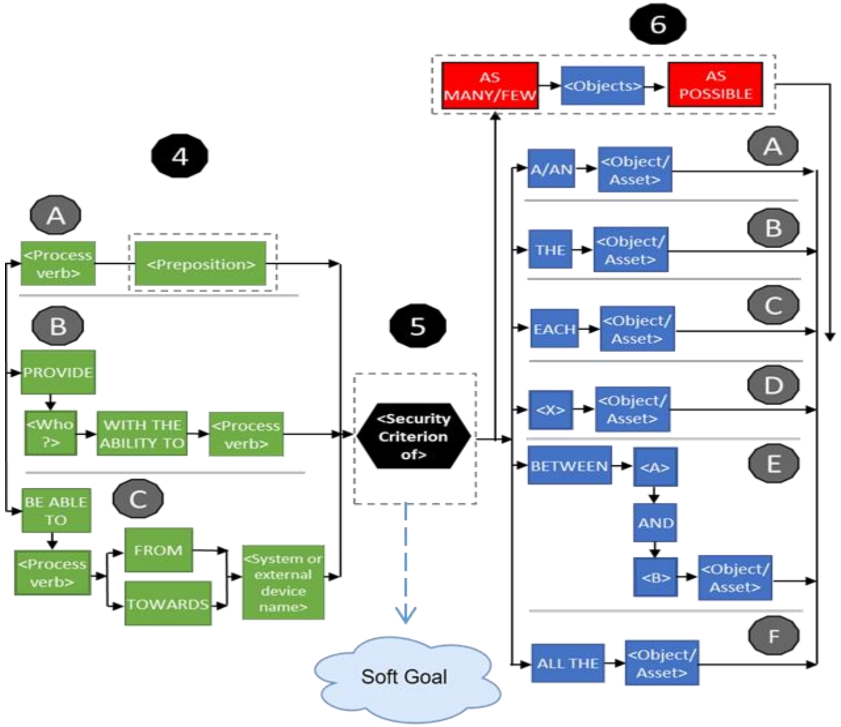
SecurityRequirement
Draft
SR1_1_2 - 1
High
The system shall guarantee physicalsecurity of all the communicated data

