7SHIELD

SEVERITY LEVEL ASSESSMENT FROM SEMANTICALLY FUSED VIDEO CONTENT ANALYSIS FOR PHYSICAL THREAT DETECTION IN GROUND SEGMENTS OF SPACE SYSTEMS

Gerasimos Antzoulatos, *Georgios Orfanidis, Panagiotis Giannakeris, Giorgos Tzanetis, Grigorios Kampilis-Stathopoulos, Nikolaos Kopalidis, Ilias Gialampoukidis, Stefanos Vrochidis, Ioannis Kompatsiaris*

CERTH CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

Centre for Research & Technology Hellas – CERTH

Information Technology Institute - ITI

iti Information Technologies Institute

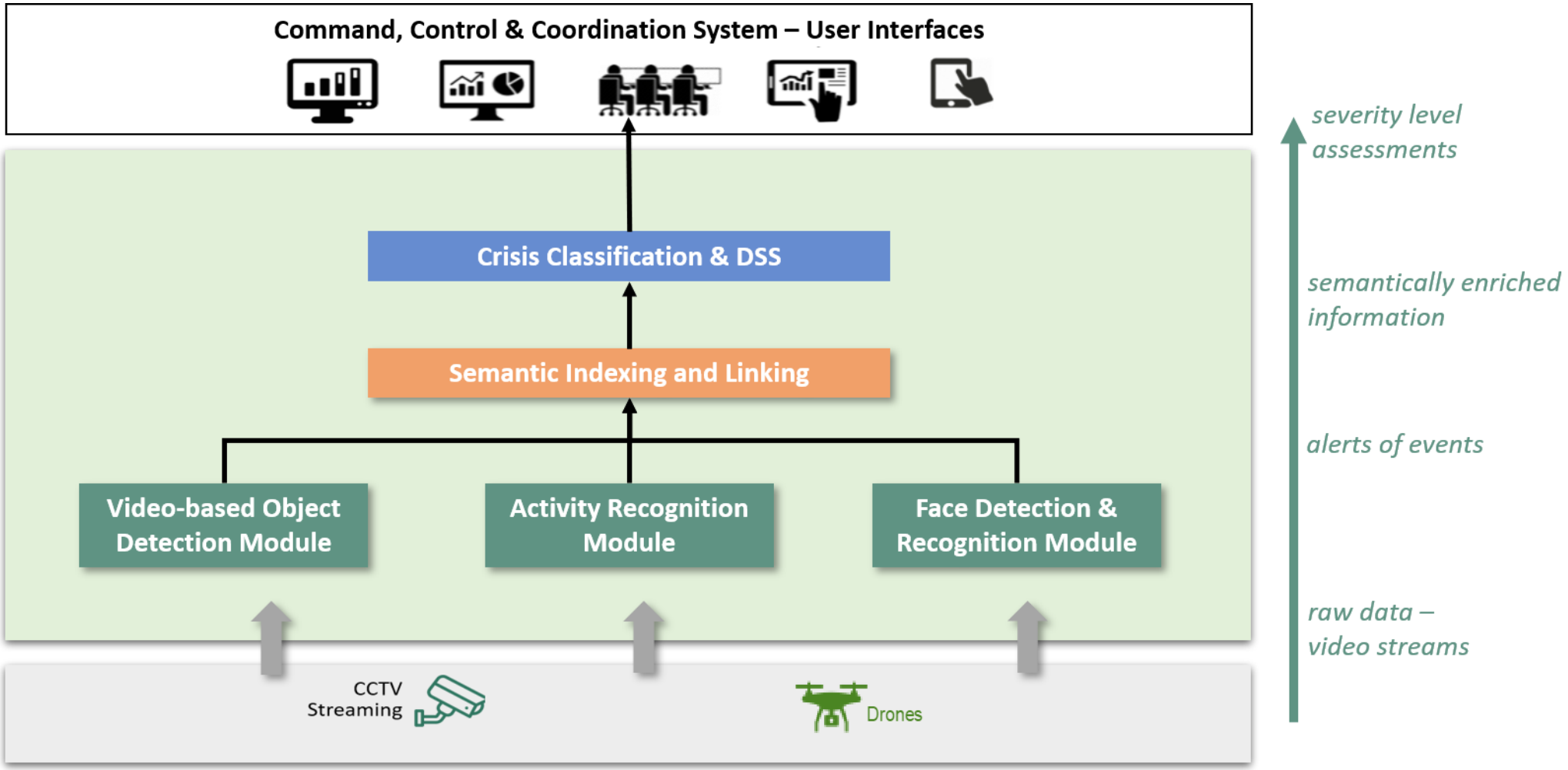
2nd CPS4CIP Workshop - 8th October 2021

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883284.

