Final Workshop

Towards Smart Autonomous Cyber-Physical Systems: Unmanned Aerial/Ground Vehicles and Robots

CPSwarm Overview

Vision scenarios and the CPSwarm Workbench

Farshid Tavakolizadeh, Fraunhofer FIT
Ákos Milánkovich, Search Lab

Turin, December 13th 2019

CPSwarm Vision Scenarios

Swarm drones, Logistic rovers, Automotive CPS

Ideation of scenarios and use case analysis

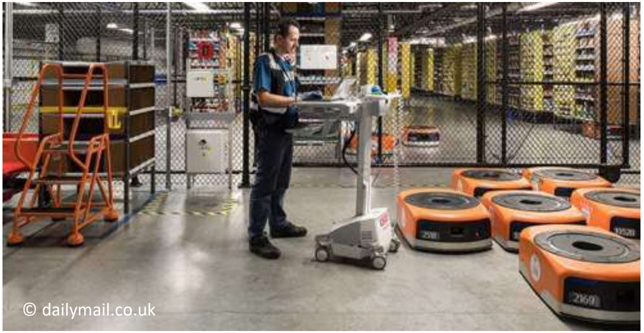
Workshops and **brainstorming** sessions were held to derive the main **scenarios** and provide input to the **use case analysis**

Application Scenarios

Three reference Application Scenarios drive the collection of requirements for the development of the **complete CPSwarm toolchain** *supporting the engineering and deployment of CPS swarms*

Phantom_Glacier: Image courtesy DJI

Swarm Drones


© dailymail.co.uk

Swarm Logistics Assistant

© Drew Kelly for WIRED

Automotive CPS

Swarm Drones

Heterogeneous swarms of ground robots/ rovers and UAVs to conduct certain missions in

- **Surveillance of critical infrastructures** like, e.g., industrial or power plants
  - intrusion detection (detection of unauthorized persons entering the plant area)
  - monitoring of actions of unauthorized persons in the plant areas
- **Search and Rescue** tasks
  - generating a situation overview of the disaster scene in case of an industrial plant accident including real-time images (VIS, IR), toxic and explosive gas leakage detection
  - finding of human casualties or persons trapped in the disaster area.

