BIECO

Building Trust in Ecosystems
and Ecosystem Components

Improving security and trust at a supply chain level.

bieco.org

The BIECO Approach

BIECO
Building Trust in Ecosystems and Ecosystem Components

The ongoing events of this decade have once more brought to the limelight the importance of ensuring proper cybersecurity and safety of Europe's critical infrastructure. As one of the more significant examples, the war in Ukraine has led to one of the largest energy crises in recent history, with experts warning that if sustained cyberattacks are targeted at the European energy sector the consequences could be disastrous. Interruptions to the already fragile energy markets could further raise fuel prices to hundreds of millions of consumers, contributing to further economic and human losses. Nevertheless, this represents a major cross-sectorial challenge, with many interdisciplinary challenges to be addressed.

As such, it is crucial European industry leaders and policy makers to bolster the overall resilience of Europe's key infrastructure against cyber attacks and vulnerabilities, with efforts including for instance the promotion of security-by-design and improved risk and vulnerability management across the value chain.

In this light, BIECO can provide a holistic approach to improve security in complex ecosystems and ecosystem components along their lifecycle, improving trust at a supply chain level.

BIECO
Building Trust in Ecosystems and Ecosystem Components

The BIECO Approach

BIECO includes over 15 different tools covering the software lifecycle from design to runtime. The large majority of these tools is integrated into a common platform to facilitate their interoperability and orchestration in easily deployed tool chains tailored to address specific business needs.

With these, BIECO leverages a combination of state-of-the-art artificial intelligence, digital twins, simulation and static analysis to address the following key areas:

- Vulnerability Assessment and Management
- Risk Assessment and Mitigation
- Resilience Mechanisms
- Security Certification and Testing
- Runtime Auditing of ICT Ecosystems

Given the cross-sectorial nature of the cybersecurity challenges currently faced in Europe, BIECO's validation takes place across three distinct business cases spanning different activity sectors, namely Energy (ICT Gateway from Resiltech, Pisa, Italy), Manufacturing and Electric Mobility (Smart Microfactory from IFEVS, Turin, Italy) and Finance (AI Investment Platform from 7Bulls, Warszawa, Poland).

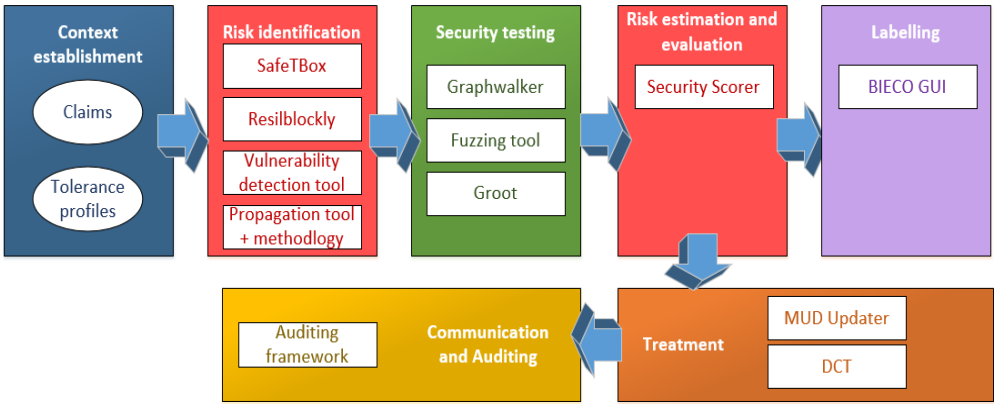
SECURITY EVALUATION METHODOLOGY

BIECO
Building Trust in Ecosystems and Ecosystem Components

BIECO defines a security evaluation methodology for complex systems based on ISO 31000, ISO 29119 and MUD standards. It is intended to serve as a basis for the security certification, providing the following **advantages**:

- Basic set of claims from standards and best practices
- Objective, automated, flexible and empirical evaluation combining testing and risk assessment
- Different security for different contexts using tolerance profiles
- Safety, operational, economical, privacy and legislative aspects considered
- Visual and dynamic label to show the results to users
- Security configuration recommended after assessment (MUD)
- Auditing process to detect suspicious behaviours and restart the evaluation

The methodology has been instantiated using tools developed within BIECO for risk assessment (risk propagation, safety assessment, modelling or detection) and testing (model-based testing, fuzzing and combinatorial).



