



**ENSTA
BRETAGNE**

COLLEGES

SCIENCES

BRETAGNE

POUR L'INGENIEUR

LOIRE

ET LE NUMERIQUE

Towards a unifying framework
for the specification,
formalization and analysis of
secure hardware and
software architectures

Hiba Hnaini

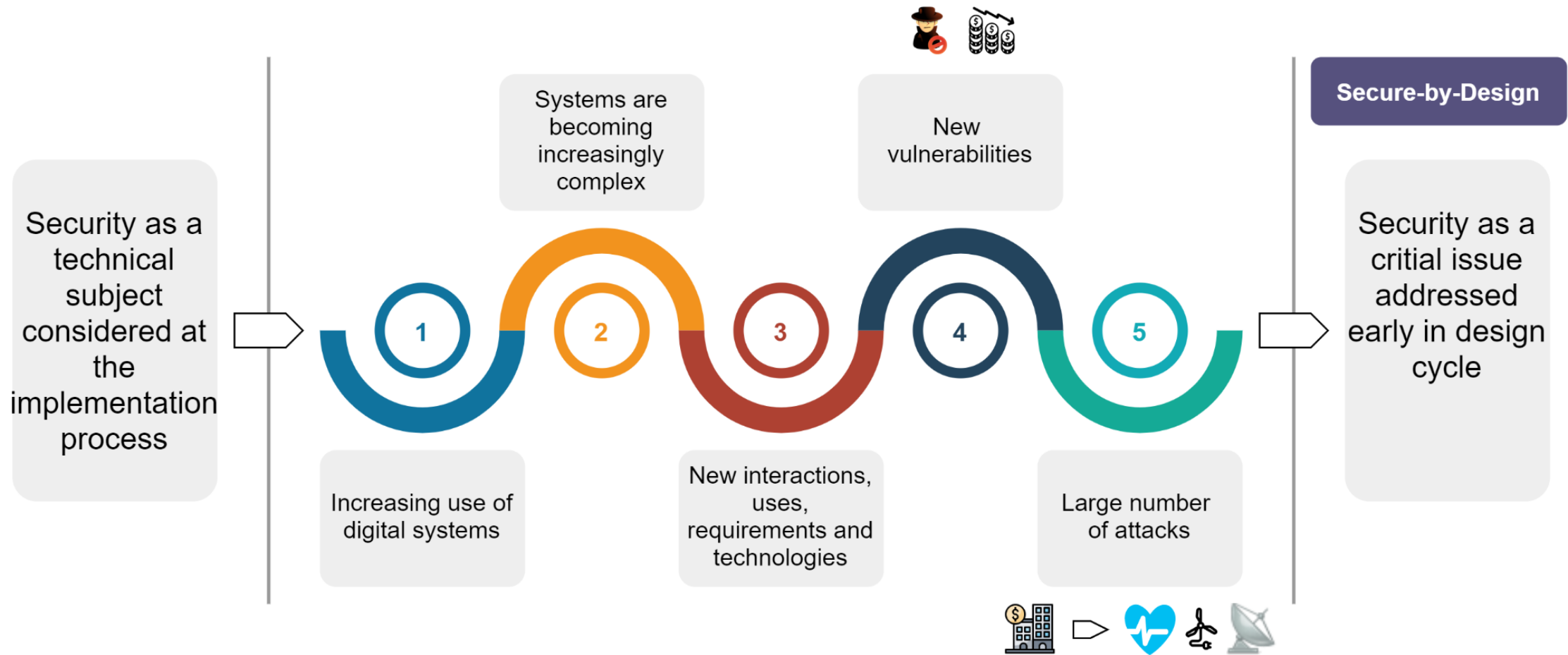
1

Objective

Design and **evaluate** a new multi-paradigm security modeling approach and its engineering framework (engineering process and tooling) allowing the **specification, formalization** and **analysis** of **secure hardware and software architectures**.

Context

Context
Innovative nature of the project
Methodology
Concepts
Proof of Concept Example
State of Art – Proof of Concept
Our Approach – Proof of Concept
Appendix



Innovative nature of the project

Context

Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix

We want to

Design secure systems

The path to designing secure systems is long
Need federated approach
(Different levels of abstraction and viewpoints)



**Using a unifying framework
(Specification, Formalization, Analysis)**

No unifying framework for the multiple languages



That is applicable in real cases

Technology transfer has a significantly lower efficiency outside limited test facilities



Going beyond a simple mix of solutions



Using different modeling and programming formalisms
(Multiparadigm)



Create a unifying framework
(Specification, Formalization, Analysis) that supports:



Reusability of the approach
(Separate between specification and analysis)



Develop reference experiments to affirm the applicability and usefulness in real cases



Example – A Smart Phone or a Family of Smart Phones

Context

Innovative nature of the project

Methodology

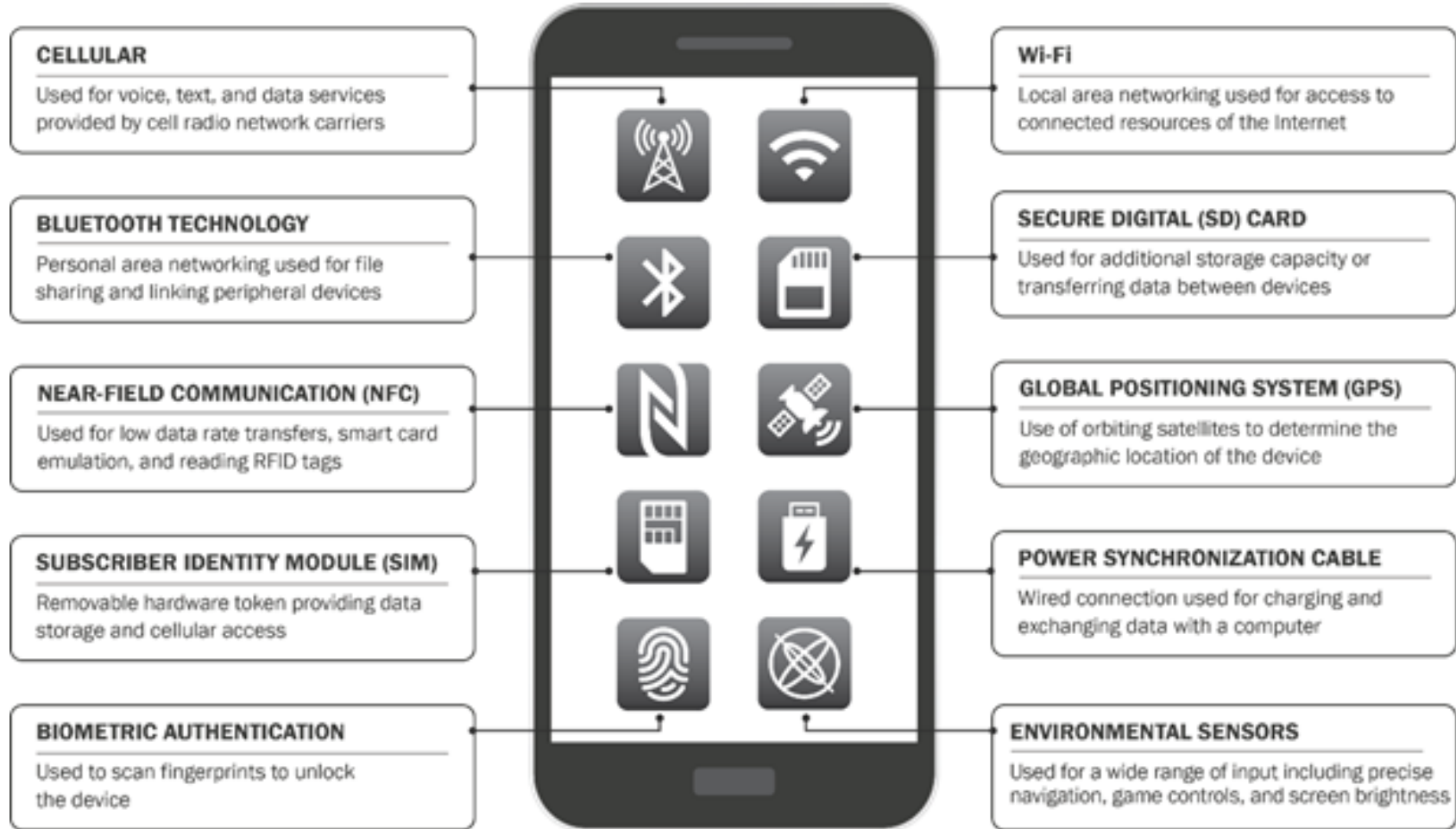
Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix



Example – A Smart Phone or a Family of Smart Phones

Context

Security Requirements according to:

[Requirements for OEM regarding Smartphone Security \(bund.de\)](#)

(defined by the German Federal Office for Information Security)

Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix

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

Example – A Smart Phone or a Family of Smart Phones

Context

Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix

The main security criteria in this domain are:

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: In case of bootloader unlock, all user data must be deleted in a safe way.

Req4: The processor must support hardware based security functions for attack defense. This includes mechanisms for ROP/JOP mitigation, attacks to speculative execution and memory encryption, and separation mechanisms (TEE).

Req 5: All new devices must be provided with the latest OS available at release time.

Security Requirements Specification

Context

Innovative nature of the project

Methodology

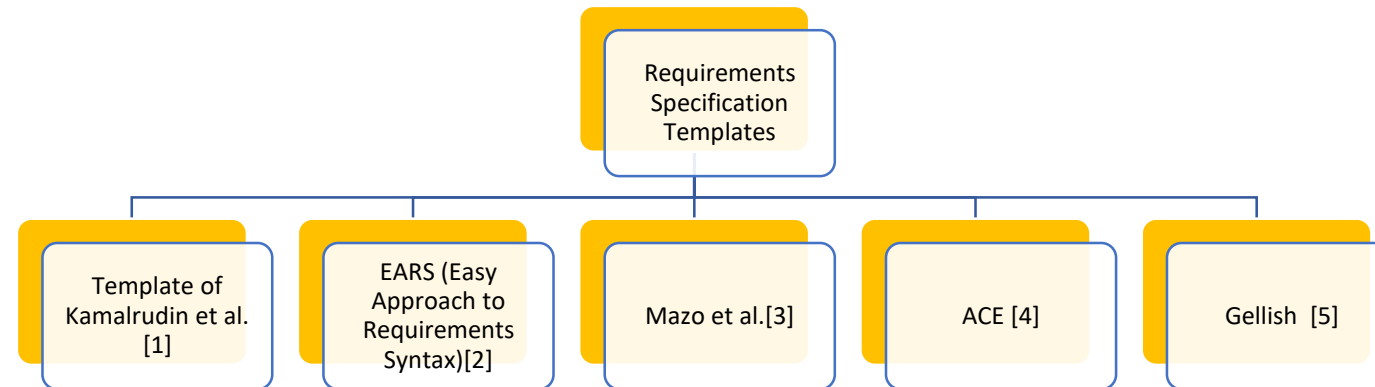
Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix



[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.