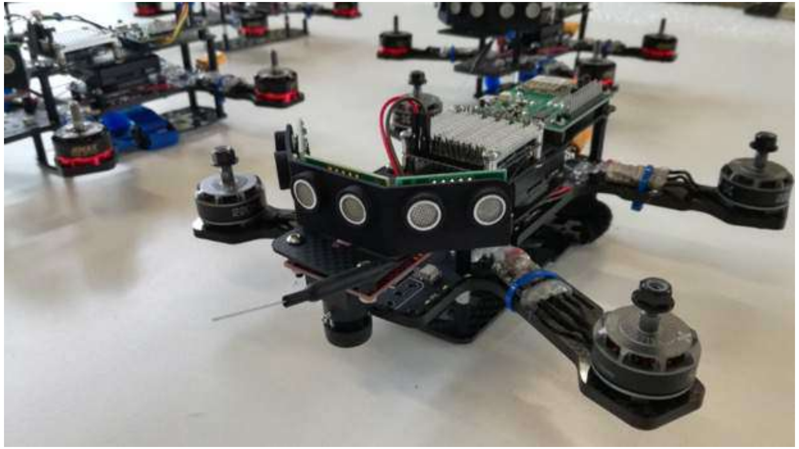
Phantom_Glacier: Image courtesy DJI

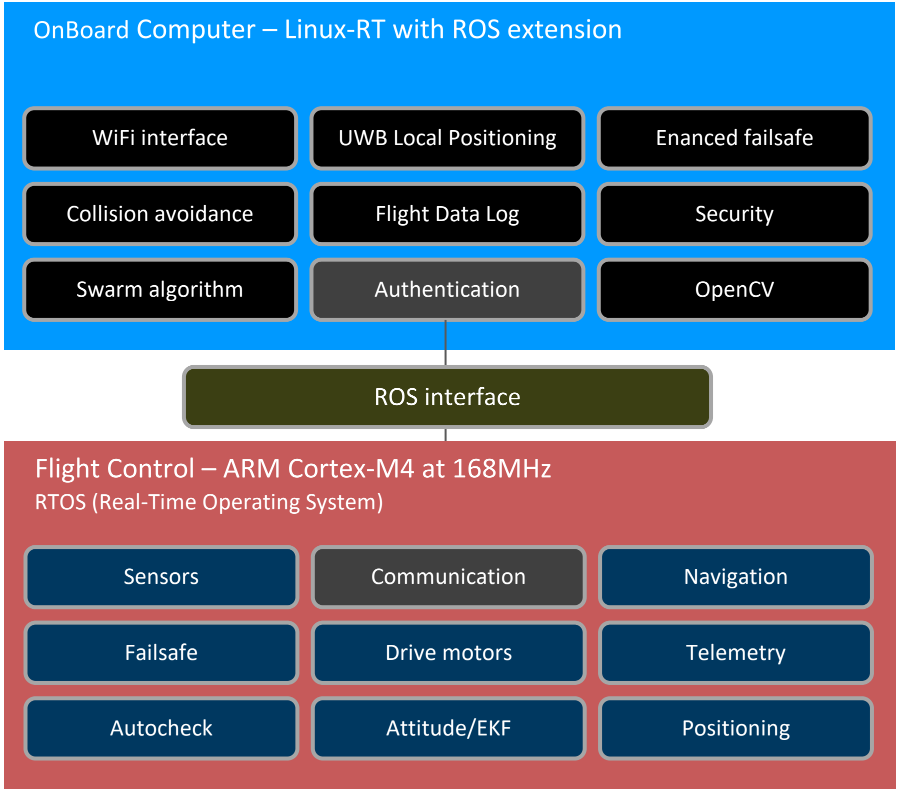
RoboCup @ Space Demo

© MAXSUR

Swarm Drones – Selected technologies

- Single board, companion computer (NanoPi)
- 3 Ultrasonic rangefinders
- Ultra-wideband local positioning (DecaWave DWM1001)
- RGB Camera
- Robotic Operating System (ROS)





OnBoard Computer – Linux-RT with ROS extension

WiFi interface

UWB Local Positioning

Enanced failsafe

Collision avoidance

Flight Data Log

Security

Swarm algorithm

Authentication

OpenCV

ROS interface

Flight Control – ARM Cortex-M4 at 168MHz

RTOS (Real-Time Operating System)

Sensors

Communication

Navigation

Failsafe

Drive motors

Telemetry

Autocheck

Attitude/EKF

Positioning

Swarm Logistics Assistant

Focus on robots and rovers designed to **assist humans in logistics domain**

- Scan the entire area of the warehouse and share the acquired information
- Collect information about the maps of the entire area
- Collect additional information implicitly e.g. room temperature, presence of humans, detection of in-path obstacles etc.
- Join forces to move a heavy obstacle from one place to another

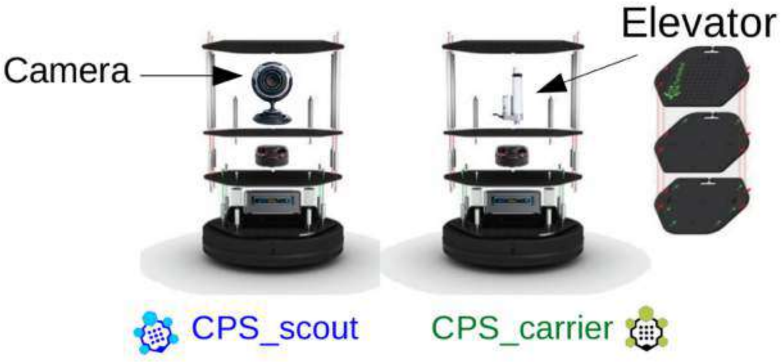
© Drew Kelly for WIRED

© OTTO

© Fraunhofer IML

Swarm Logistics Assistant – Selected technologies

- Embedded on-board computer (Intel NUC)
- Laser rangefinder (Hokuyo UST-10LX)
- RGB Camera
- Stereo Camera (Rubedos VIPER + NVIDIA Jetson TX2)
- Robotic Operating System (ROS)



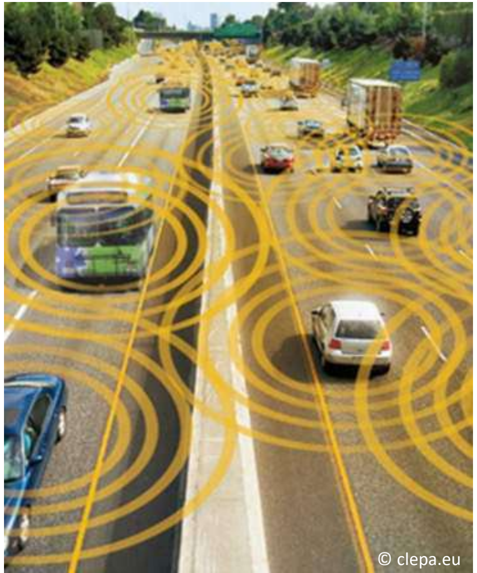
Turtlebot

Automotive CPS

- Applications for **collective driving** with a focus on **autonomous driving vehicles intended for freight transportation**
  - independent vehicles could join or leave a swarm at any point during the journey

- Laboratory level demonstrator (TRL 3 to TRL 4, demonstration in breadboard lab environment)
  - E.g., trucks, vans or cars and connecting them via kind of an electronic drawbar.