cated data

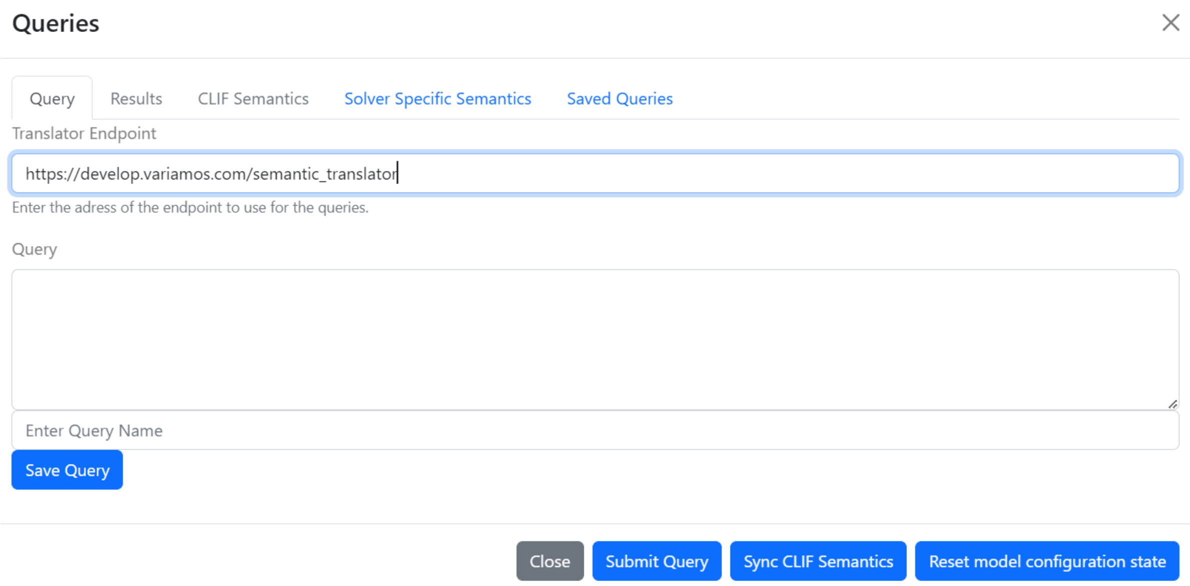
cated data

TRANSFORMATION EXAMPLE

- Security criterion in security requirement -> Softgoal in SERENA
- Activity + object in functional requirement -> Goal in SERENA
- Security mechanism in security requirement -> Security mechanism in SERENA