Security Requirements Specification

Context

Mazo et al. template [1]

Innovative nature of the project

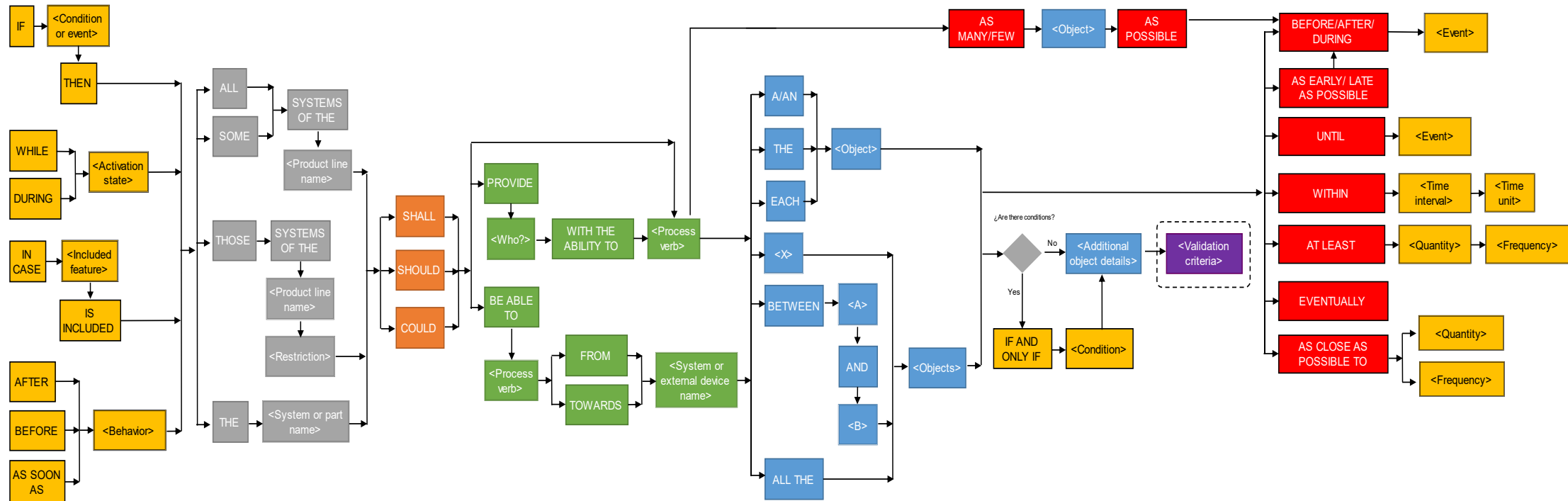
Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept



[1] 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.

Security Requirements Specification

Context

Mazo et al. template [1]

Innovative nature of the project

Req1: The <Cellular Interface>_{system or part name} <should>_{priority} <ensure>_{process verb} <data>_{object} <confidentiality by Radio Canal Ciphering Algorithms >_{additional object information}

Methodology

Req2: The <HSE>_{system or part name} <should>_{priority} <ensure>_{process verb} <data>_{object} <integrity by storing security critical data >_{additional object information}

Concepts

Req3: < When the bootloader is unlocked >_{condition} The <App Processor>_{system or part name} <should>_{priority} <ensure>_{process verb} <data>_{object} <privacy by deleting user data>_{additional object information}

Proof of Concept Example

...

State of Art – Proof of Concept

Req5: <All new devices>_{systems} <should>_{priority} <ensure>_{process verb} <availability of data>_{object} <by having the latest OS at release.>_{additional info}

Our Approach – Proof of Concept

Appendix

Security Requirements Specification

Context

Mazo et al. template[1]

Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

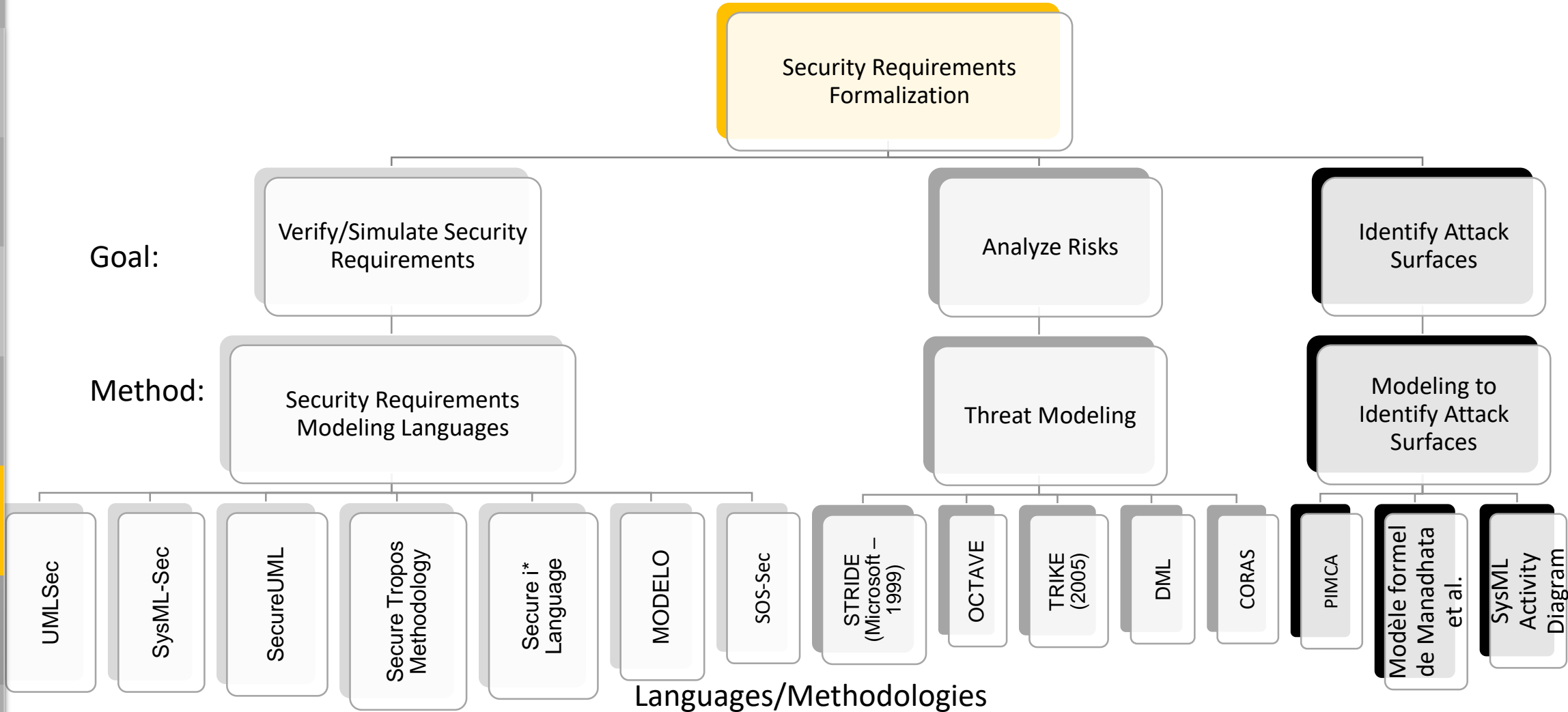
Appendix

Advantages	Disadvantages
Requirements Specification	Security Criteria considered as additional object info.
Structured Natural Language	Security Mechanism considered as additional object info.
Applies to a family of systems and auto-adaptive systems	

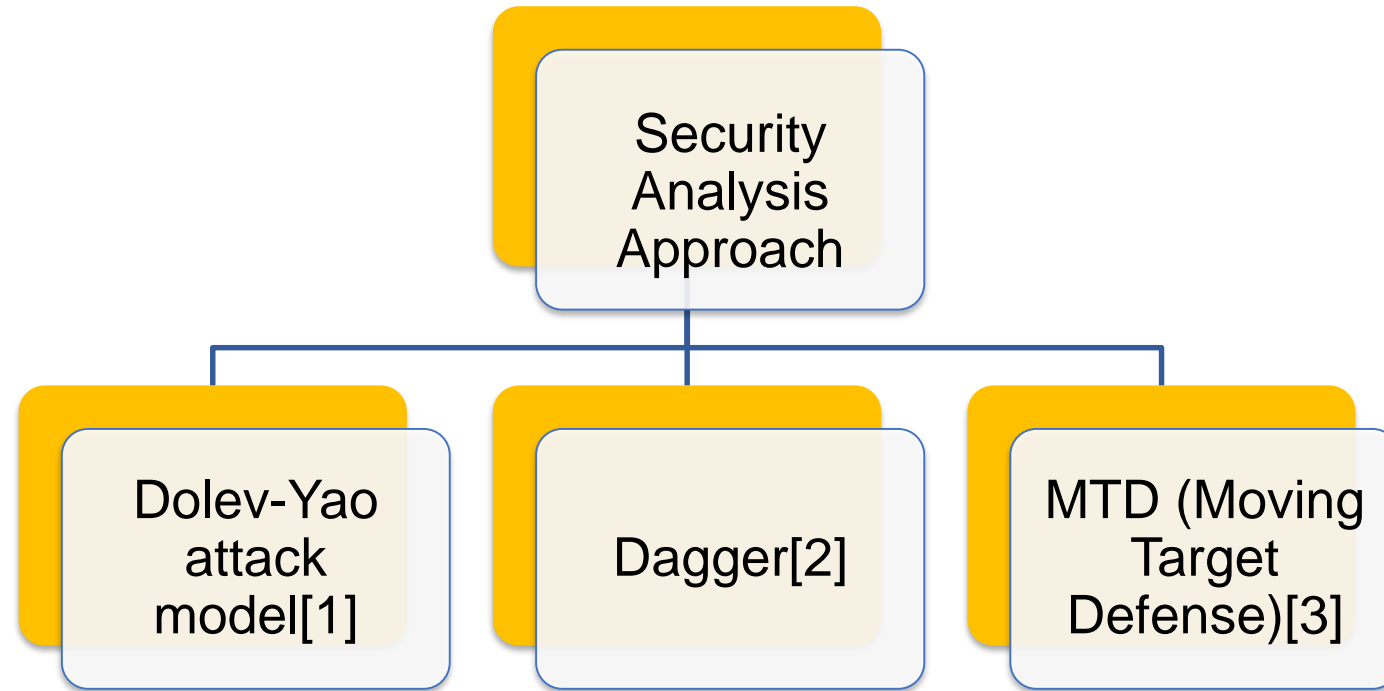
[1] Mazo, Raúl & Jaramillo, Carlos & Vallejo, Paola & Medina, Jhon. (2020). Towards a new template for the specification of requirements in semi-structured natural language. Journal of Software Engineering Research and Development. 8. 3. 10.5753/jserd.2020.473.