© dailymail.co.uk



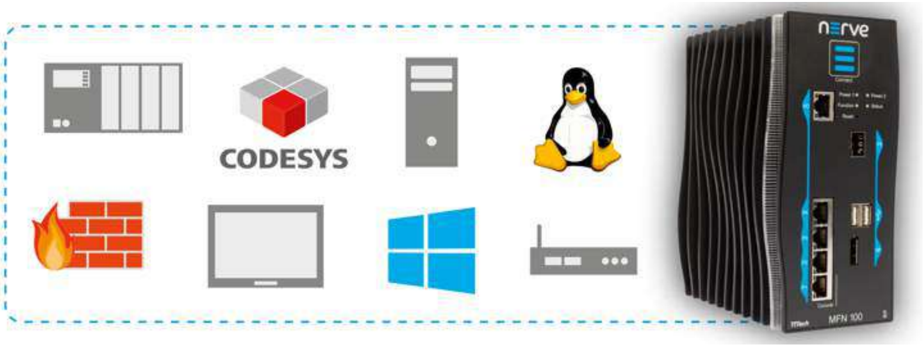
© clepa.eu

© Daimler

Automotive CPS – Relevant technologies

- Automotive on-board computer (TTTech Fog Node)
- Deterministic, time-triggered Ethernet (TTEthernet)
- AUTomotive Open System Architecture (AUTOSAR)