Outline

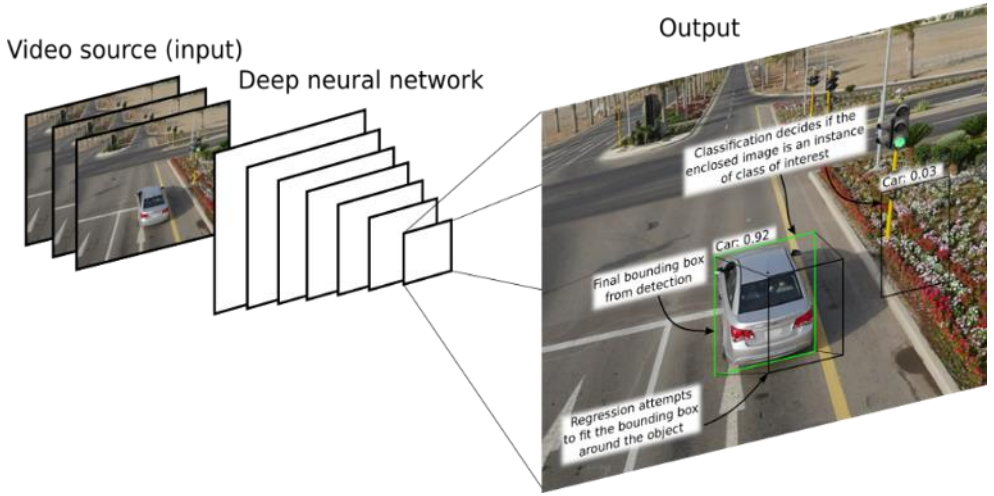
- Methodological Framework for physical attack detection and response
- *Main Components*:
  - Video-based Object Detection and Activity Recognition
  - Face Detection and Recognition
  - Semantic Indexing and Linking
  - Crisis Classification & DSS Module
- Experimental validation and evaluation
- Conclusions & Future Work

Methodological Framework



Video-based Object Detection

- **Video-based Object Detection** (**VOD**) module aims to visually locate and identify the objects of interest inside the ground segment of space systems
  - ***Input***: video streams
  - ***Analysis***: processing with deep learning techniques
  - ***Output***: group of bounding boxes around each detected object of interest accompanied by a confidence score, which reveals how certain is the network for this detection, and label to denote the class the object belongs to