Security Requirements Formalization

Security Requirements Formalization



Security Analysis



[1]Cervesato, Iliano. (2001). The Dolev-Yao Intruder is the Most Powerful Attacker

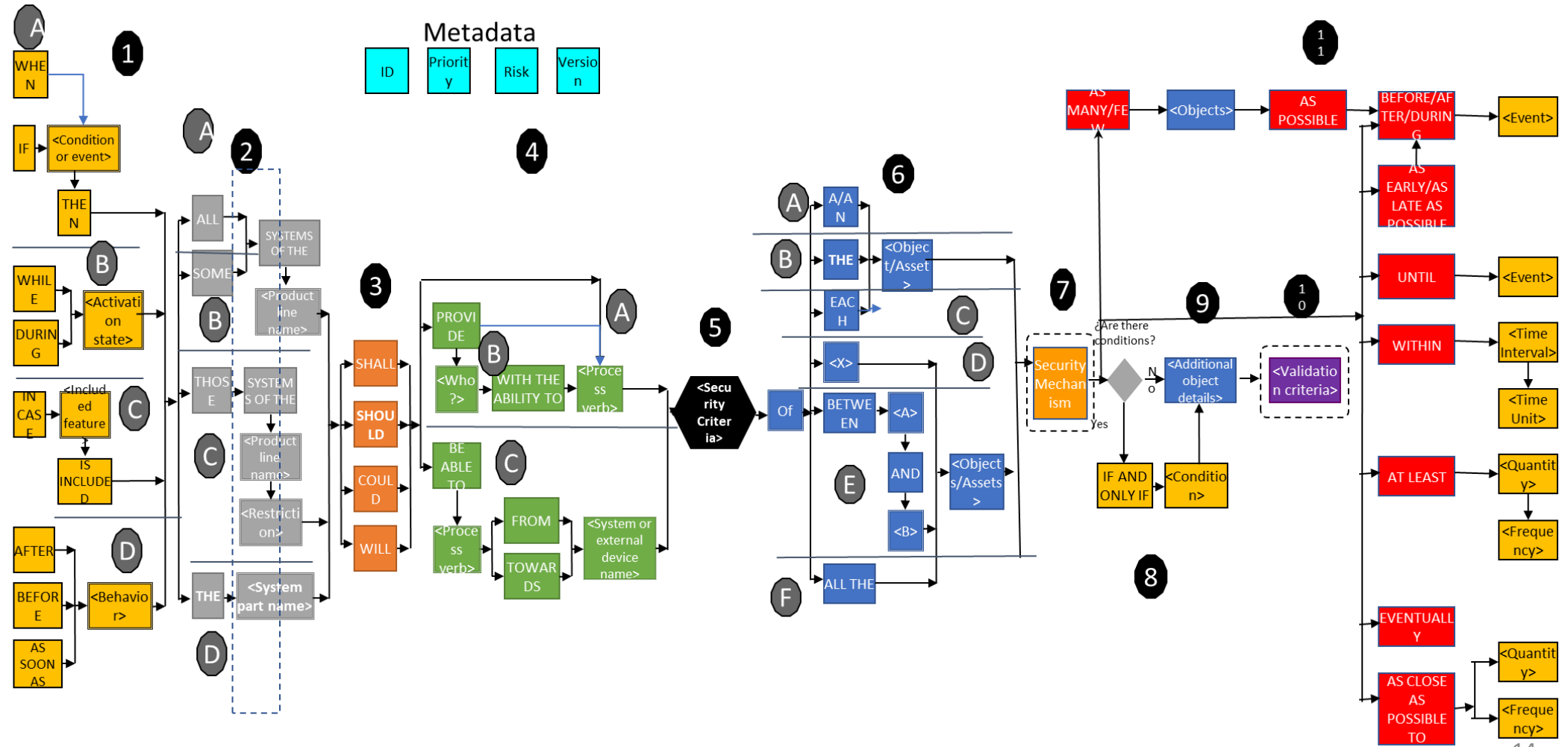
[2]Peterson, Elisha. (2016). Dagger: Modeling and visualization for mission impact situation awareness. 25-30. 10.1109/MILCOM.2016.7795296.

[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.

Security Requirements Specification

SECRET : Template based on the new template for the specification of requirements in semi-structured natural language

- Context
- Innovative nature of the project
- Methodology
- Concepts
- Proof of Concept Example
- State of Art – Proof of Concept
- Our Approach – Proof of Concept
- Appendix

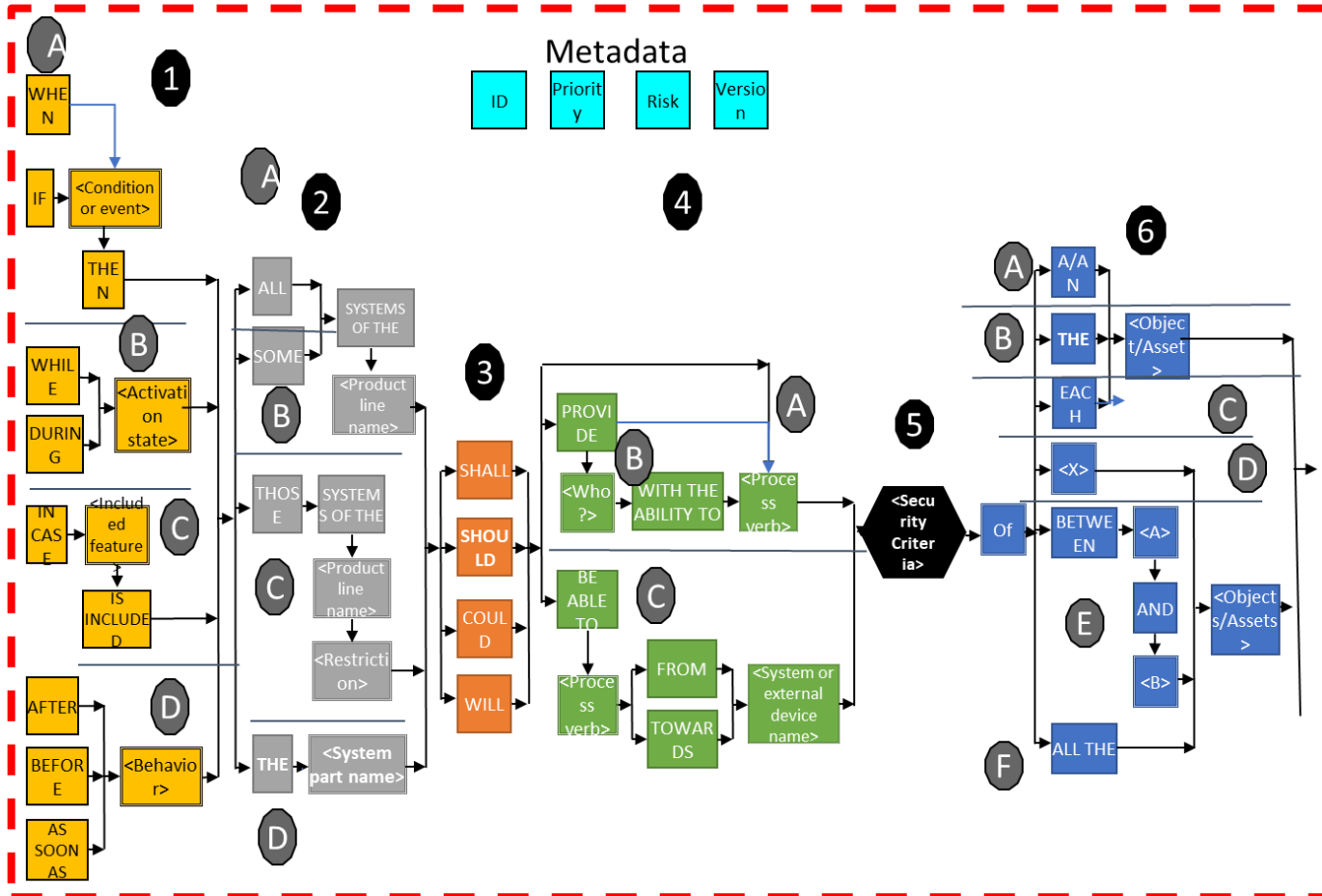


Security Requirements Specification

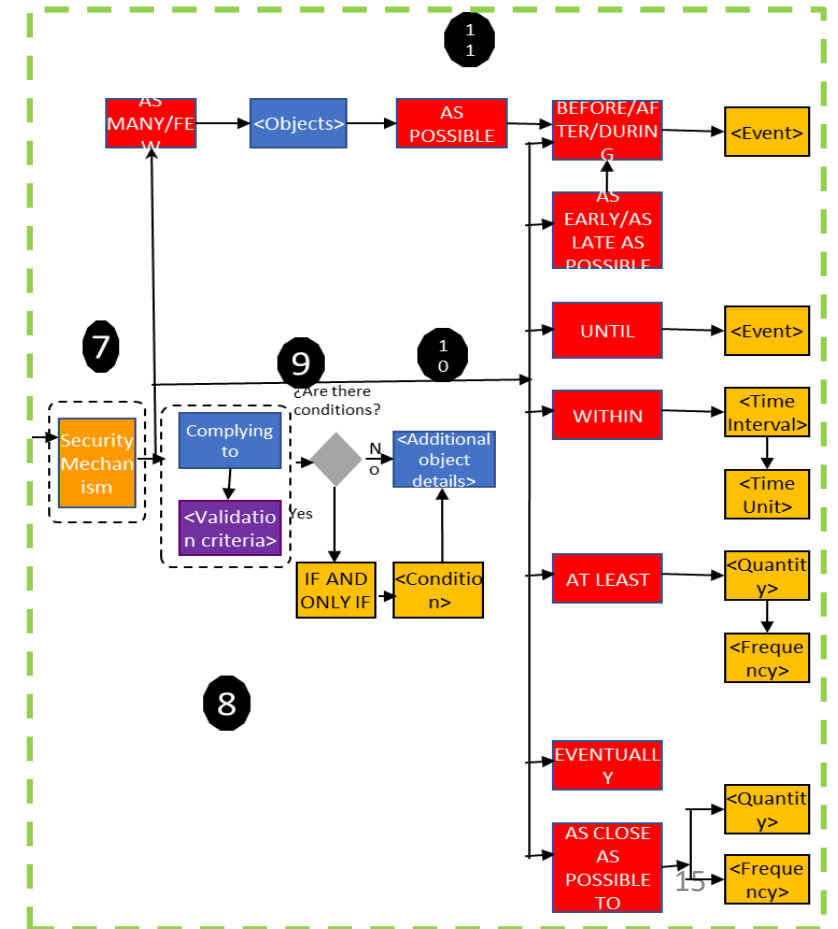
SECRET : Template based on the new template for the specification of requirements in semi-structured natural language