Automotive
Fog node



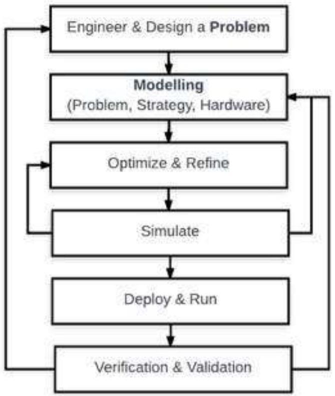
Deterministic
Ethernet Switch

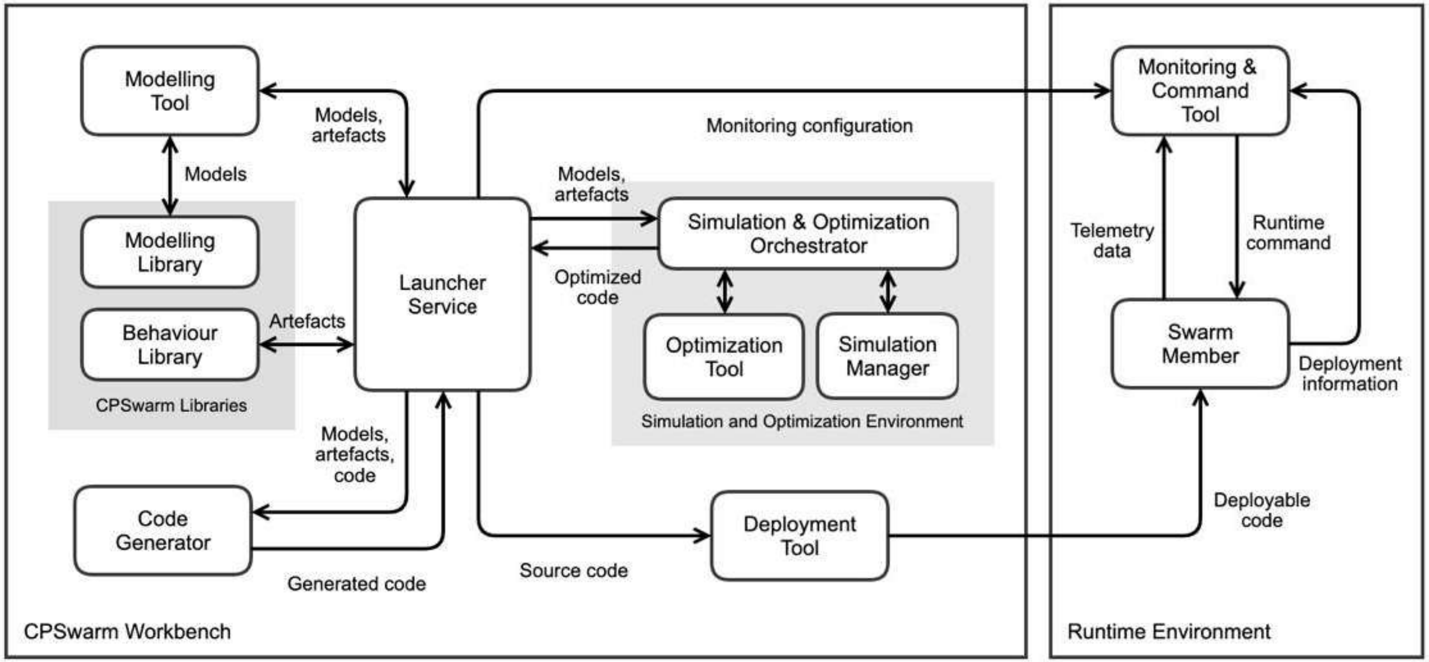
CPSwarm Workbench

The CPSwarm Prototype

github.com/cpswarm

CPSwarm Architecture

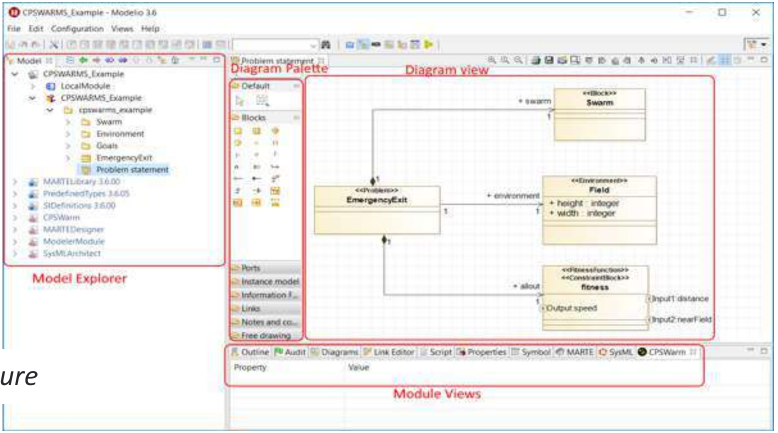

Engineer & Design a **Problem**
Modelling
(Problem, Strategy, Hardware)
Optimize & Refine
Simulate
Deploy & Run
Verification & Validation



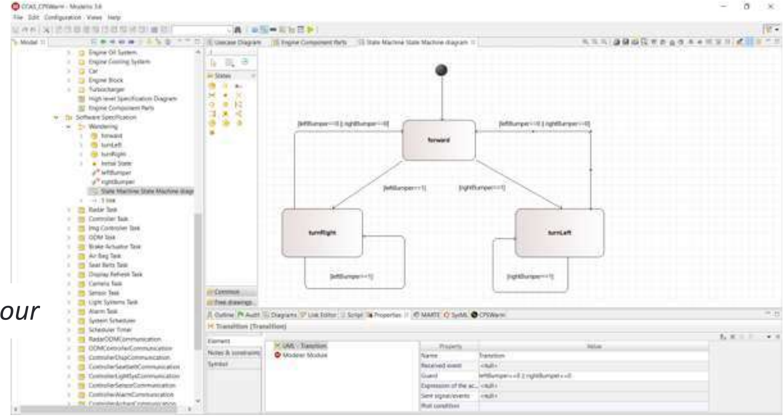
Modelling Tool

- Built on top of **Modelio**
  - Modeling of swarm behavior, swarm composition, swarm goal
- Uses SysML and MARTE modelling languages
- Generates SCXML outputs
- Provides a **Modelling Library** of reusable components:
  - CPS hardware specifications
  - Environments
  - Cost functions
- The modelling library is an archive of SysML 1.2 models serialized using XMI 2.1 standard

modelio
the open source modeling environment


CPSWARMS_Example - Modelio 3.6
File Edit Configuration Views Help
Diagram Palette
Diagram view
Model Explorer
Module Views
Swarm
EmergencyExit
Field
+ height : integer
+ width : integer
fitness
Outline Audit Diagrams Link Editor Script Properties Symbol MARTE SysML CPSWarm
Property
Value

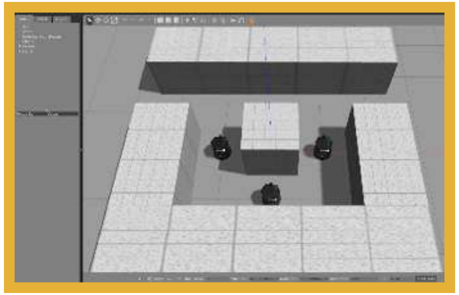
Structure

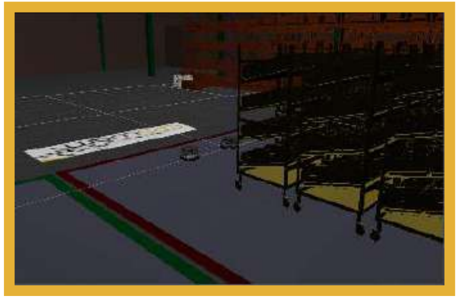


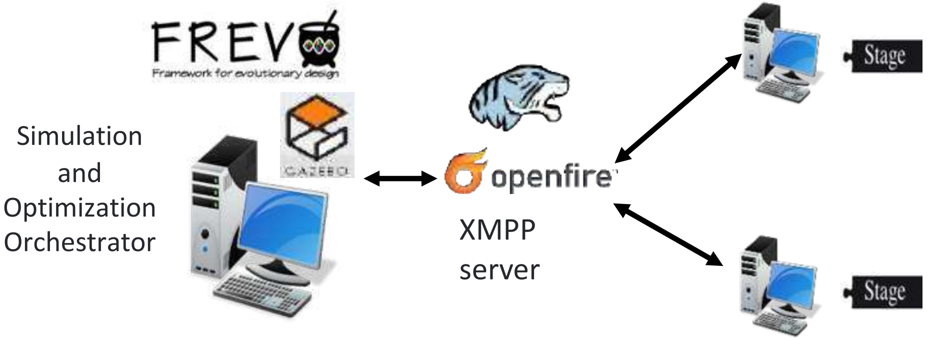
Behaviour

Simulation & Optimization

- **Simulation & Optimization Orchestrator** works as stand-alone or in combination with the Optimization Tool (i.e. **FREVO**) to iteratively evolve the controller algorithm/module.
- **FREVO** uses evolutionary methods to automatically optimize the algorithm of individual swarm members that collectively contribute to a target swarm emergent behavior.
- Support for Stage and Gazebo simulators using first-party **Simulation Managers**
- Scalable architecture, using Docker, Kubernetes, XMPP for distributed simulations
- Integrated with ThingsBoard and ROS