BIECO
Building Trust in Ecosystems and Ecosystem Components

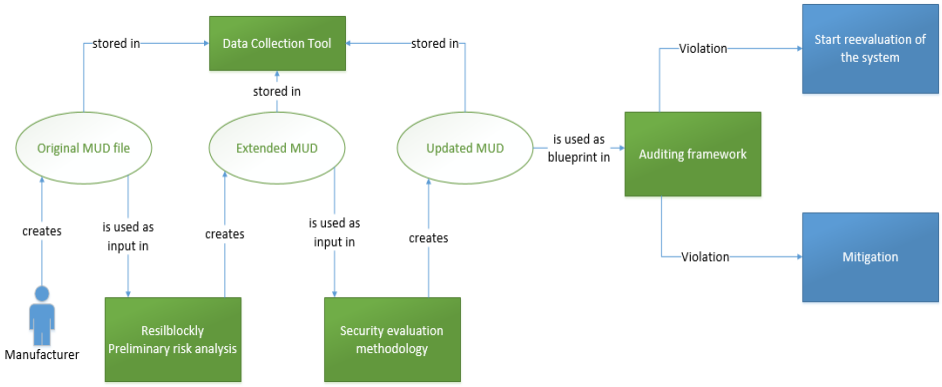
Manufacturer Usage Description (MUD) file

MUD is an IETF standard intended to limit the attack surface of a IoT device by allowing manufacturers to establish network behaviour profiles in a flexible and scalable way.

BIECO improves and integrates this standard to manage the security of a device during its whole lifecycle:

- Integration of the MUD information in the system modelling activities
- Extended MUD model to integrate additional information beyond network layer
- Usage of the MUD to detect misbehaviours at runtime
- Secure storage and retrieval of the MUD
- Generation of extended MUD from the assessment process and testing results to provide recommended security configuration

Security evaluation results are typically used only to validate or certify the security of the system, missing valuable information that reports security flaws and mitigation actions.



29 file (58 de pagini)
albe (netipărite)
În total broșura va avea 40 file (80 de pagini) + 2 coperți

ResilBlockly

BIECO
Building Trust in Ecosystems and Ecosystem Components

ResilBlockly is a tool for Model-Based Design and Safety+Security Assessment of complex System-of-Systems (SoS).

Some of its new **features** in BIECO are:

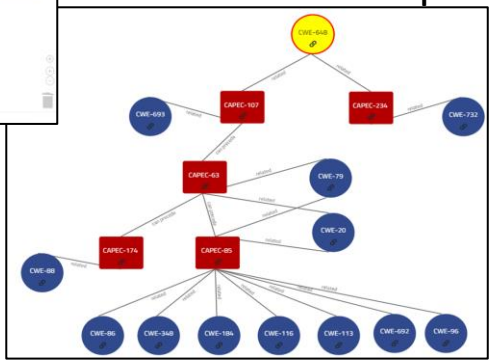
- Security threat modelling, risk analysis, and graphical representation of attack paths;
- Integration with open catalogues of vulnerabilities, weaknesses and attack patterns (CWE, CVE, CAPEC).

Stakeholders might be interested in ResilBlockly since:

- it allows the creation of customized profiles for any domain or context of use;
- it supports the early identification of vulnerabilities;
- it allows prevention and prompt intervention to reduce the likelihood of exploitation by attackers;
- It supports in activities required for the compliance with security standards (e.g., IEC 62443).

Model Designer

Attack Graph



RESILTECH
Technologies for Resilience

BIECO
Building Trust in Ecosystems and Ecosystem Components

SafeTbox: Model-Based Safety Engineering Tool

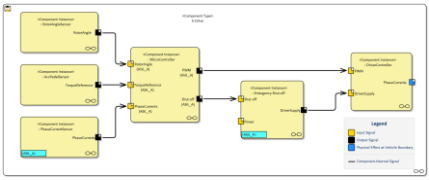
Challenge

- Safety assurance for complex systems
- Analysis information management
- Trace requirements from specification to production
- Associate safety with security requirements

Solution

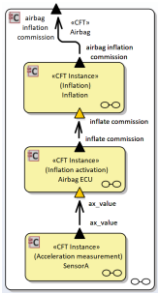
- Model-based Safety Assurance
- Enterprise Architect Add-In
- Supports **traceable**
  - System modeling
  - Hazard Analysis and Risk Assessment
  - Failure Analysis
  - Safety Case Modeling
  - Conditional Safety Certificates
- Integrates with ResilBlockly for security assurance

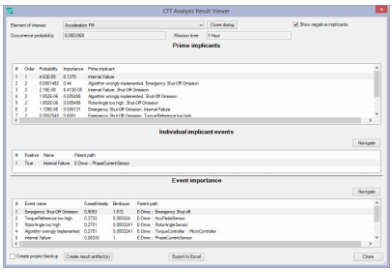
System Modeling



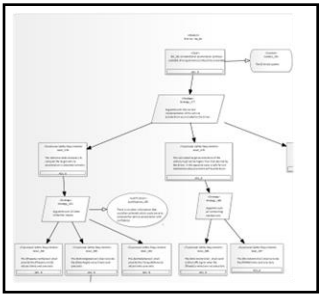
ResilBlockly

Failure Analysis





Safety Cases



Fraunhofer IESE

safeTbox

ConSerts: Conditional Safety-Security Certificates

BIECO
Building Trust in Ecosystems and Ecosystem Components

Adapting to risk statically means assuming worst-case conditions, which kills performance when this happens.