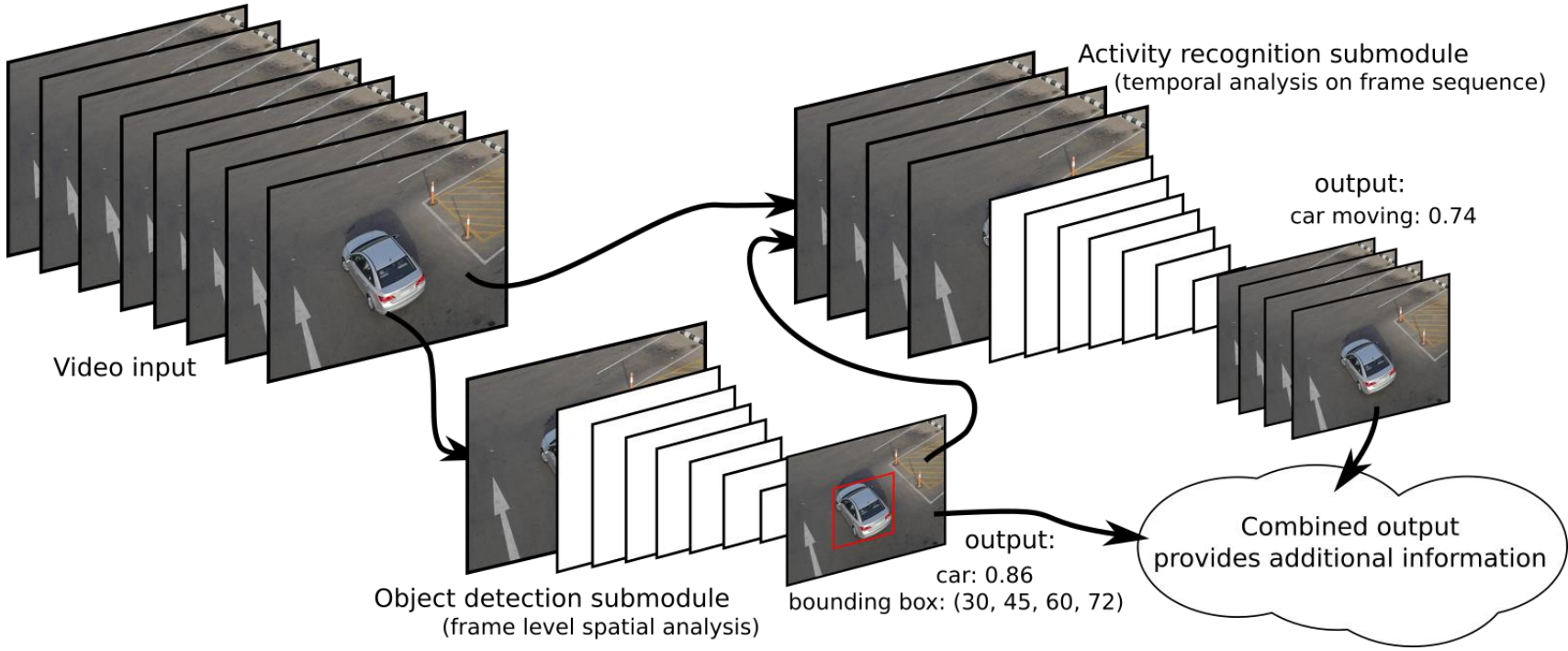
Activity Recognition

- **Activity Recognition** (**AR**) module aims to identify an activity given a specific frame span (or equivalently a time span) and to decide if it is potential harmful and suspicious

Input: AR is triggered by VOD if certain conditions are met

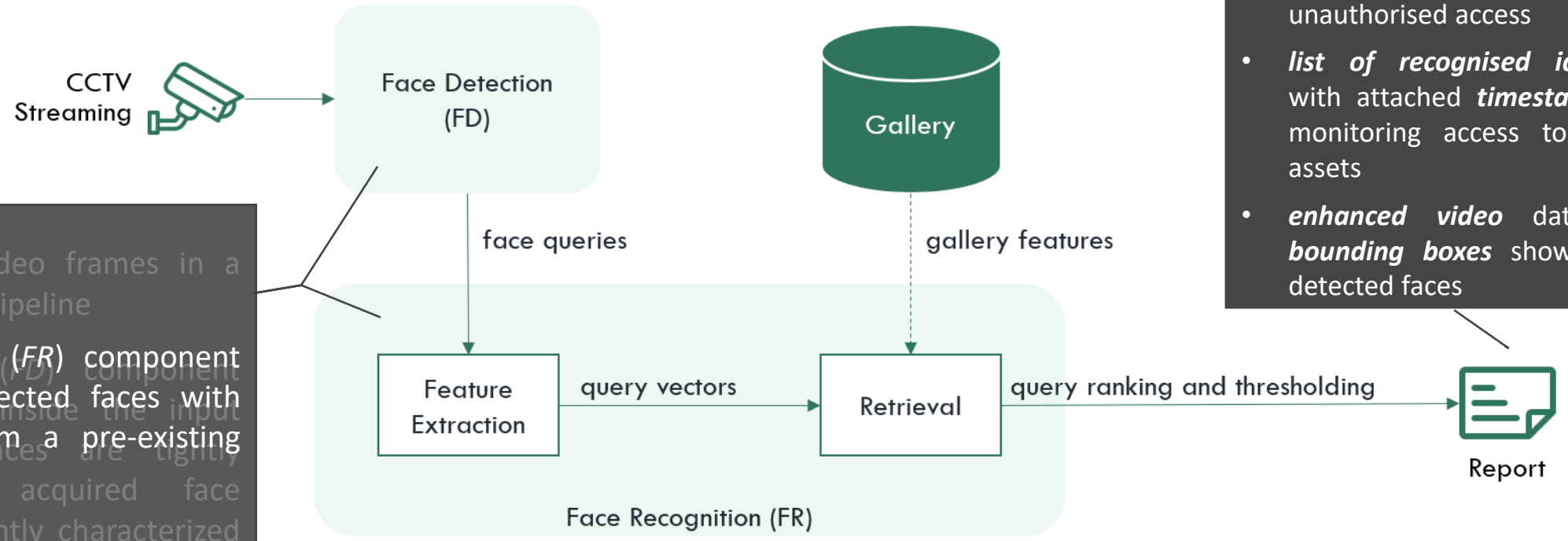
Analysis: temporal analysis of time frequency