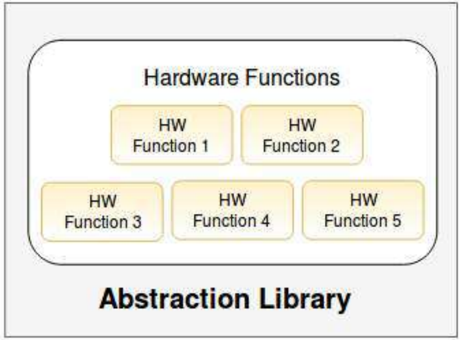
Simulation and Optimization Orchestrator

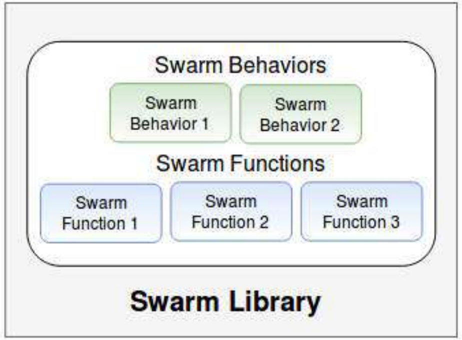
XMPP server

Behavior Library

Libraries that enable device homogeneity

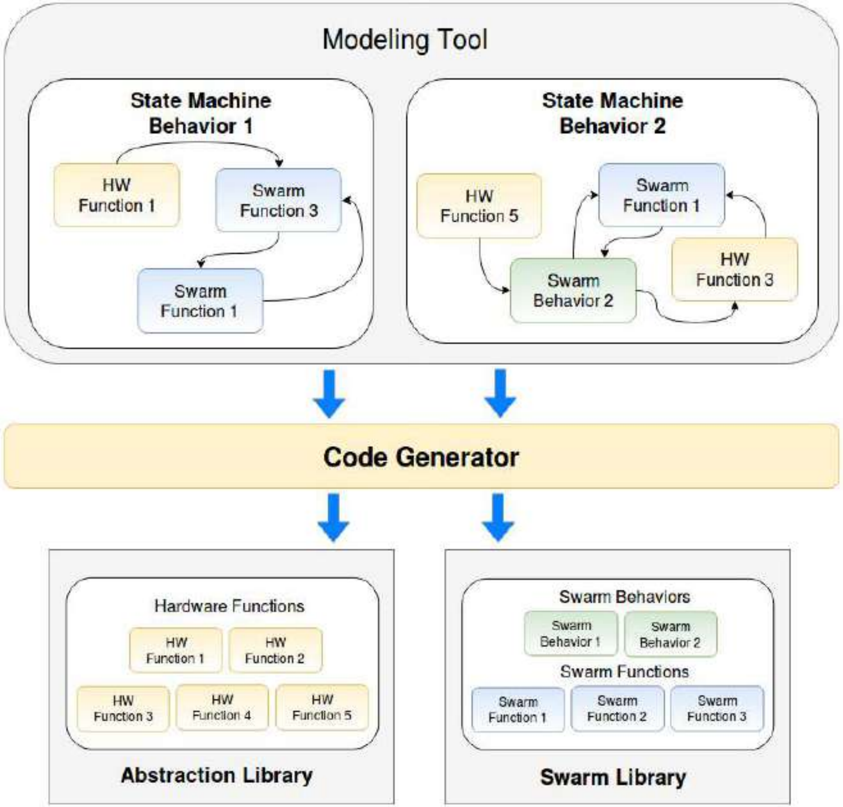
- **Abstraction Library**
  - Communication functionalities: **Swarmio**
  - Abstraction of heterogenous hardware and native functionalities
- **Swarm Library**
  - Generic behavior algorithms
  - Generic utility functions