BIECO's ConSerts can help your system do better.

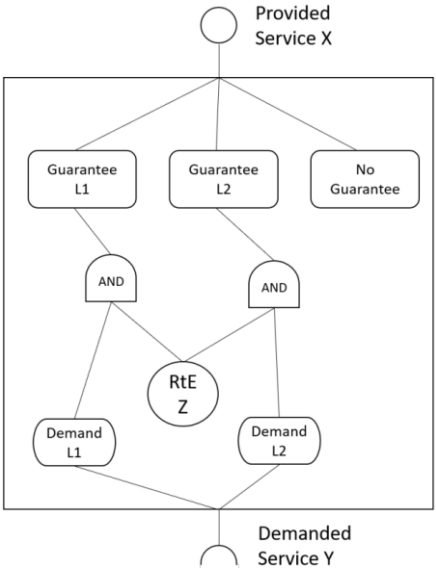
ConSerts allow you to associate different operational conditions with risk guarantees based on your provided and required services.

Guarantees represent the level of freedom from risk your service offers based on current operational conditions.

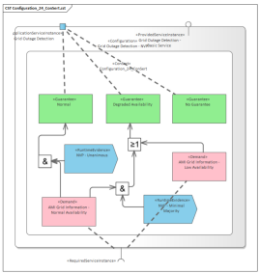
Demands represent the necessary guarantees your required services must provide for your guarantees to be satisfied.

Runtime Evidence (**RtE**) represent information your own system monitors and makes available to support your guarantees.

Abstract ConSert



ConSert modeled in SafeTbox



With ConSerts, you can

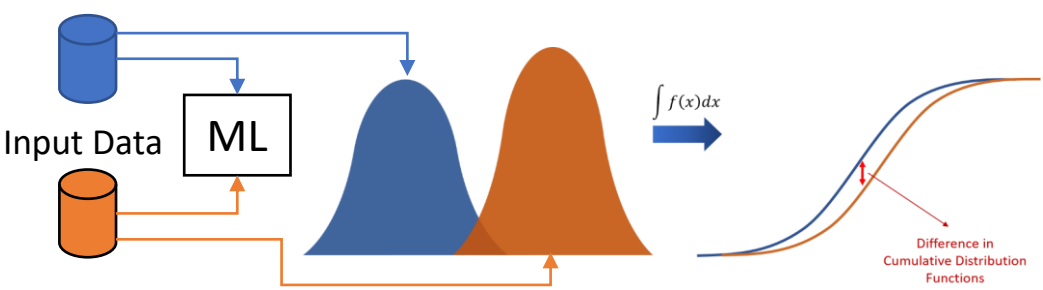
- **Build your system to adapt using risk awareness.**
- **Compose your system-of-systems services while being risk-compatible.**

Fraunhofer IESE

SafeML: Statistical Dissimilarity Measures for ML Uncertainty Estimation

3ECO
Building Trust in Ecosystems and Ecosystem Components

An ML model applied to a novel context is uncertain to perform as expected. Thus, we need to check if the application context of the input has changed compared to the training.



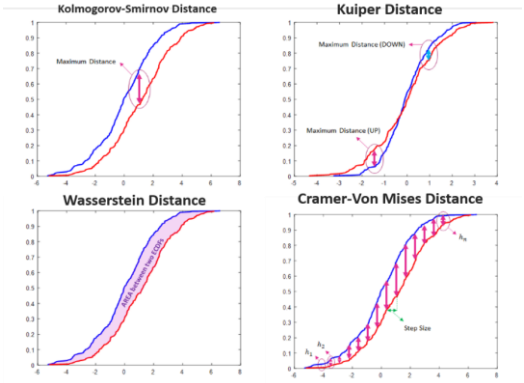
"SafeML" is a collection of statistical measures which evaluate whether samples from two datasets are likely to belong to the same distribution (see top figure).

The measures are based on the Empirical Cumulative Distribution Function (ECDF), and compare in various ways the difference across the two datasets (see bottom-right figure).

