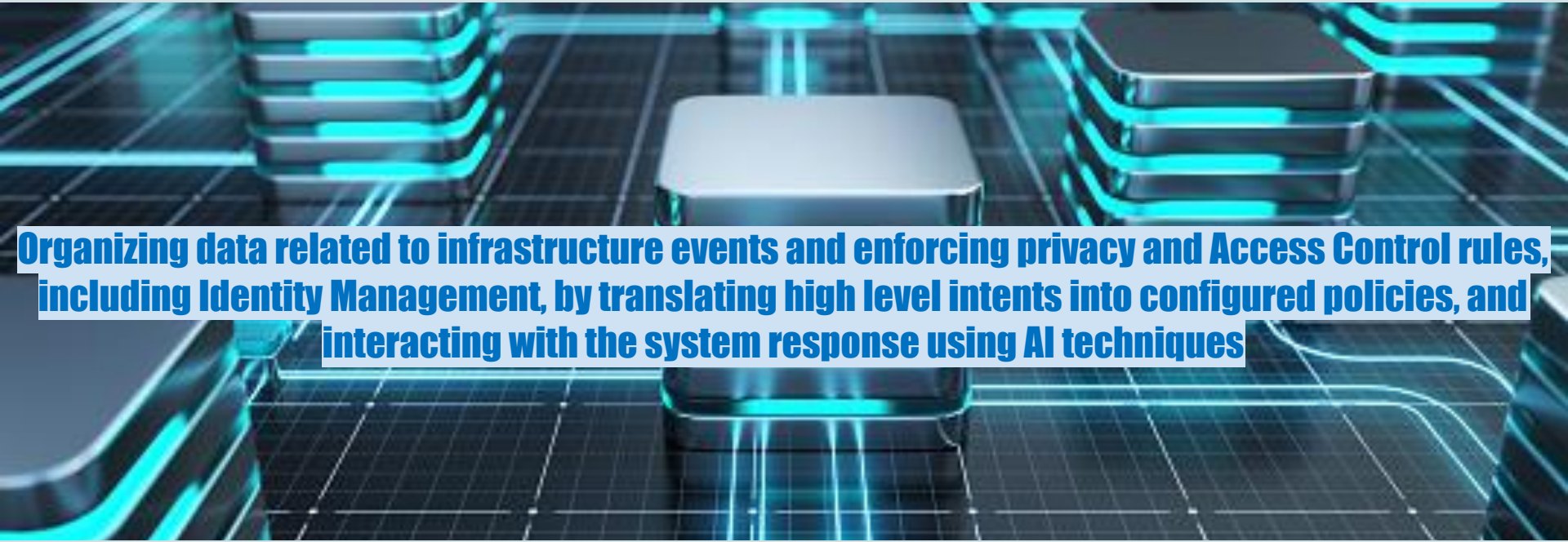
KER 5: Security & Privacy Dataspace Infrast

UNIQUE VALUE PROPOSITION



Organizing data related to infrastructure events and enforcing privacy and Access Control rules, including Identity Management, by translating high level intents into configured policies, and interacting with the system response using AI techniques

KER 5: Security & Privacy Dataspace Infras

SOLUTION BENEFITS

ACCESS CONTROL

Advanced policy and rules definition and enforcement technology

IDENTITY MANAGEMENT

Identity Management strategy, which is fundamental in a supply chain environment where different users' perspectives and demands must coexist

DATA SANITIZATION AND FLOW CONTROL

Data sanitization and flow control from low-level on-premise components, according to previously defined privacy rules.

KER 5: Security & Privacy Dataspace Infrast

INNOVATION SCOPE

INNOVATION

An enhanced framework for system events' management, including metrics from different sources and promoting co-relation with added semantics, incorporating new pre-processing mechanisms (anonymization, new metadata models…)

PROBLEM

Current information systems development frameworks promote using highly distributed components that better fit the virtualization-based infrastructure and the IoT paradigm. Interconnected components and modules will expose entry points and data (at local or global levels), enlarging the potential surface attack. Missing that goal can expose the system to a high risk of being untrustable and rejected by final users.

SOLUTION

Organizing data related to infrastructure events and enforcing privacy and Access Control rules, including Identity Management

VALUE

Secure data transfer between monitored infrastructure and FISHY platform, with data anonymization

KER 5: Security & Privacy Dataspace Infrast

EARLY ADOPTERS

FARM 2 FORK

This component applies security policies to mitigate risks, attacks or intrusions detected, applying security configurations when a non-compliance situation is detected.

SMART FACTORIES

The module is used to receive from IRO the registration of new IoT devices and keeps an updated list of registered devices

CONNECTED AUTOMOTIVE

This component applies security policies to mitigate risks, attacks or intrusions detected, applying security configurations when a non-compliance situation is detected.