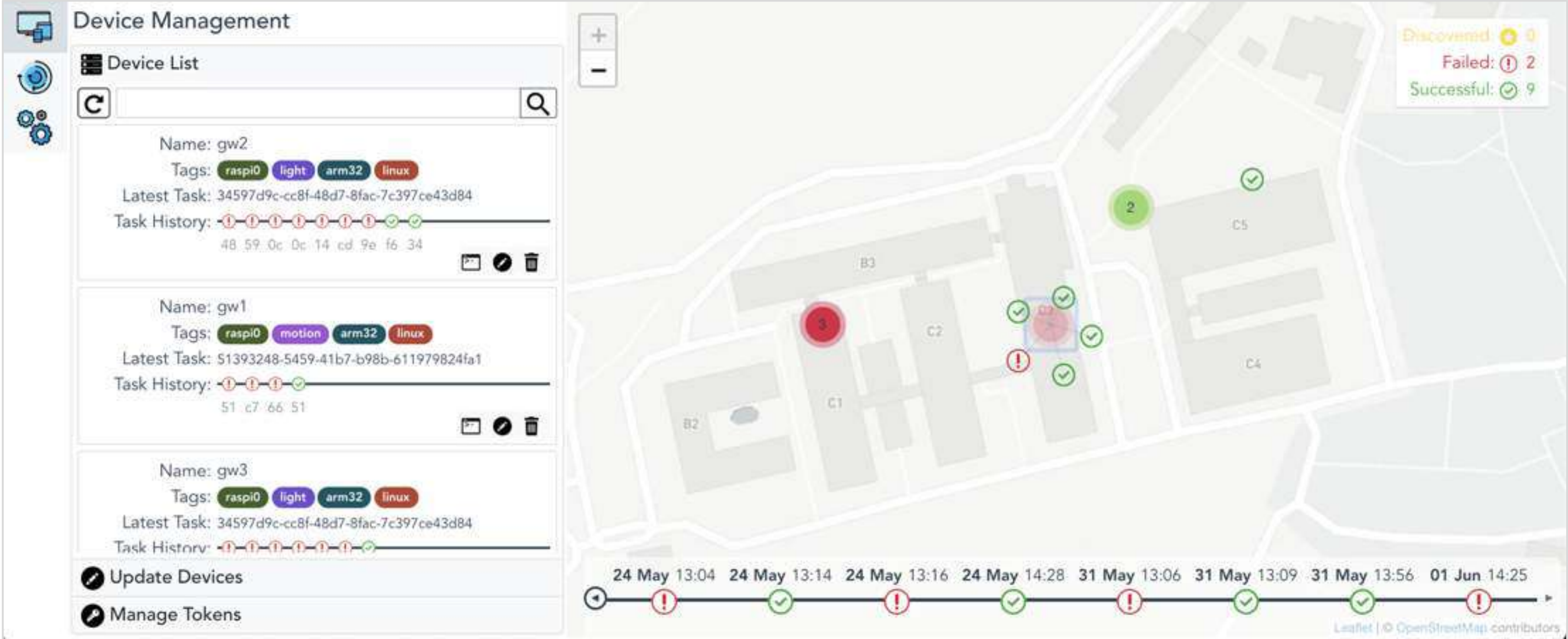
Code Generator

- The Code Generator perform two tasks:
  - ○ Interpret CPS models using specific formalisms.
  - ○ Generate CPS modules and libraries that can be installed on the actual CPSs.
- Supports the generation of Python code starting from the formal description of a Finite State Machine.
- Driven by Velocity, a Java-based template engine



Deployment Tool

- Remote software deployment and lifecycle management (build, deployment, execution)
- Communication using ZeroMQ, secured by CurveMQ
- Secure registration
- Tailored for resource-constrained environments



Device Management

Device List

Name: gw2
Tags: raspi0 light arm32 linux
Latest Task: 34597d9c-cc8f-48d7-8fac-7c397ce43d84
Task History: 48 59 0c 0c 14 cd 9e f6 34

Name: gw1
Tags: raspi0 motion arm32 linux
Latest Task: 51393248-5459-41b7-b98b-611979824fa1
Task History: 51 c7 66 51

Name: gw3
Tags: raspi0 light arm32 linux
Latest Task: 34597d9c-cc8f-48d7-8fac-7c397ce43d84
Task History:

Update Devices

Manage Tokens

Discovered: 0
Failed: 2
Successful: 9

CPSwarm Security

,”There is no safety without security”

Security and safety perspective on CPSwarm

Aimed at making security an overarching feature, from modeling to the runtime environment during the project lifecycle:

Secure behaviour	Security requirements and Attack-tree models
Secure deployment	Certificate Manager
Secure communication	Secure Communication Library