Using SafeML, you can estimate uncertainty

- **Evaluate, during ML model development, whether the model is robust to data deviation.**
- **Evaluate, during ML model operation, whether input data is similar to training.**

Statistical Dissimilarity Measures



Fraunhofer IESE

Vulnerability Detection Tool

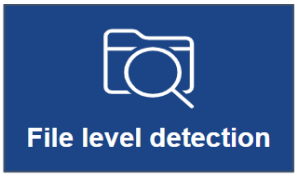
BIECO
Building Trust in Ecosystems and Ecosystem Components

The Vulnerability Detection Tool integrated in BIECO detects vulnerabilities within the source code by a static analysis and the use of ML techniques.

One of the main factors which can help attackers to corrupt a system is the existence of vulnerabilities in the code. Thus, it is vital to execute a suitable vulnerability assessment to the code in a quick way. The tool allows companies to offer an extra level of security by detecting possible security breaches within the source code in the form of vulnerabilities in an **automatic way**.

Using the tool, it is possible to obtain:

- ✓ **One tool for different languages**, since it is applicable for the tree main programming languages (**Python**, **Java** and **C**).
- ✓ Discover unidentified vulnerabilities, also called **0-day vulnerabilities**.
- ✓ Detection of the vulnerable file, which helps the expert to **focus efforts** for its analysis.



gradiant

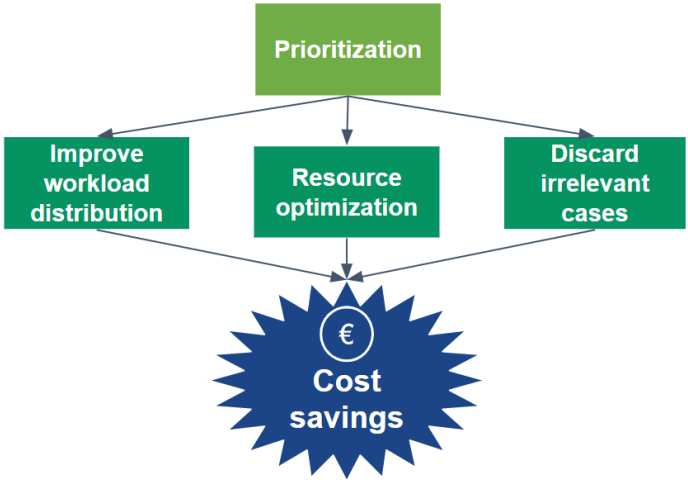
BIECO
Building Trust in Ecosystems and Ecosystem Components

Vulnerability Exploitability Forecasting Tool

The Vulnerability Exploitability Forecasting Tool provides the probability of a known published vulnerability to be exploited in a time window.

Onces a known vulnerability is detected within the source code, it is necessary to focus the efforts to mitigate its possible attacks. From BIECO, we are conscious that experts needs to prioritise possible attacks for a more effective results. Thus, the exploitability forecasting tool offers an assessment of a given **CVE** by indicating if it can be **exploited in the next 3, 6 or 12 months from the date of publication.**

This helps cyber analytics to **prioritise** the analysis of a vulnerability and its mitigation, **saving time, efforts and**, consequently, **money.**



gradiant

Vulnerability Propagation Tool

BIECO
Building Trust in Ecosystems and Ecosystem Components

The main goal of the Vulnerability Propagation Tool is to find and indicate the components or elements a single vulnerability can affect and, therefore, its path within the source code.

Sometimes, the most obvious way to reach a vulnerability is by knowing its location. But vulnerabilities can propagate through the source code, offering open doors to cyber attackers to exploit them. Calculating the path affected by a vulnerability helps the cyber security expert to **prioritise its mitigation** not only directly, but their possible **alternative access in the source code**.

With this tool, cyber analytics will be able to:

- ✓ Obtain the propagation **path** of a located vulnerability within the source code in the **3 main languages.**

- ✓ Have a measure of the **magnitude of the vulnerability** in the source code, helping the assessment process.

- ✓ Have more detailed information for **mitigation strategies.**

gradiant

BIECO
Building Trust in Ecosystems and Ecosystem Components

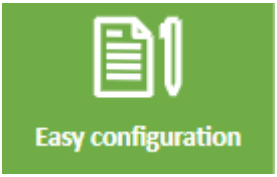
Fuzzing Tool

The Fuzzing Tool offered in BIECO finds, through a dynamic analysis, security weaknesses in a REST API which might be related to a possible vulnerability in the system.

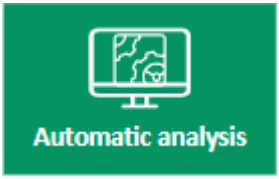
The existence of this tool within the BIECO framework allows companies to offer an extra level of security, using the description of the API to analyse which request can lead to an **undesired response**.