Output: a) Awareness of surroundings via recognized activities; b) Label for each activity along with the participating objects



Face Detection and Recognition

- **Face Detection and Recognition** (**FDR**) module aims to ensure that restricted access to facilities is under secure control by detecting, recognising and notifying about unauthorized trespassers



Process single video frames in a serial processing pipeline

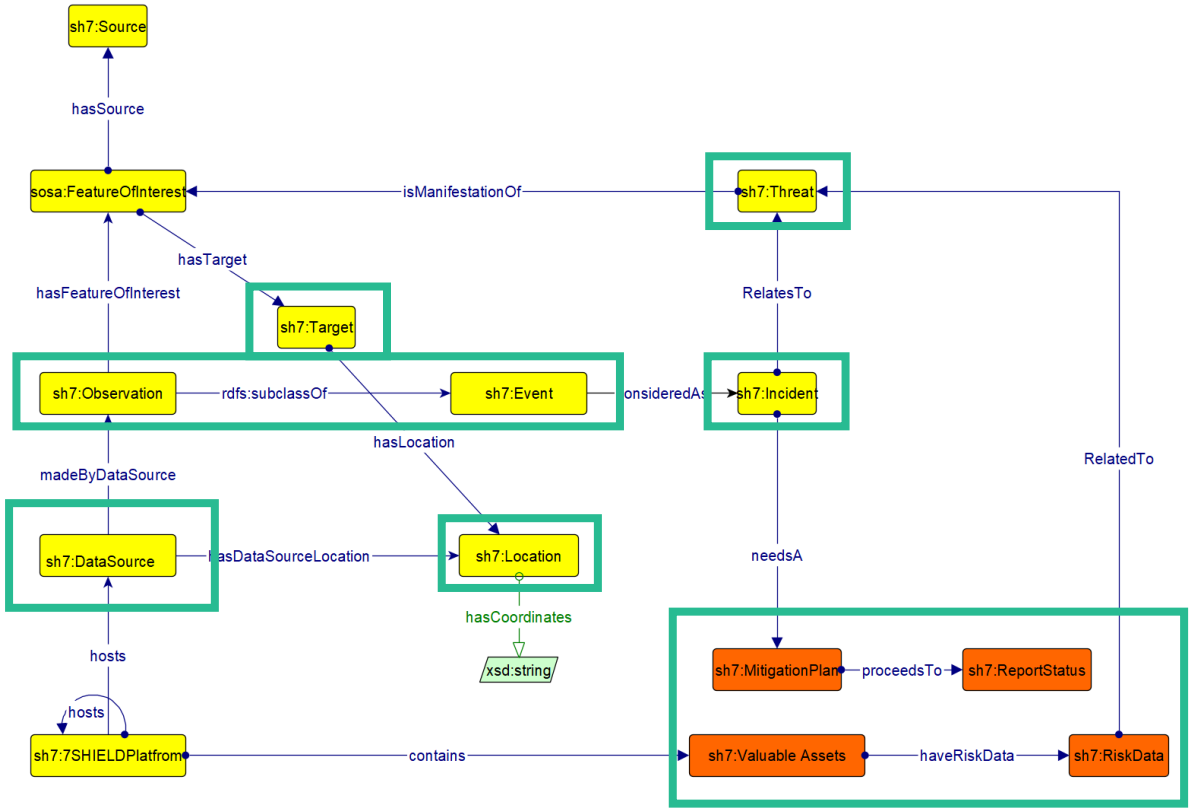
Face Recognition (*FR*) component matches the detected faces with known faces from a pre-existing gallery