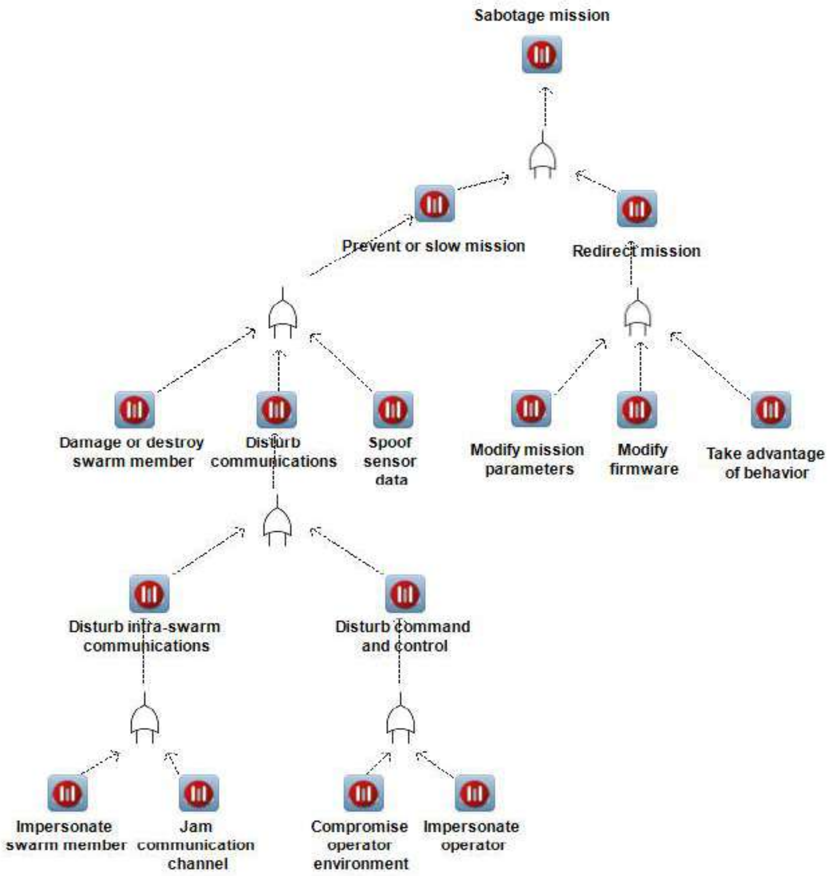
Security requirements

- Applicable norms
  - Information security management systems -- Requirements: ISO/IEC 27001
  - Common Criteria for Information Technology Security Evaluation: ISO/IEC 15408

- CPSwarm‘s security requirements:
  - The Modelling Tool shall make it possible to define events; distinguish between swarm, member and component scope events; trigger events based on the current value of the inputs and outputs; add additional swarm scope events to each state transition; and to configure all communications and its parameters.
  - The Abstraction Layer shall have low level support for remote shutdown requests that works regardless the status of the current behavior.
  - The Optimization Tool shall only optimize one behavior at a time, but shall let the simulation used include other behaviors .
  - The Deployment Manager shall sign all packages with an operator specific key.
  - The Monitoring and Configuration Tool shall be able to trigger remote events on individual swarm members and enable the user to launch an external tool to take remote control of a specific swarm member.
  - All communications between the swarm and the tools in the workbench shall be authenticated, authorized, encrypted and their integrity protected.

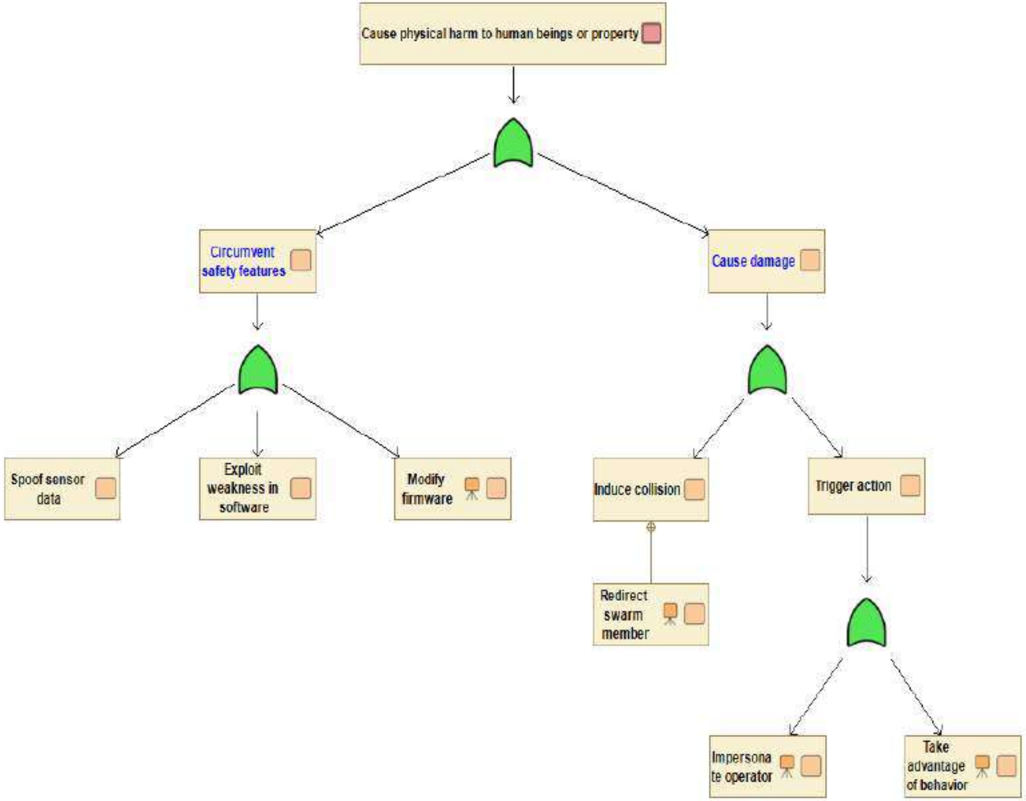
Attack-tree models and MODELIO plugin

- Visualization for attack-trees
- Helps security experts to create attack trees
- Facilitates security-consciousness
- Example attack trees for CPSwarm included