The tool offers:

- ✓ **Easy configuration**. It only requires a Swagger file as input.



- ✓ **Automatic analysis of the output**. The output do not need to be analysed by the user.



- ✓ Determine if the service is susceptible to **Buffer overflow**, **Path transversa**l, **Command injection**, **Code injection** and **SQL injection**.

gradiant

GROOT

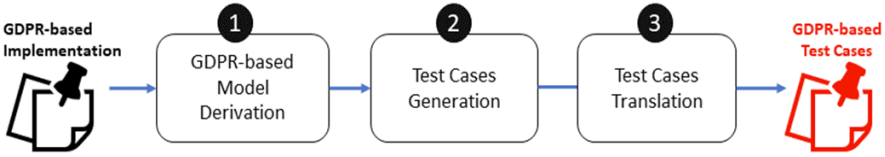
GdpR-based cOmbinatOrial Testing Tool

BIECO
Building Trust in Ecosystems and Ecosystem Components

ICT systems are currently adopting different means of managing personal data. Effective and efficient validation methods must be applied, considering the peculiarity of the reference legal framework, i.e., the General Data Protection Regulation (GDPR).

GROOT is based on a combinatorial testing methodology for assessing the compliance with the GDPR in the access control domain.

- It guarantees the trustworthiness of (personal or sensitive) data;
- It protects information technology systems against inappropriate or undesired user access.



GROOT

1. Derives the set of parameters P, and the associated set of sets V;
2. Provides different combinatorial strategies such as: all-combinations, pairwise combinations or t-wise combinations;
3. Provides executable test case according to the domain specific language.

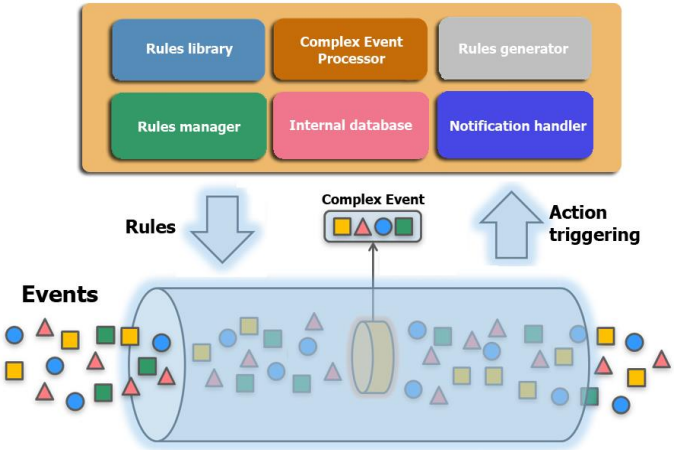
For more details, please see the GROOT video at:
https://www.youtube.com/watch?v=k-K2Fs0hvR4

BIECO
Building Trust in Ecosystems and Ecosystem Components

Runtime Monitoring

The Runtime Monitoring provides:

- **Runtime evaluation of functional and non-functional properties;**
- **Notification of properties violations;**
- **Countermeasures enforcement.**



Main Features:

- Runtime rules evolution, generation and instrumentation;
- Supports BPMN model for SUT behavioral specification;
- Event-based for loosely-coupled heterogeneous comms;
- Multiple CEP instances and languages supported;
- Smart-agents for injecting countermeasures during execution;
- Multiple probes and smart-agents available;
- Report integration with Grafana, InfluxDB;
- Available for free under GPL3 License.