Reports:

- ***alarm notifications*** of potential unauthorised access
- ***list of recognised identities*** with attached ***timestamps*** for monitoring access to critical assets
- ***enhanced video*** data with ***bounding boxes*** showing the detected faces

Semantic Indexing and Linking

- **Knowledge Base** (**KB**), is a knowledge representation model for semantically representing concepts relevant to the cyber-physical threats



Classes that interact with other components

Valuable Assets: contains information concerning the assets and their vulnerabilities

Mitigation Plan: comprises actions to mitigate/response to a malicious event (ERP)

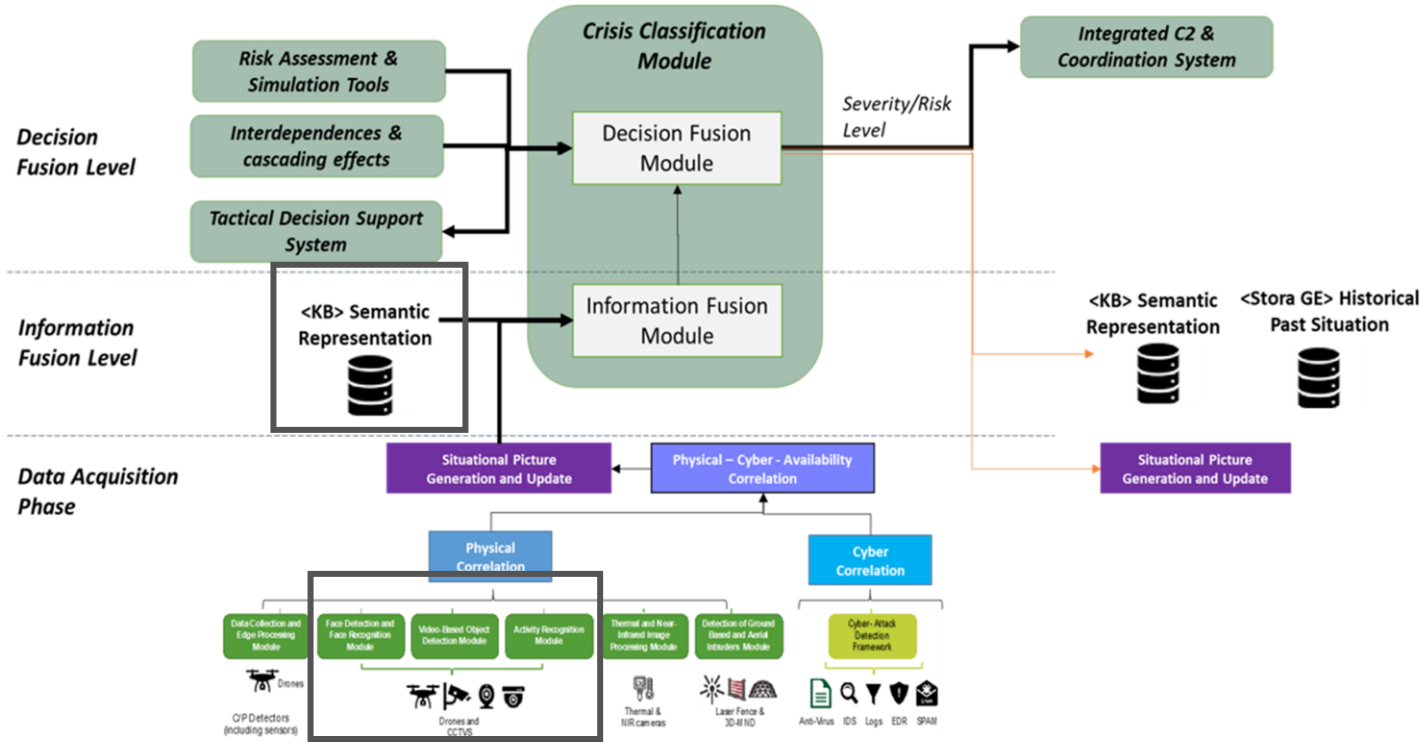
Report Status: contains details for the P/C attack