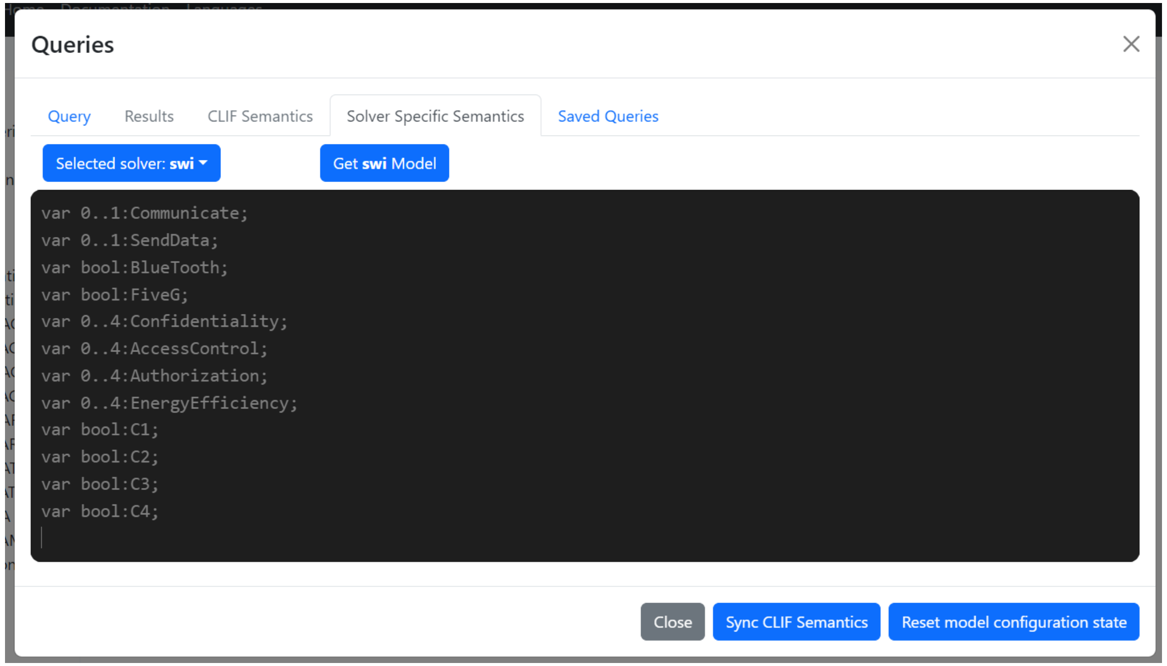


IMPLEMENTATION
SECURITY ANALYSIS - CLIF GENERATION



Translator Endpoint: https://develop.variamos.com/semantic_translator

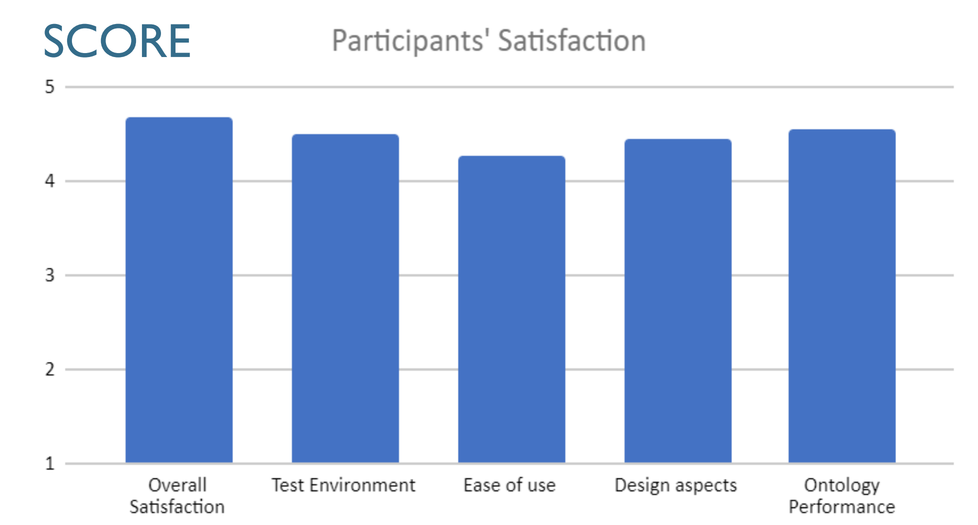
Enter the adress of the endpoint to use for the queries.



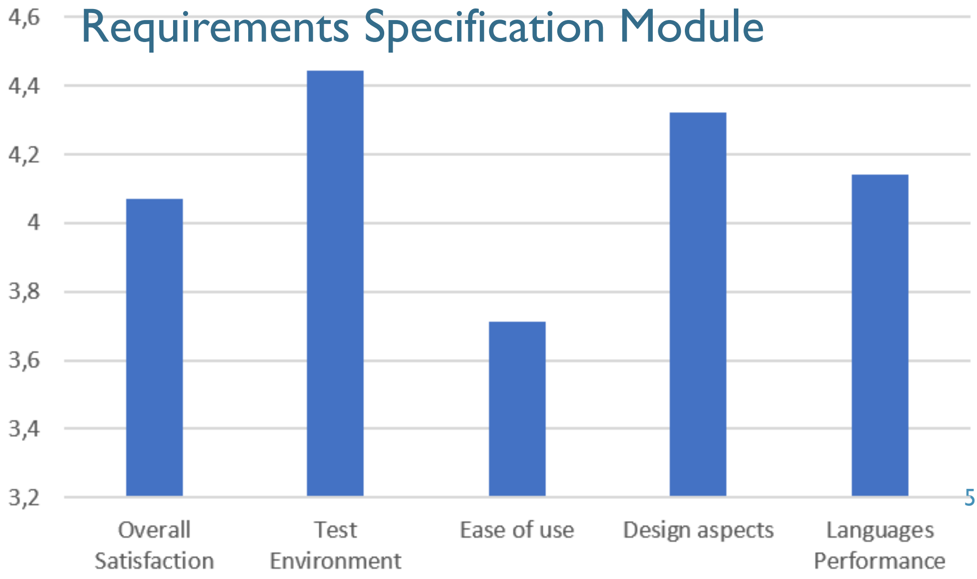
Selected solver: swi

```
var 0..1:Communicate;
var 0..1:SendData;
var bool:BlueTooth;
var bool:FiveG;
var 0..4:Confidentiality;
var 0..4:AccessControl;
var 0..4:Authorization;
var 0..4:EnergyEfficiency;
var bool:C1;
var bool:C2;
var bool:C3;
var bool:C4;
```

EVALUATION & VALIDATION



- SCORE Ontology: Experts Evaluation & Usability Test
- SECRET Template: Action Research
- Requirements Specification Module: Usability Test & Use Case
- SERENA & its semantics (Minizinc code generation) : Use Case



CONCLUSION

- Guided approach to specify strutured requirements and additional security requirements.
- Multi-view modeling language and its automatic transformations from the specified requirements.
- From SERENA Model to security analysis with objective security score.
- Each component of the Framework can be used independently.

PERSPECTIVES

- Domain Engineering
  - Create the link between domain requirements and application requirements by system configuration
  - Add other modeling languages to the framework (e.g. Features Model) for product line configuration
- Security Analysis
  - Add other security analysis methods at the level of risk model and treatment model
  - Enrich the SCORE ontology with security concept to facilitate the risk and treatment assessment
  - Extend the use of the framework