https://github.com/ISTI-LABSEDC/Concern

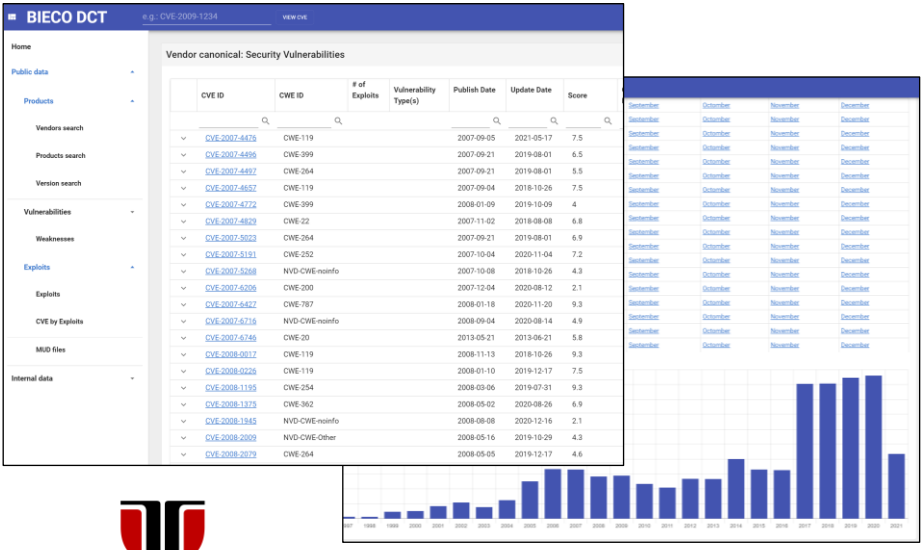
Data Collection Tool

BIECO
Building Trust in Ecosystems and Ecosystem Components

The Data Collection Tool (DCT) is a repository of vulnerabilities, weaknesses, exploits, Manufacturer Usage Description (MUD) files and bugs.

The vulnerabilities data structure is modeled based on the Common Vulnerabilities and Exposures (CVE) and Common Platform Enumerations (CPE) from the National Vulnerability Database (NVD), and on the Common Weakness Enumeration from MITRE. The exploits data structure is designed to keep information gathered from the Exploit Database (EDB).

The DCT has a web interface and communicates with the other BIECO tools through a REST API.



TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

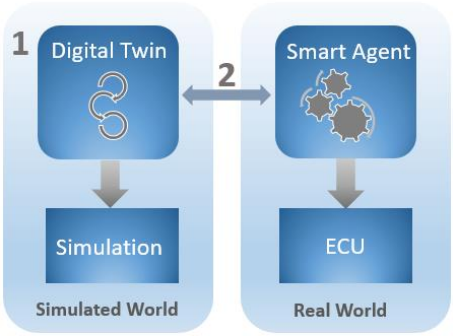
Predictive Simulation

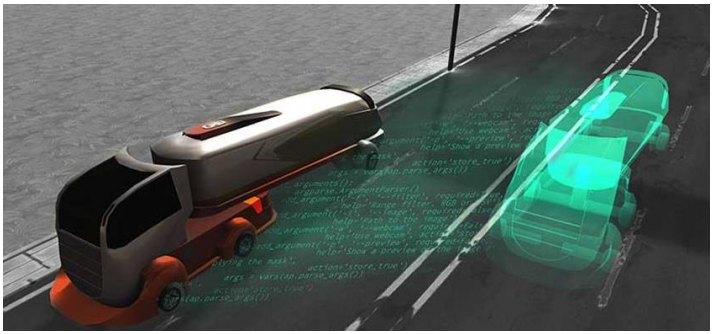
Challenge

- Trustworthy Integration of 3rd party Black Box Components
- Ensure Safety when security attacks manifest at Runtime

Solution

- Runtime Prediction of behavior that enables timely safe reaction
- Prediction within a virtual environment where virtual, not real world entities are endangered