Sabotage mission
Prevent or slow mission
Redirect mission
Damage or destroy swarm member
Disturb communications
Spoof sensor data
Modify mission parameters
Modify firmware
Take advantage of behavior
Disturb intra-swarm communications
Disturb command and control
Impersonate swarm member
Jam communication channel
Compromise operator environment
Impersonate operator

Safety related Attack-trees

- Attack-trees analyse
  - Attackers' goals
  - Methods of attacks
  - Countermeasures and mitigations
  - Risk assessment
- CPSwarm safety considerations
  - are based on policies related to flying conventional drones, autonomous vehicles and the integration of robots in the workplace.
  - The attacks are labelled as safety-related with blue font color.
  - The attacks marked with a red rectangle denote root attacker goals.
  - Lower level attacks are marked with a yellow rectangle inside.


Cause physical harm to human beings or property
Circumvent safety features
Cause damage
Spoof sensor data
Exploit weakness in software
Modify firmware
Induce collision
Trigger action
Redirect swarm member
Impersonate operator
Take advantage of behavior

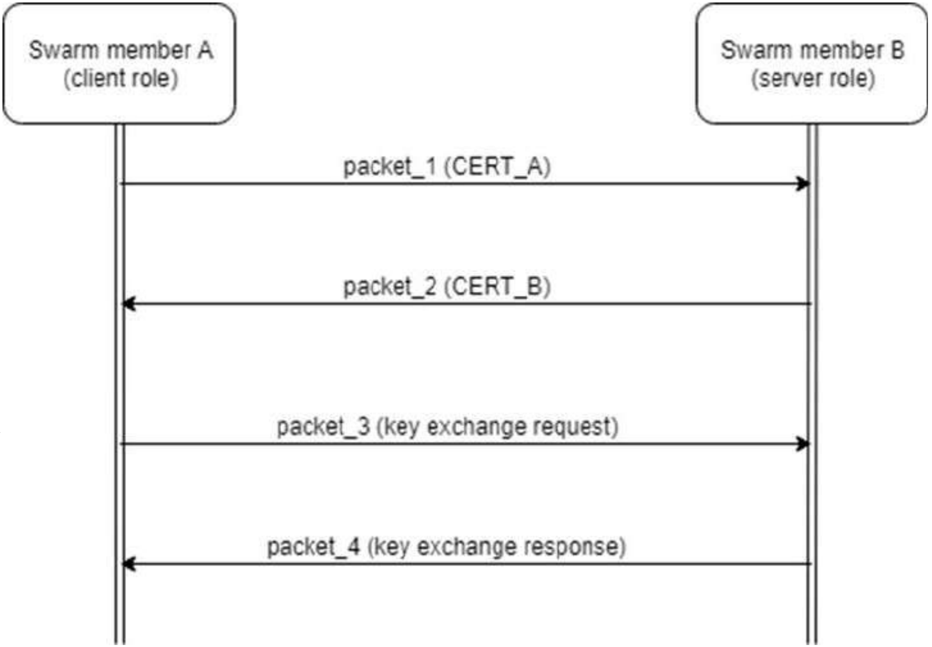
Certificate Manager

- As part of the Deployment Manager the Certificate Manager ensures secure registration by
  - providing utility functions related to certificate generation and key management to be used by other components for authentication and encryption
  - supporting the Registry for validation of keys during device registration and
  - loading existing keys from Storage and inserts them into the Transport Server for authentication requests from clients as well as for data encryption and decryption.

Access control	provided for provisioned nodes by certificate checking, using a pre-shared signing key
Authentication	provided by signature checking
Non-repudiation	provided by signature and timestamp checking for each packet
Confidentiality	provided end-to-end by payload encryption
Integrity checking	provided by using a tag for packet integrity
Availability	maintained by using each nodes security table, which stores valid authentication credentials

Secure Communication

- Deployment of a swarm member
- On deployment, the Deployment tool generates the unique communication key pair and a member certificate. The device should store its SK_pub certificate and its communication key pair, and the multicast key
- Unicast key exchange/update


Swarm member A (client role)
Swarm member B (server role)
packet_1 (CERT_A)
packet_2 (CERT_B)
packet_3 (key exchange request)
packet_4 (key exchange response)

Use cases specific risks

Search and rescue – high risk

Security compromise can result in severe harm or even death of humans, sabotage of mission or theft of sensitive data.

Logistics warehouse – low risk

It is located in a physically protected space, therefore security compromise can result in theft of items, system downtime (non-availability) or miss-delivery of items.

Lead vehicle linked to the platoon via wireless communications

Automotive – very high risk

The system is operating in public roads, therefore security compromise can create safety critical system failure (accident or crash), theft of vehicle and transported goods, or delay of delivery

THANKS!
ANY QUESTIONS?

CPSwarm

http://www.cpswarm.eu

Follow @CPSwarm_EU

Coordinator

LINKS

Partners

Fraunhofer FIT

Lakeside Labs

TTTech

Alpen-Adria Universität

Robotnik

SOFTEAM Cadextan

DigiSky

SEARCH-LAB

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731946.