Risk Data: contains the assessments of the risk

Crisis Classification & DSS Module

- **Crisis Classification (CRCL) & DSS** module aims to assess the severity level of an ongoing physical and/or cyber-attack in critical satellite and ground segments

- ***Information Fusion level***: the real-time (or "near" real-time) information, generated by the fusion of heterogeneous data from detection modules, is analysed using machine learning techniques
- ***Decision Fusion level***: the outcomes are enriched semantically with information extracted from Knowledge Base.
- ***Output***: accurate estimation and classification of crisis events, generated by C/P attacks, in terms of their severity level



Experimental validation and evaluation (1/4)

Evaluation of ***Video-based Object Detection*** module

Faster R-CNN two-phase detector model
- ✓ *Training set*: collected dataset of over 20k samples
- ✓ 6 classes: UAV, Car, Bus, Truck (including Van), combined Motorcycle/Bicycle, Person
- ✓ *Evaluation set*: roughly 200 samples

Efficient-Det (φ=0) detector model
- ✓ *Training set*: collected dataset of over 10k samples
- ✓ 6 classes: Car, Bus, Truck, Motorcycle, Bicycle, Person
- ✓ *Evaluation set*: roughly 200 samples

	Person	Car	Bus	Truck	Moto-Bike	Bicycle	Motorcycle	UAV	mean Avg. Precision
Faster RCNN	**0.82152**	**0.75726**	**0.57315**	**0.53351**	0.73409	-	-	0.75330	**0.6954**
Efficient-Det (ϕ=0)	0.4563	0.4668	0.5562	0.3790	-	0.3438	0.3968	-	0.4332

Experimental validation and evaluation (2/4)

Evaluation of ***Face Detection and Recognition*** module

Face Detection:
- ✓ Methods: (i) TinyFaces, (ii) PyramidBox, (iii) DSFD
- ✓ WIDER FACE benchmark dataset for evaluation
  - 30,000 images based on 61 event classes
  - The human faces appear with a high degree of variability in scale, pose and occlusion

Face Recognition:
- ✓ Methods: (i) Facenet, (ii) PFE, (iii) Arcface
- ✓ LFW benchmark dataset for evaluation
  - 13,000 images of faces collected from the web
  - known public figures like politicians, athletes, actors, musicians and other various celebrities

Method	WIDER FACE AP (%)
TinyFaces (2017)	90.7
PyramidBox (2018)	94.3
DSFD (2019)	**95.5**

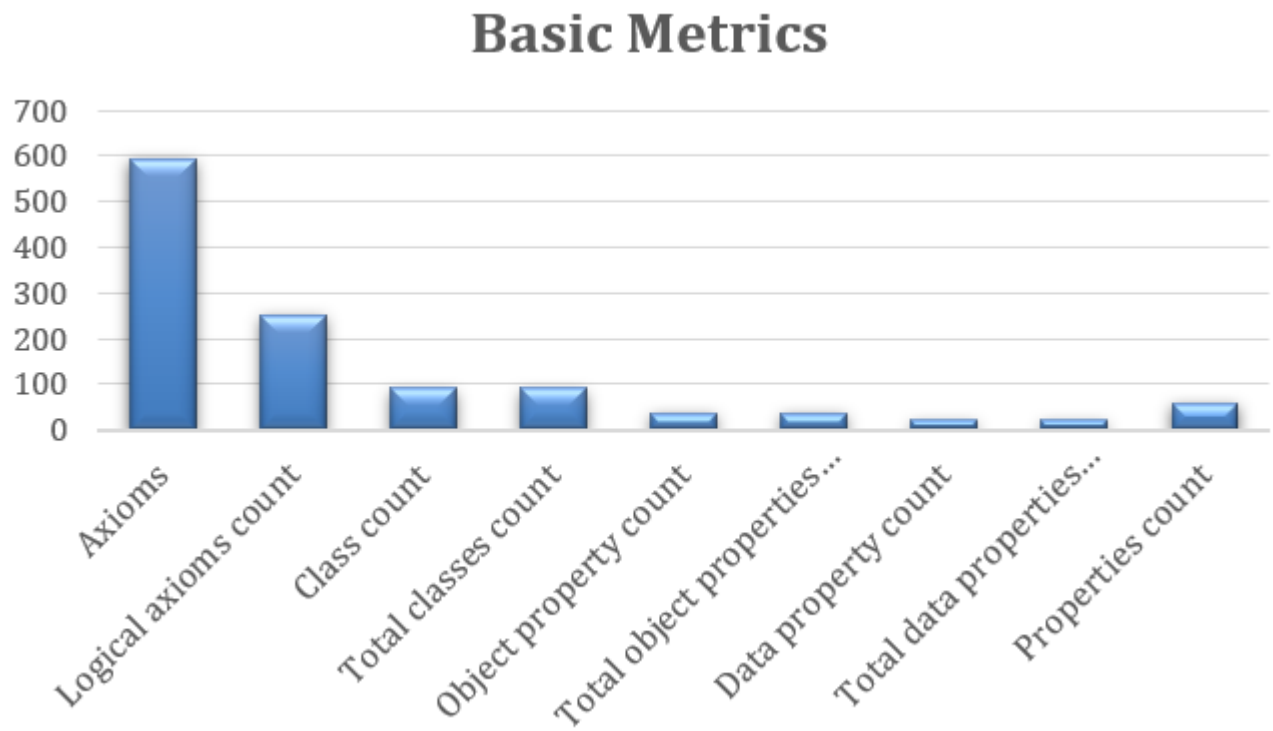
Method	LFW AP (%)
Facenet (2015)	99.4
PFE (2019)	99.6
Arcface (2019)	**99.7**