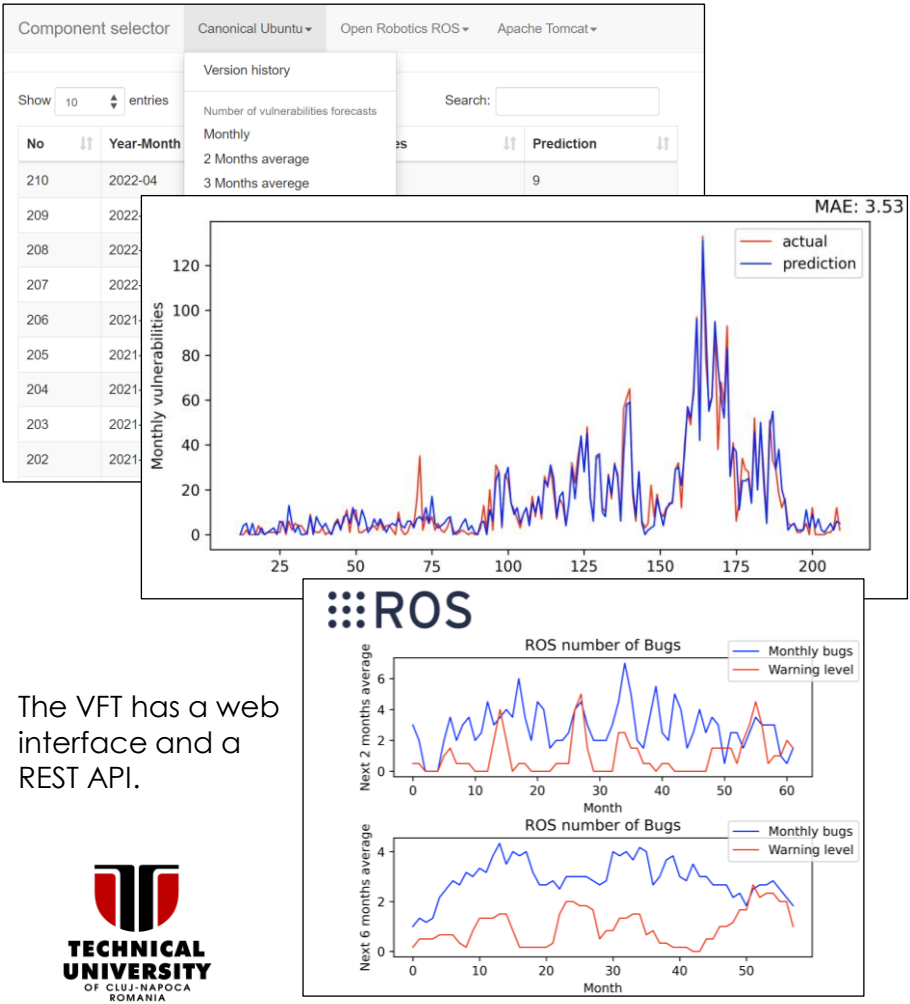




Vulnerabilities Forecasting Tool

BIECO
Building Trust in Ecosystems and Ecosystem Components

The Vulnerabilities Forecasting Tool (VFT) provides an estimation of the number of bugs and vulnerabilities to be expected for the main software components used within complex ICT systems.



The VFT has a web interface and a REST API.

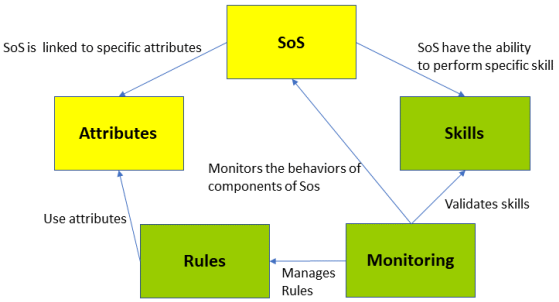
TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

DAEMON

Domain bAsEd Monitoring ONtology

DAEMON is an ontology that formally models knowledge about Monitoring and System of Systems (SoS) domains.

The main objective of DAEMON is to provide stakeholders with functional and non-functional properties of different parts of SoS, and the corresponding definition of concrete monitoring rules.



As a result, a set of meaningful reference rules to be monitored during the SoS execution are defined to automatically demonstrate the compliance (non-compliance) with the selected properties.

DAEMON is divided into 5 modules:

1. **SoS**: composition of System, influenced by a specific environment in which it operates and is executed
2. **Attributes**: functional and non-functional property related to a specific SoS concept
3. **Skills**: ability of an agent to perform a specific action
4. **Rules**: set of instructions related to analysis of the occurrences of one or more events in a stream or a cloud of events
5. **Monitoring**: observes rules organized in Calendar (each Calendar is able to validate a specific *Observable Skill* at run-time defined in the Skills module).

DAEMON architecture

Ontology Server RESTful

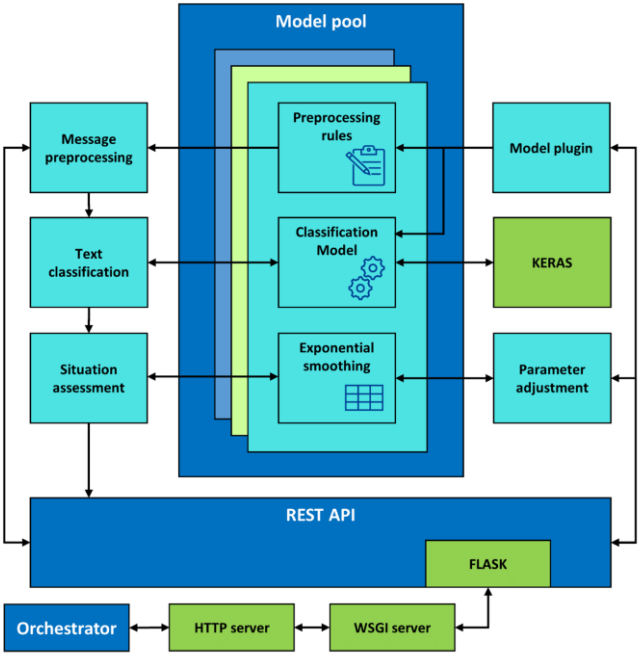
Failure Prediction Tool

BIECO
Building Trust in Ecosystems and Ecosystem Components

The Failure Prediction Tool (FPT) monitors the logs of the components that make up one or more systems at run time and forecasts their failures.

FPT classifies each log message using a neural network model, then calculates an alert level using exponential smoothing.

The tool supports model plugins and parameter adjustments.

