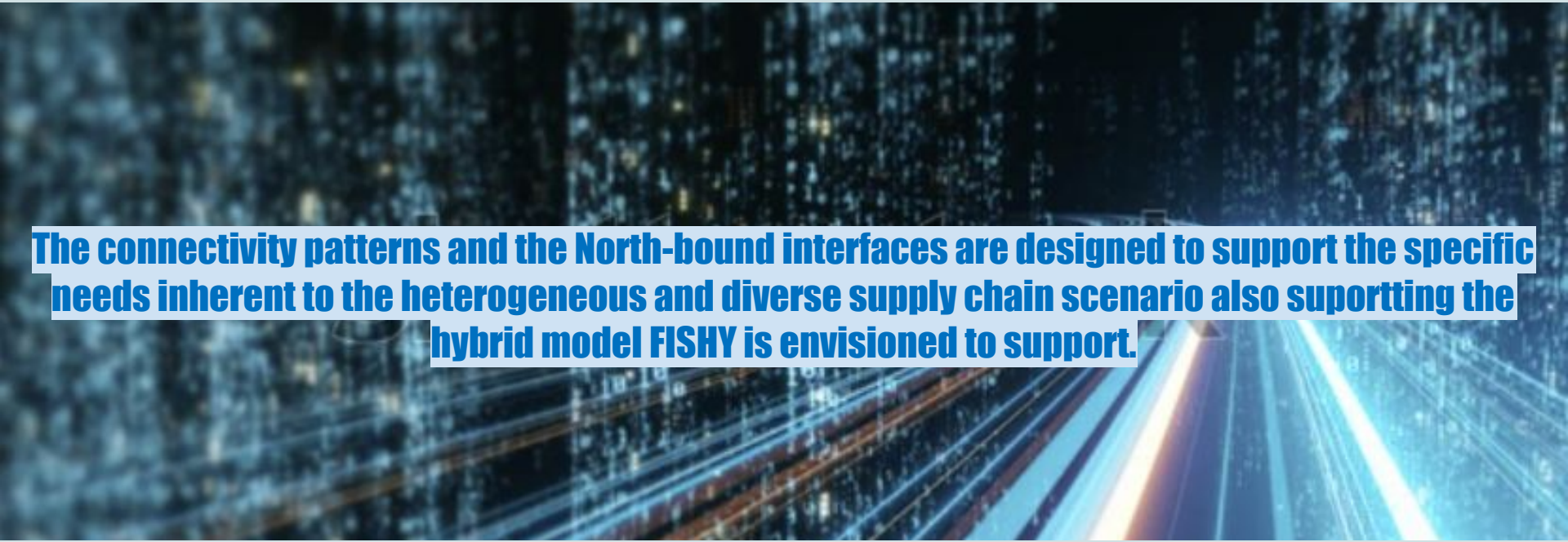
KER 7: Secure Infrastructure Abstraction

UNIQUE VALUE PROPOSITION



The connectivity patterns and the North-bound interfaces are designed to support the specific needs inherent to the heterogeneous and diverse supply chain scenario also suportting the hybrid model FISHY is envisioned to support.

KER 7: Secure Infrastructure Abstraction

SOLUTION BENEFITS

NETWORK FUNCTION ORCHESTRATION

OSM-enabled network function orchestration

VIRTUALIZATION ENVIRONMENTS SUPPORT

Able to support virtualization environments based on VMs (OpenStack) and containers (Kubernetes)

SECURE MULTI-DOMAIN CONNECTIVITY

Secure multi-domain connectivity relaying on IPsec

KER 7: Secure Infrastructure Abstraction

INNOVATION SCOPE

INNOVATION

Seamless and transparent base infrastructure management, with multi-domain connectivity and functional orchestration aware of the FISHY framework

PROBLEM

Provide a common interface for the orchestration of the network-based functions used by FISHY, in all its phases (monitoring data collection, threat detection, policy translation and enforcement), including the deployment and management of functions using standard cloud-native interfaces, and multi-domain connectivity management.

SOLUTION

Model-based support for the management of network and computer infrastructure, with seamless support of multi-domain scenarios. SIA is the base for the FISHY Reference Framework (FRF) and sandbox environment.

VALUE

Abstract interface allowing the execution of verification, detection and mitigation actions on different types of underlying infrastructure (IoT, IaaS, baremetal, etc)

KER 7: Secure Infrastructure Abstraction

EARLY ADOPTERS

FARM 2 FORK

SIA is able to be a transceiver of information from cloud-based IT platforms that support IoT and blockchain technologies.

SMART FACTORIES

This component ensures the collection of telemetry from the IoT Hub and of information logs from the WLAN controller to then send them to the TIM, EDC or SACM components.

CONNECTED AUTOMOTIVE

SIA is used as part of the securitisation of services, facial identity management and certified version management in vehicles. Communication are done in a secure way through the NED, allowing restrictions or configurations to be applied if intrusions or risks are detected in the vehicle.