Experimental validation and evaluation (3/4)

Validation of the ***Fusion layer***

Knowledge Base:

- ✓ *OntoMetrics* tool, an online framework that evaluates the ontology based on predefined metrics WIDER FACE benchmark dataset for evaluation



Experimental validation and evaluation (4/4)

Annotation Tool:

- ✓ the utilisation of Machine Learning techniques needs annotated datasets, namely, datasets that assess the severity level of an attack relied on its characteristics
- ✓ ***Annotation Tool*** *to generate scenarios of P/C attacks in specific locations/assets in pilot sites*
- ✓ ***End-users involvement****: request experts to characterize those scenarios in terms of likelihood of the attack and potential consequence of it*

Severity		Potential Consequences				
		Not Significant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain	Moderate	High	Extreme	Extreme	Extreme
	Likely	Moderate	High	High	Extreme	Extreme
	Possible	Low	Moderate	High	High	Extreme
	Unlikely	Low	Moderate	Moderate	High	High
	Rare	Low	Low	Low	Moderate	Moderate

Conclusions & Future work

- Unified framework for the detection, semantic indexing and severity level estimation during physical attack scenarios in ground segments of space systems
  - ✓ Robust detection algorithms with promising experimental results in terms of their precision
  - ✓ Sufficient semantic indexing and Knowledge Base establishment
  - ✓ Web-based app to capture the knowledge and experience of experts in a simple, fast and user-friendly way (Annotation tool)
- *Future Work*:
  - ✓ Enhance the detection algorithms by training them to identify more classes (e.g. backpack) and recognise more activities
  - ✓ Analyse video from UAVs – embedded AI algorithms for computing at the edge
  - ✓ Enrich Knowledge Base with classes for emergency response plans and create reports
  - ✓ Assess the severity level of an attack by training machine learning algorithms based on the annotated datasets
  - ✓ Evaluate the whole framework for its performance and efficiency to confront P/C attacks

- Gerasimos Antzoulatos (gantzoulatos@iti.gr)
- Georgios Orfanidis (g.orfanidis@iti.gr)
- Panagiotis Giannakeris (giannakeris@iti.gr)
- Giorgos Tzanetis (tzangeor@iti.gr)
- Grigorios Kampilis-Stathopoulos (grigstat@iti.gr)
- Nikolaos Kopalidis (nikokopa@iti.gr)
- Ilias Gialampoukidis (heliasgj@iti.gr)
- Stefanos Vrochidis (stefanos@iti.gr)
- Ioannis Kompatsiaris (ikomg@iti.gr)

7SHIELD

https://www.7shield.eu/

Thank You