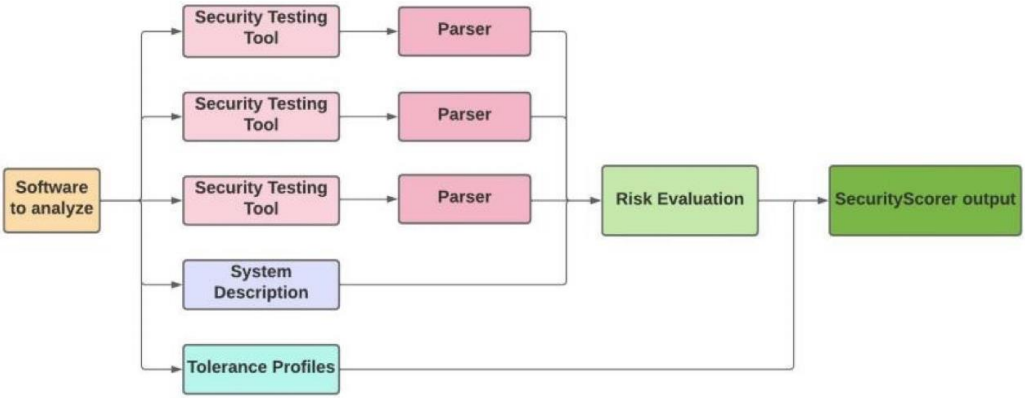


TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

BIECO
Building Trust in Ecosystems and Ecosystem Components

SecurityScorer

SecurityScorer is a tool that analyzes the outputs of the system testing tools and system description to evaluate numerical results describing system safety.



SecurityScorer is used in the Risk Estimation and Evaluation phases of the BIECO methodology. It takes the output of each tool used in the previous phases and analyzes it. Then, using the system description file and tolerance profiles, SecurityScorer creates an internal representation of the system and links the test results to the proper parts of the system.

With all this information, SecurityScorer implements and evaluates the mathematical model described by the BIECO to calculate the final results for the security categories.

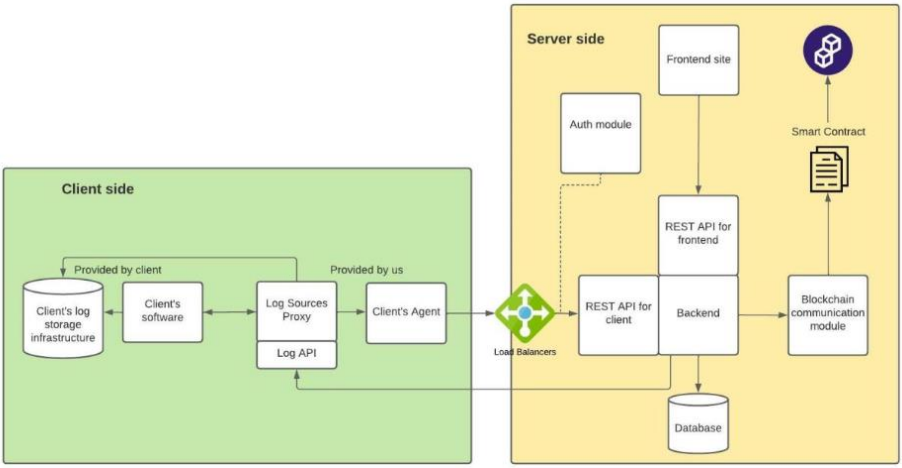
```
{
  "scores": {
    "confidentiality": 1.0,
    "integrity": 2.0,
    "availability": 0.0,
    "authorization": 4.2,
    "authentication": 0.6,
    "non_repudiation": 1.0
  }
}
```

7bulls.com

LogForgeryBlocker

BIECO
Building Trust in Ecosystems and Ecosystem Components

LogForgeryBlocker enhances the security of the application logs providing non-repudiation thanks to blockchain technology.



It consists of two parts: central app and clients, deployed onto any number of your app servers, VMs, etc.

Clients monitor the log files you specified and communicate with the server, providing updates.

The server is configured to use a blockchain of your choice to store the logs. Precisely, a special hash function of new log contents is calculated, and only that hash is then stored in the blockchain.

This solution allows for the non-repudiation of logs. It means you can always verify if your logs were modified or deleted by comparing them to the hashed information stored in the blockchain. For example, you can detect a situation when an attacker deleted the logs showing malicious behavior on your server.

7bulls.com

BIECO
Building Trust in Ecosystems and Ecosystem Components

The BIECO consortium

Building Trust in Ecosystems and Ecosystem Components

This project has received funding from the European Union´s Horizon 2020 Research and Innovation Program under Grant agreement No. 952702.