Context
Innovative nature of the project
Methodology
Concepts
Proof of Concept Example
State of Art – Proof of Concept
Our Approach – Proof of Concept
Appendix

Problem Space



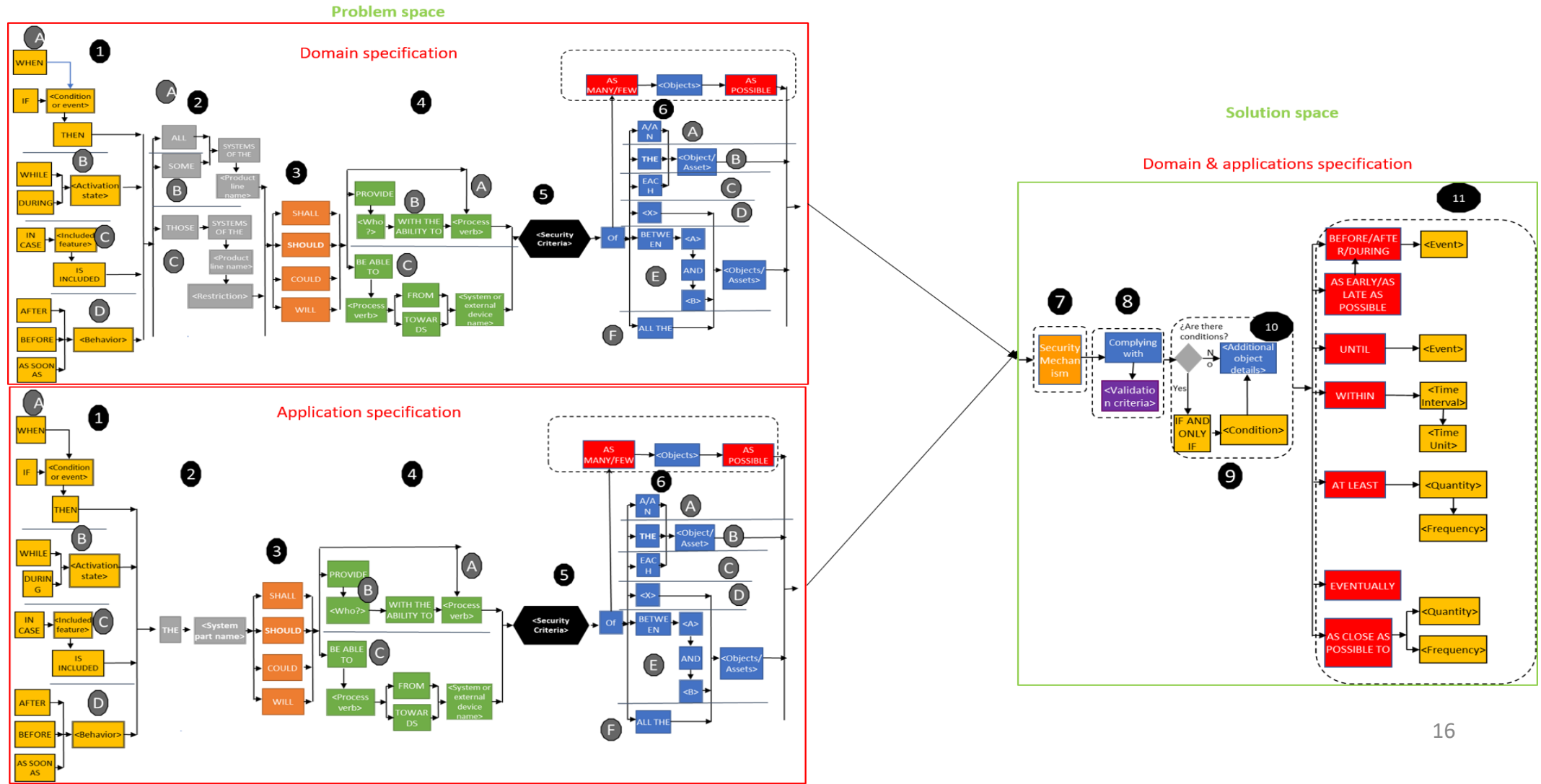
Solution Space



Security Requirements Specification

SECRET : Template based on the new template for the specification of requirements in semi-structured natural language

- Context
- Innovative nature of the project
- Methodology
- Concepts
- Proof of Concept Example
- State of Art – Proof of Concept
- Our Approach – Proof of Concept
- Appendix



Security Requirements Specification

Context

SECRET : Template based on the new template for the specification of requirements in semi-structured natural language –

Creating a microservice for text suggestion based on SECRET

Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix



Security Requirements Specification

SECRET : Template based on the new template for the specification of requirements in semi-structured natural language –
Creating a microservice for text suggestion based on SECRET

Application Security Requirements

SecurityRequirement
Draft
Req1 - 1
High
The system

Status

Draft ▾

Description

The system

shall

should

could

will

Domain Security Requirements

SecurityRequirement
Draft
Req1 - 1
High
undefined

Description

If

When

While

During

In Case

After

Before

As soon as

All

Some

Those

Context

Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix

Security Requirements Specification

Context

Ontology of Security Criteria – Proof of Concept

Writing Requirements Without the Typology (4 requirements only):

Req1: The <Cellular Interface>_{system or system part} <should>_{priority} <ensure>_{process verb} <confidentiality>_{security criteria} of <data>_{asset to protect} <by Radio Canal Ciphering Algorithms>_{security mechanism}

Req2: The <HSE>_{system or system part} <should>_{priority} <ensure>_{process verb} <integrity>_{security criteria} of <data>_{asset to protect} <by storing security critical data>_{security mechanism}

...

Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix

Security Requirements Specification

Context

Ontology of Security Criteria

– Proof of Concept

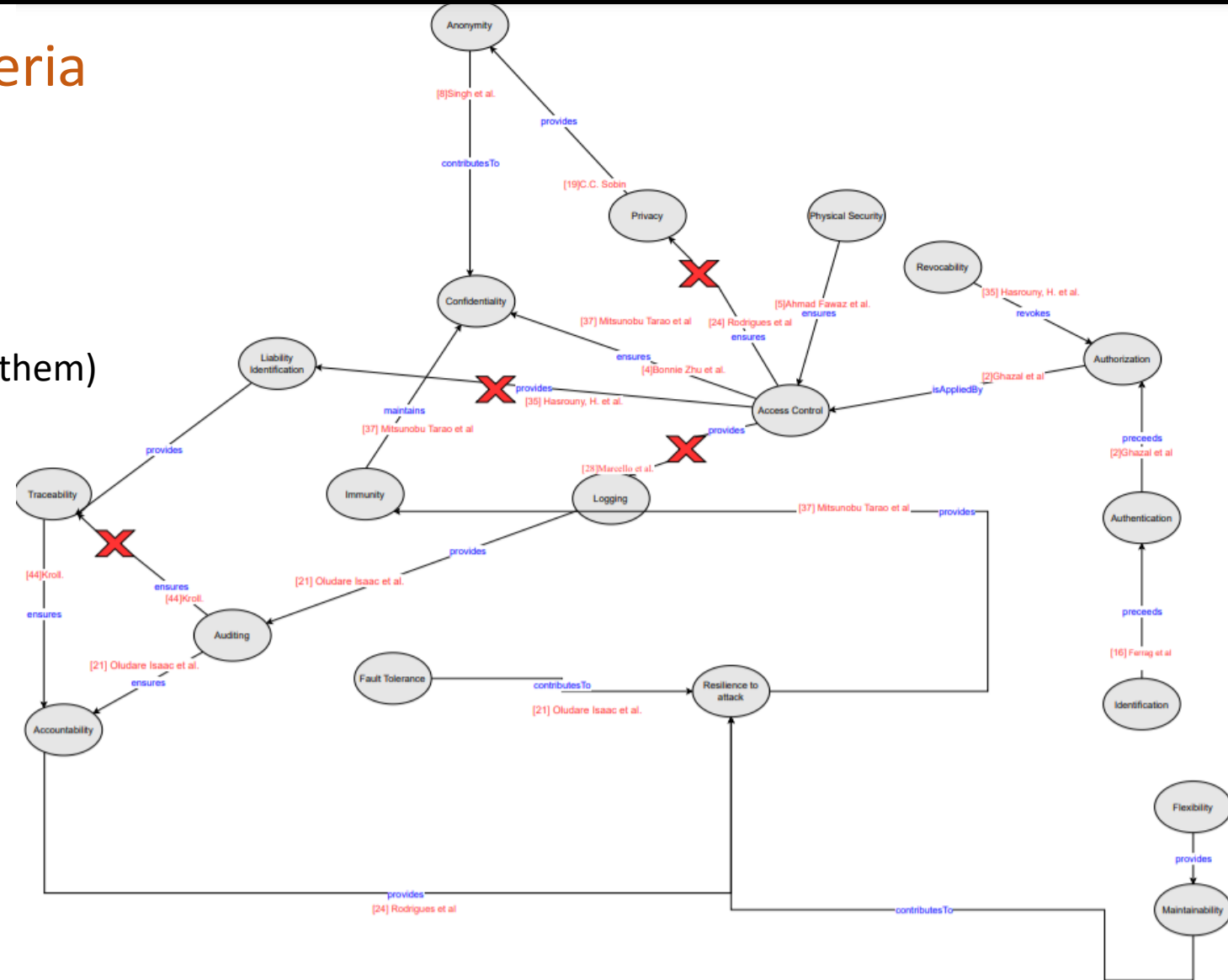
Keep Confidentiality

+

The criteria that contribute to it (all of them)

+

Break loops with repetitive criteria



Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix

Security Requirements Specification

Context

Ontology of Security Criteria – Proof of Concept

Writing Requirements With the Ontology:

Req1: The <Cellular Interface>_{system or system part} <should>_{priority} <ensure>_{process verb} <confidentiality>_{security criteria} of <data>_{asset to protect} <by Radio Canal Ciphering Algorithms>_{security mechanism}

- Req1.1: The <Cellular Interface>_{system or system part} <should>_{priority} <ensure>_{process verb} <access control>_{security criteria} of <data>_{asset to protect} <.....>_{security mechanism}
- Req1.2: The <Cellular Interface>_{system or system part} <should>_{priority} <ensure>_{process verb} <authorization>_{security criteria} of <users>_{asset to protect} <.....>_{security mechanism}

Req2: The <HSE>_{system or system part} <should>_{priority} <ensure>_{process verb} <integrity>_{security criteria} of <data>_{asset to protect} <by storing security critical data>_{security mechanism}

...

Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix

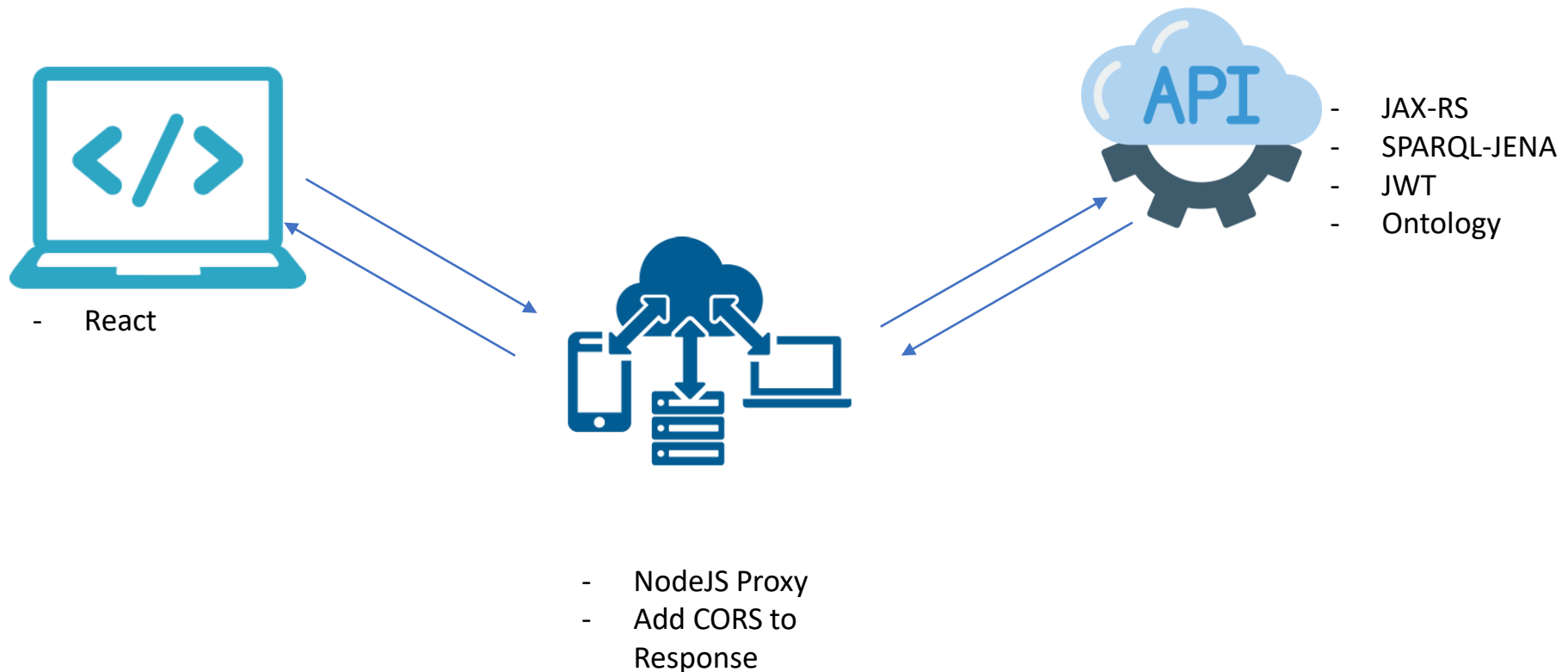
Security Requirements Specification

Context

Ontology of Security Criteria

API of Security Criteria Ontology – Web Interface:

A web interface is created to simplify the step of ontology evaluation for experts:



Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix

Security Requirements Specification

Context

Ontology of Security Criteria

API of Security Criteria Ontology – Web Interface:

A web interface is created to simplify the step of ontology evaluation for experts:

- Get the security mechanisms of security criteria in a domain

The screenshot displays the 'SECURITY CRITERIA ONTOLOGY' web interface. The navigation bar includes 'Home', 'About', 'Use Ontology', 'Visualizer', and 'Feedback'. The main content area is titled 'Use Ontology' and contains a form with the following sections:

- What is your domain?** A text input field containing 'SmartPhones'.
- What we know about your security criteria...** A row of five buttons: AUTHENTICATION, INTEGRITY, CONFIDENTIALITY, IDENTIFICATION, and NONREPUDIATION. The 'AUTHENTICATION' button is highlighted.
- You have chosen** The text 'Authentication' is displayed.
- What would you like to know?** A row of two buttons: SECURITY MECHANISMS and ADDITIONAL CRITERIA. The 'SECURITY MECHANISMS' button is highlighted.
- What we know about your security mechanisms...** A grid of 30 buttons representing various security mechanisms, including: SIGNATURE_RECOGNITION, HOMOMORPHIC_ENCRYPTION, MESSAGE_AUTHENTICATION_CODE, GAIT_RECOGNITION, CHAOTIC_HASH, TEETH_IMAGE, CLASSIFICATION_ALGORITHMS, RHYTHM, ORDER_PRESERVING_ENCRYPTION, ELECTROCARDIOGRAM, IDENTITY-BASED_ELLIPTIC_CURVE_ALGORITHM, SYMMETRIC_ENCRYPTION, PROBABILISTIC_POLYNOMIAL_TIME_ALGORITHMS, ENCRYPTION_WITH_PAIRWISE_MASTER_KEY, BEHAVIOUR_PROFILING, FINGERPRINTS, CHANNEL_CHARACTERISTICS, PATTERN, PASSWORD, TAG_NUMBER, ELLIPTIC_CURVE_CRYPTOSYSTEM, CAPACITIVE_TOUCHSCREEN, A_UNIQUE_INTERNATIONAL_MOBILE_EQUIPMENT_IDENTIFICATION_NUMBER, MULTI-TOUCH_INTERFACES, ASYMMETRIC_ENCRYPTION, CERTIFICATELESS_SIGNATURE, INITIAL_RANDOM_SEED_NUMBER, VOICE_RECOGNITION, KEYSTROKE_ANALYSIS, SELF-CERTIFIED_PUBLIC_KEYS, HASH_FUNCTION, and SCHNORRS_SIGNATURE_SCHEME.

Security Requirements Specification

Context

Ontology of Security Criteria

API of Security Criteria Ontology – Web Interface:

A web interface is created to simplify the step of ontology evaluation for experts:

- Get the suggested criteria of security criteria in a domain

The screenshot shows a web interface titled "Use Ontology" with the following steps and options:

- What is your domain?** Input: SmartPhones
- What we know about your security criteria...** Selected: AUTHENTICATION, INTEGRITY, CONFIDENTIALITY, IDENTIFICATION, NONREPUDIATION
- You have chosen** Authentication
- What would you like to know?** Selected: SECURITY MECHANISMS, ADDITIONAL CRITERIA
- What additional criteria?** Selected: ADDITIONAL CRITERIA TREE, ALL ADDITIONAL CRITERIA, HIGH PRIORITY ADDITIONAL CRITERIA, MEDIUM PRIORITY ADDITIONAL CRITERIA, LOW PRIORITY ADDITIONAL CRITERIA
- High Priority Criteria** Additional criteria that precede Authentication: IDENTIFICATION
- Medium Priority Criteria** None
- Low Priority Criteria** None

Security Requirements Specification

Context

Ontology of Security Criteria

API of Security Criteria Ontology – Web Interface:

A web interface is created to simplify the step of ontology evaluation for experts:

- Get the tree of additional security criteria
- Example: If you need confidentiality, then it is advised that you define sub-requirement with the immunity, access control ... security criteria.

Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

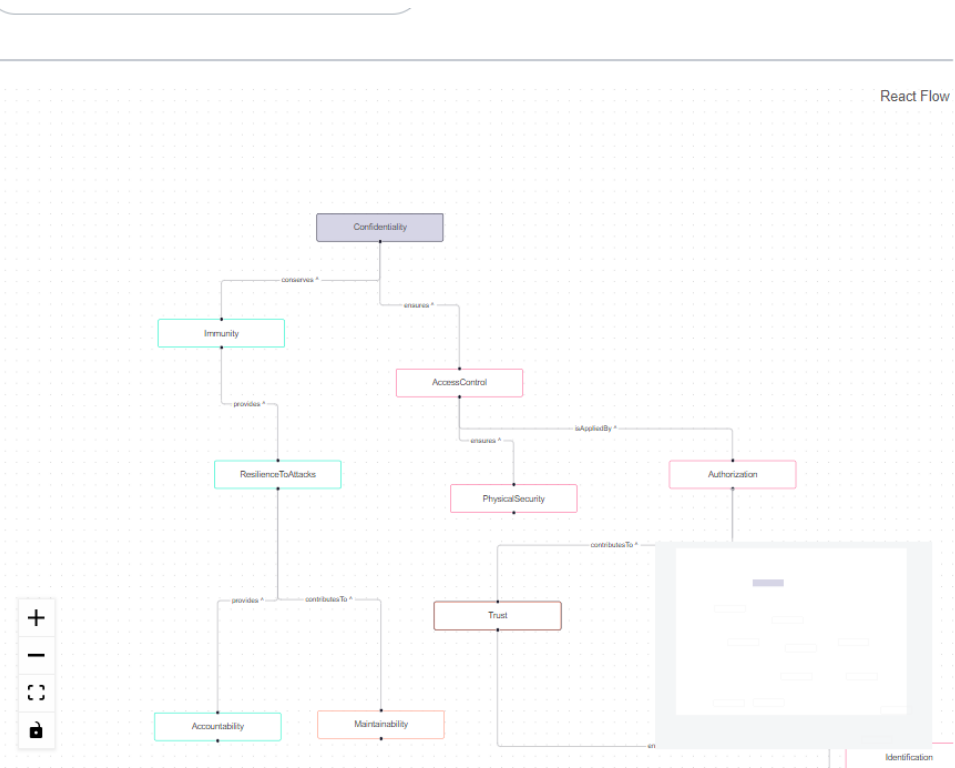
Our Approach – Proof of Concept

Appendix

Criteria Tree

Security Mechanisms:

CREDENTIAL-BASED_AUTHENTICATOR



Security Requirements Formalization

Context

SERENA

Soyer et al. Example

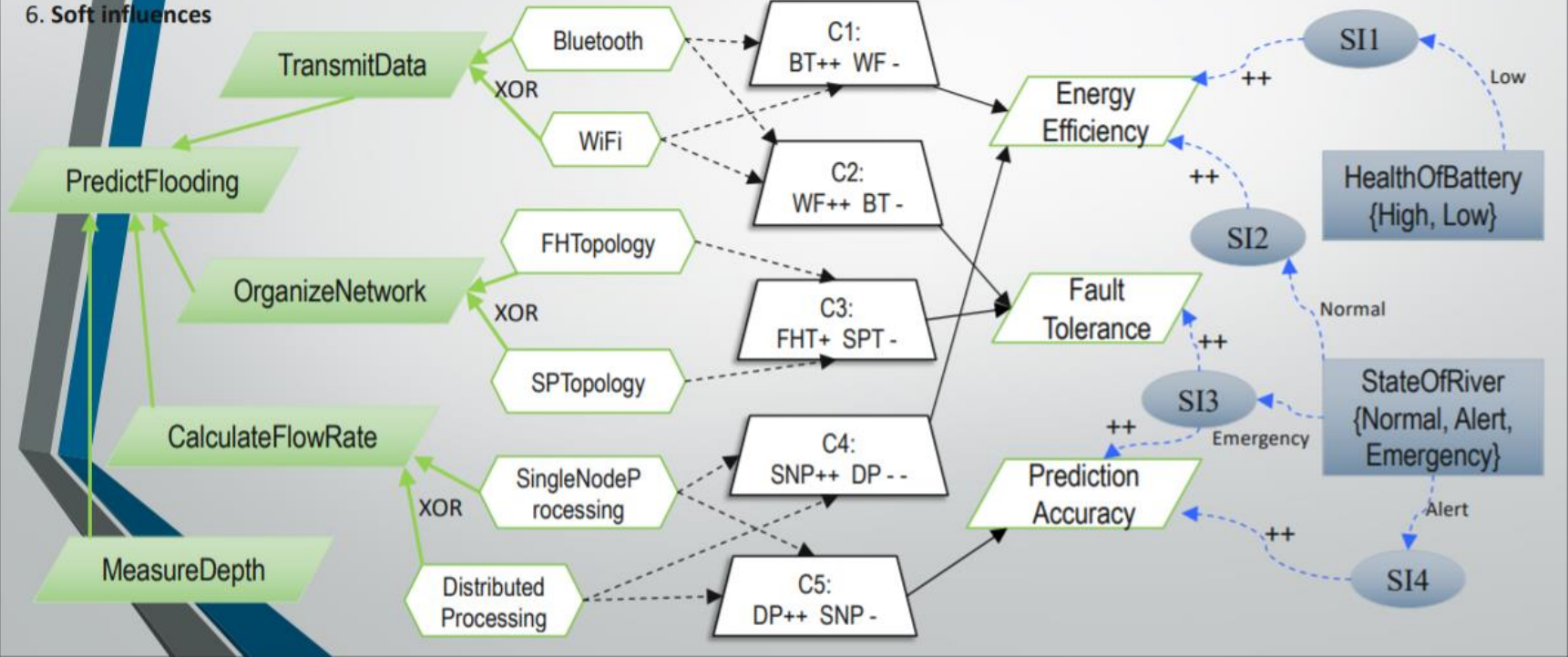
Innovative nature of the project

Methodology

Representation:

1. Goals
2. Softgoals
3. Goal operationalizations
4. Claims
5. Context variables
6. **Soft influences**

Soft influences express required levels of softgoal satisfaction for a particular context variable value. They are soft in the sense that it may prove impossible to satisfy them for all possible values.



Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix

Security Requirements Formalization

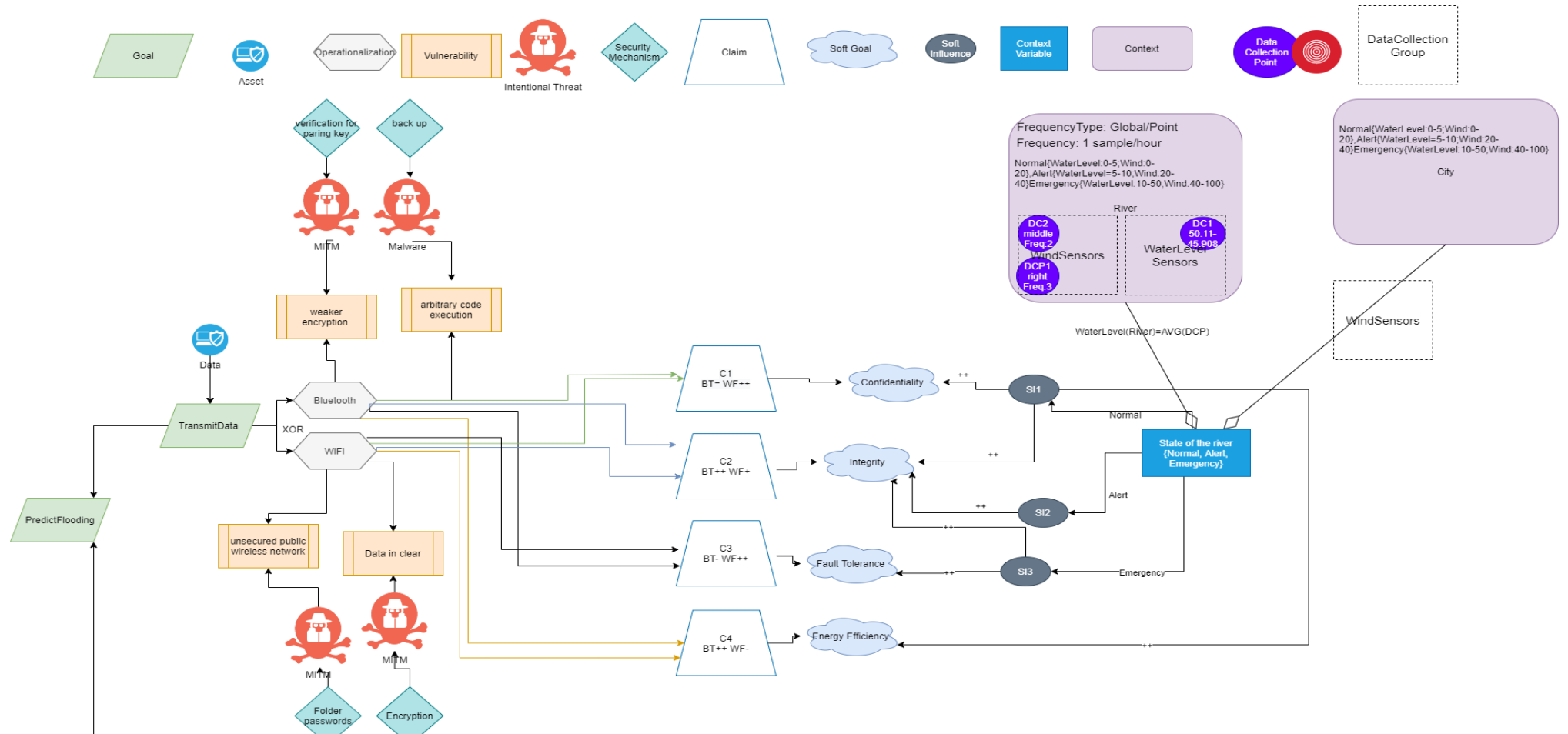
Context

SERENA

Example

Context has:

- Frequency if global for all data collection points
- ContextLevels
- DataCollectionGroups (According to the sensor or data needed) that have:
 - Frequency if not global in context
 - Data Collection Points that have:
 - Location
 - Frequency if not global in context or DataCollectionGroup



Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix

Security Requirements Formalization

Context

SERENA

Example in VariaMos

Innovative nature of the project

Methodology

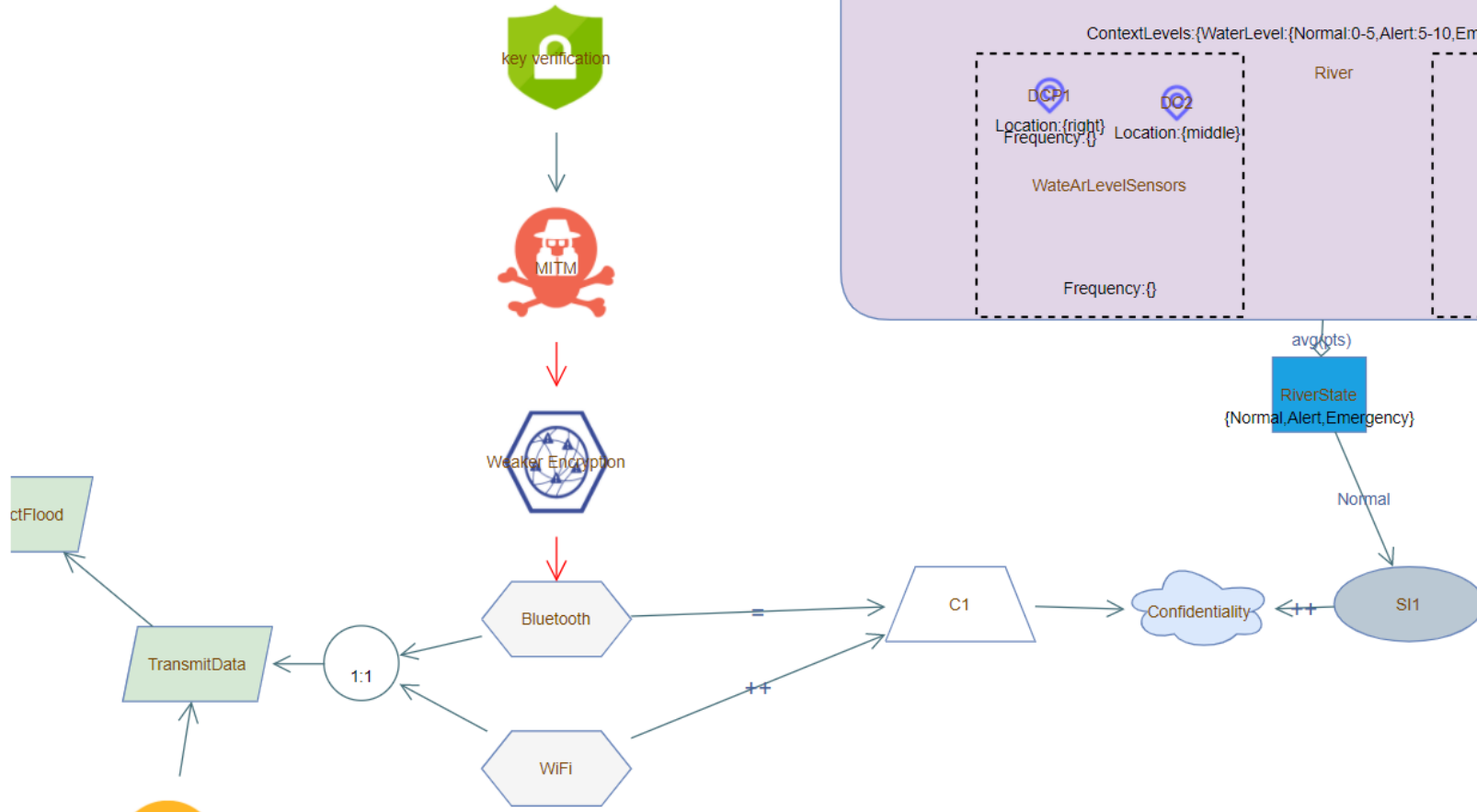
Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix



Security Requirements Formalization

Context

SERENA

Security Criteria Diagram (Like asset diagram in CORAS)?

