UNINOVA

Fraunhofer IESE

National Research Council of Italy

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

gradiant

UNIVERSIDAD DE MURCIA

RESILTECH Technologies for Resilience

HOLISUN

TTTechAuto

7bulls.com

IFEVS

The research consortium is composed of 11 partners, from 7 European countries (Portugal, Italy, Romania, Austria, Spain, Poland, Germany).

Contact us:

www bieco.org

facebook.com/bieco.org

twitter.com/bieco_org

instagram.com/bieco_org/

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

BIECO

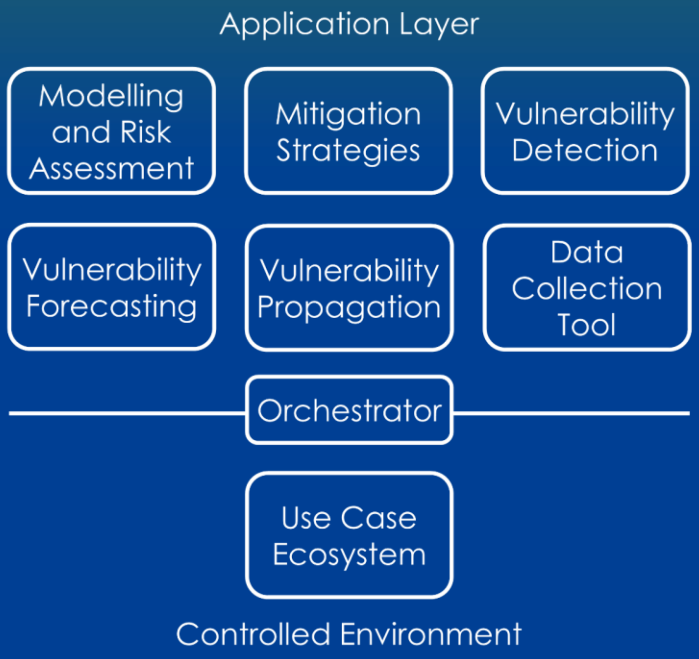
Building Trust in Ecosystems and Ecosystem Components

In the light of fast development of cyber threats, the complexity of heterogenous ICT ecosystems raise major security concerns.

BIECO aims at developing methods and tools for building trust in ecosystems and ecosystem components with particular focus on safety and security aspects at design and runtime.

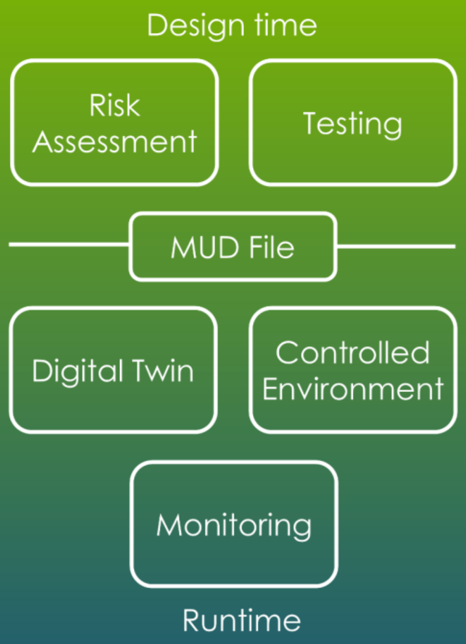
BIECO provides various mechanisms for malicious failure prediction and trust assurance, considering the design time and runtime phase of a technical ecosystem component. These mechanisms are instrumented by an online framework that connects various methods and tools.

The public and internal information about the use cases is stored in a Data Collection Tool. The public information sources are vulnerability databases, exploits databases and MUD files repositories. The main consumers of the Data Collection Tool information, are the machine learning algorithms of BIECO, trained for detection and forecasting of software vulnerabilities, failure prediction and exploits forecasting.



During design time, a use case ecosystem is modelled with a toolchain including features of threat and risk analysis, simulation and identification of mitigations. Moreover, a vulnerability assessment process (consisting of vulnerability detection, forecasting and propagation) for software components is also performed. Then, a security evaluation process combining security risk assessment and testing is executed to identify vulnerabilities and determine the security level achieved by the system. The evaluation is connected with the runtime by the creation of a MUD file, which integrates a set of security policies that the system should follow to reduce the attack surface.

During runtime phase, failure prediction is performed by the synergy of a predictive simulation environment, a runtime monitor mechanism and a controlled environment. These three components enable complex auditing and triggering of fail-over behavior for assuring functional and non- functional properties including security and safety. Specifically, the predictive simulation executes in a simulated environment (the digital twins), which are abstractions of software component's behavior instrumented with probes created according to a Domain Specific Language.



The execution of the Digital Twins provides to the Runtime Monitor the predicted trusted behavior. In turn, the Runtime Monitor continuously checks that functional and non-functional established properties remain within established boundaries and compares the parallel execution of the software in the controlled environment against the behavior signature offered by the predictive simulation. In case of deviations, a fail-over behavior is triggered in order to keep the system in a safe and trusted state.