Innovative
nature of the
project

Methodology

Concepts

Proof of
Concept
Example

State of Art –
Proof of
Concept

Our Approach
– Proof of
Concept

Appendix



Let the user add the goals they need then use the ontology in a risk mode (For example, the user needs confidentiality and privacy in the system. If a threat denies (to a certain level) confidentiality, it also denies privacy with a level that depends on the relationship defined between confidentiality and privacy in the ontology (level of confidentiality denial divided by the level of relationship). Another idea: suggest additional security criteria?

Security Requirements Formalization

Context

SERENA

Security Criteria Diagram (Like asset diagram in CORAS)?

Innovative nature of the project

Methodology

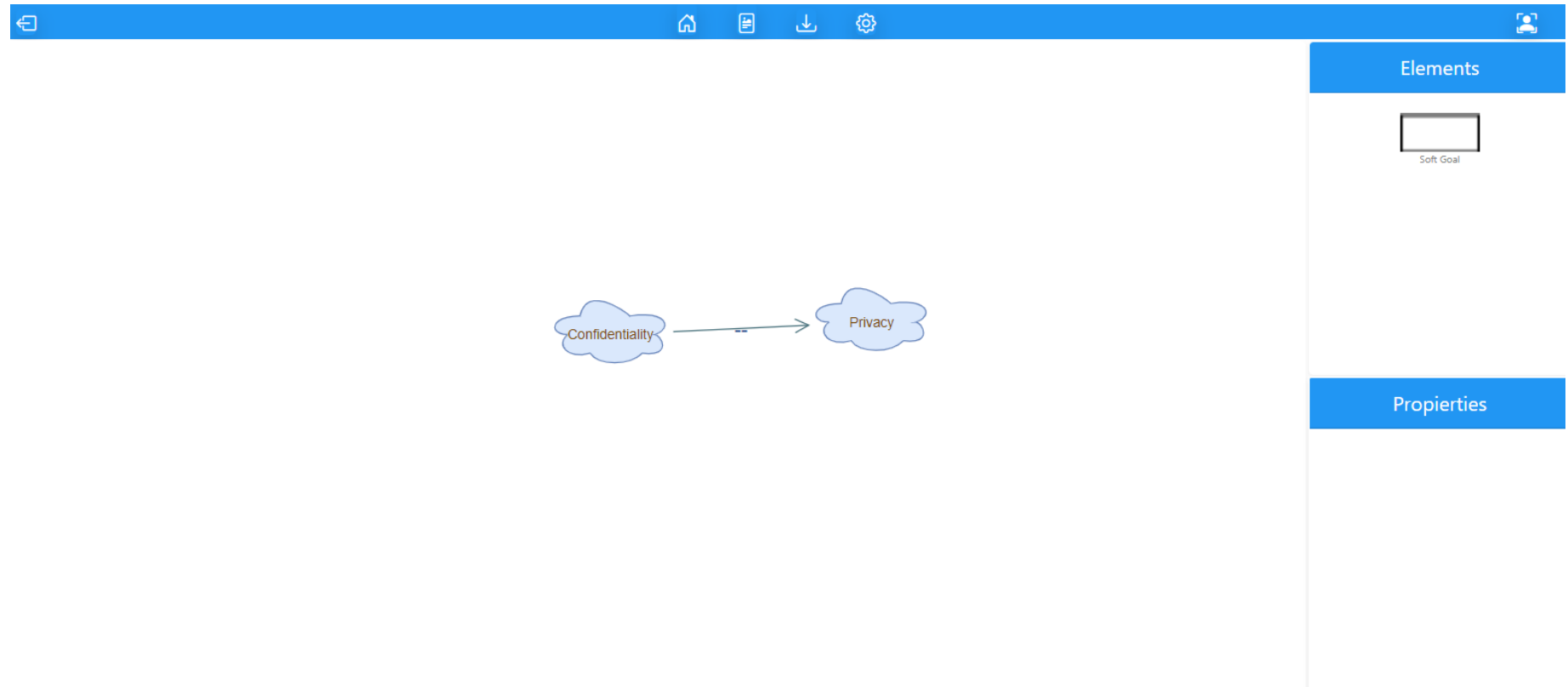
Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix



Security Requirements Formalization

Context

SERENA

Risk Diagram Suggestion

Innovative nature of the project

Methodology

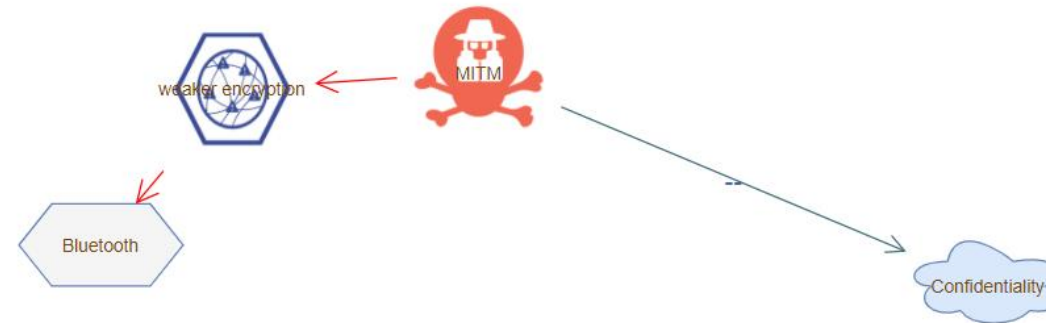
Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix



Elements



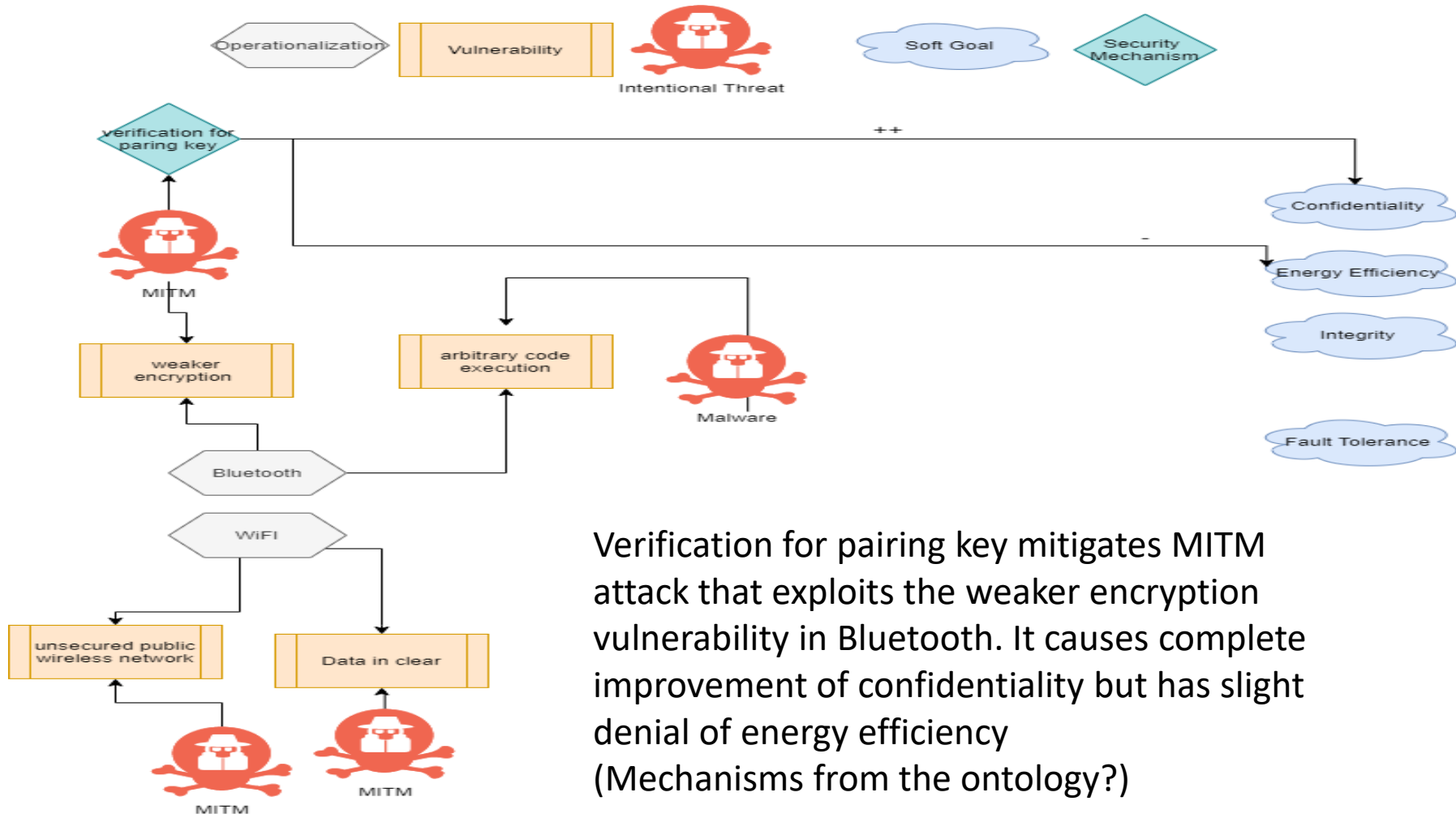
Properties

Security Requirements Formalization

Context

SERENA

Treatment Diagram Suggestion



Verification for pairing key mitigates MITM attack that exploits the weaker encryption vulnerability in Bluetooth. It causes complete improvement of confidentiality but has slight denial of energy efficiency (Mechanisms from the ontology?)

Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix

Security Requirements Formalization

Context

SERENA

Treatment Diagram Suggestion

Innovative nature of the project

Methodology

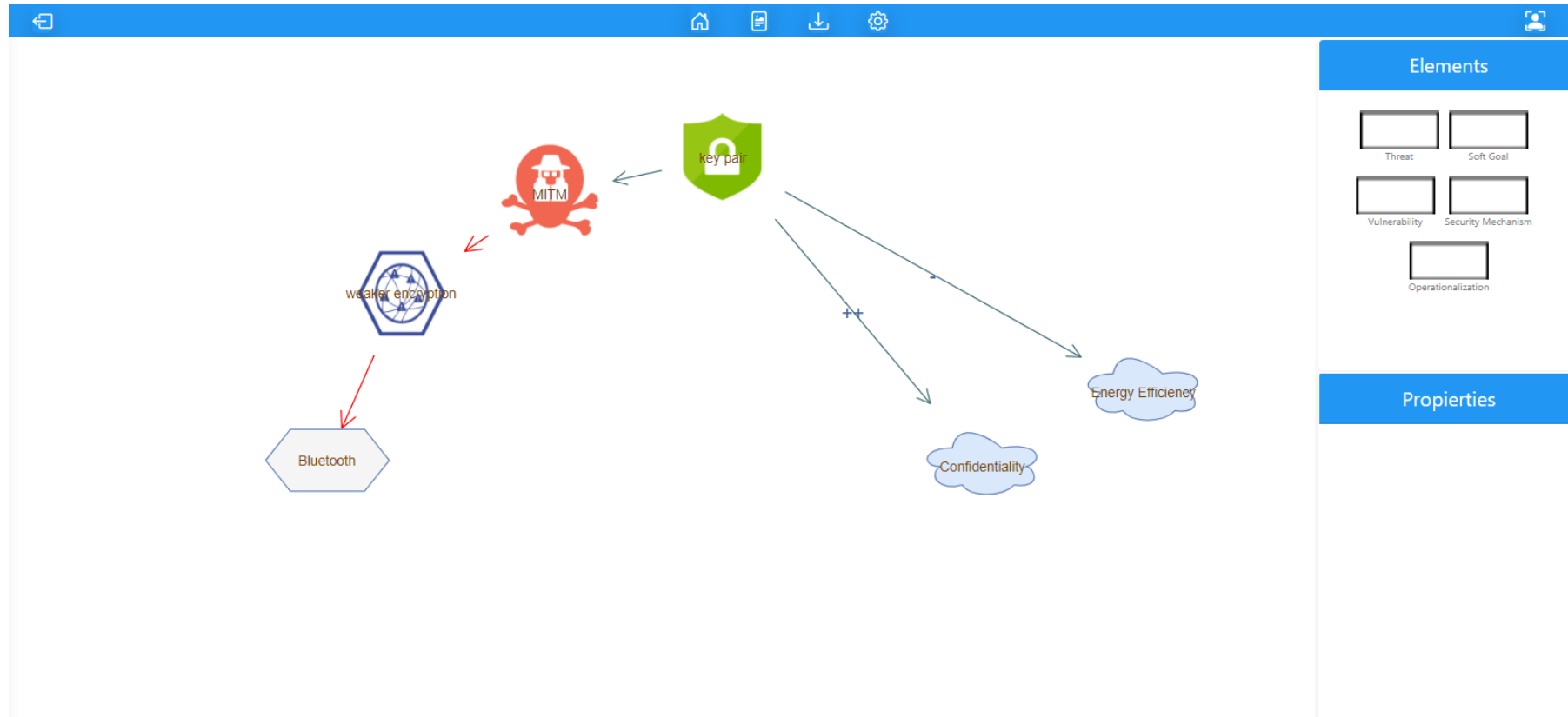
Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix



Security Analysis

Context

SERENA Using Variamos

1- Abstract Syntax – Language definition (Elements & Relationships & Restrictions) (JSON)

```
{  
  "elements": {  
    "Goal": {  
      "properties": [ {  
        "name": "Description",  
        "type": "String",  
        "comment": "Functional Goal"  
      } ]  
    }  
  }  
}
```

1- Concrete Syntax – Graphical Definition of the Language (JSON)

```
{  
  "elements": {  
    "Goal": {  
      "draw": "PHNoY"  
      "icon": "  
        {  
          "label": "Goal",  
          "width": 100,  
          "design": "shape=Goal",  
          "height": 50,  
          "label_property": "Description"  
        }  
      }  
    }  
  }  
}
```



1 - I want to create a new language!

2- I want to create a model using this language!

3- I want to analyze the model I created

```
{  
  "elements": {  
    "Goal(G,[SGs],[OPs],Card)": {  
      "minizinc": {  
        "type": "var 0..1",  
        "value": "",  
        "constraints": [ {  
          "condition":  
            "target(Rel(SubGoal))" "constraint": "G=1",  
          } ]  
        }  
      }  
    }  
  }  
}
```

Upload

Upload



Variamos Model JSON + Semantic Definition JSON + Name of the model + Type of the model (domain or application)

Translator (minizinc)



Minizinc code of the model

3-Semantic Syntax – How is the language translated (JSON). Example: How to translate a SecureKAOS model into minizinc code.

Innovative nature of the project

Methodology

Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix

Security Analysis

Context

SERENA Using Variamos

Innovative nature of the project

Methodology

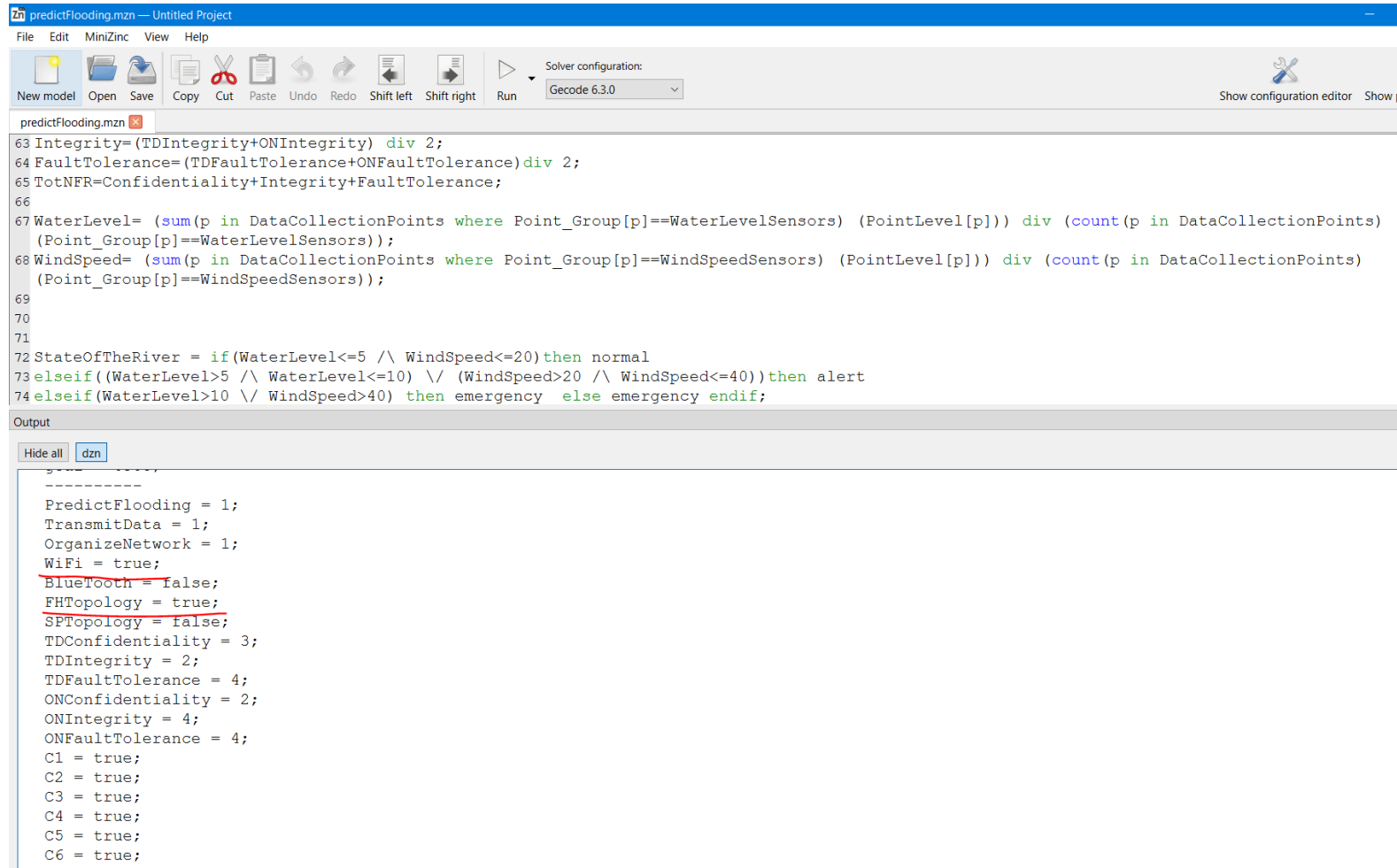
Concepts

Proof of Concept Example

State of Art – Proof of Concept

Our Approach – Proof of Concept

Appendix



```
predictFlooding.mzn — Untitled Project
File Edit MiniZinc View Help
New model Open Save Copy Cut Paste Undo Redo Shift left Shift right Run Solver configuration: Gecode 6.3.0
Show configuration editor Show p

predictFlooding.mzn
63 Integrity=(TDIntegrity+ONIntegrity) div 2;
64 FaultTolerance=(TDFaultTolerance+ONFaultTolerance)div 2;
65 TotNFR=Confidentiality+Integrity+FaultTolerance;
66
67 WaterLevel= (sum(p in DataCollectionPoints where Point_Group[p]==WaterLevelSensors) (PointLevel[p])) div (count(p in DataCollectionPoints)
(Point_Group[p]==WaterLevelSensors));
68 WindSpeed= (sum(p in DataCollectionPoints where Point_Group[p]==WindSpeedSensors) (PointLevel[p])) div (count(p in DataCollectionPoints)
(Point_Group[p]==WindSpeedSensors));
69
70
71
72 StateOfTheRiver = if(WaterLevel<=5 /\ WindSpeed<=20)then normal
73 elseif((WaterLevel>5 /\ WaterLevel<=10) \/ (WindSpeed>20 /\ WindSpeed<=40))then alert
74 elseif(WaterLevel>10 \/ WindSpeed>40) then emergency else emergency endif;

Output
Hide all dzn
-----
PredictFlooding = 1;
TransmitData = 1;
OrganizeNetwork = 1;
WiFi = true;
BlueTooth = false;
FHTopology = true;
SPTopology = false;
TDConfidentiality = 3;
TDIntegrity = 2;
TDFaultTolerance = 4;
ONConfidentiality = 2;
ONIntegrity = 4;
ONFaultTolerance = 4;
C1 = true;
C2 = true;
C3 = true;
C4 = true;
C5 = true;
C6 = true;
```