



SINAPSE Project

WP4: Cybersecurity

SESAR Research project - CNS for ATM (“Intelligent CNS Network”), ATM Excellent Science & Outreach phase

SINAPSE Cyber Security 15th Sept. 2021



Founding Members



The Team



Agenda

SINAPSE Project Overview/Objectives

SINAPSE Cybersecurity Architecture

ML algorithms for Cybersecurity

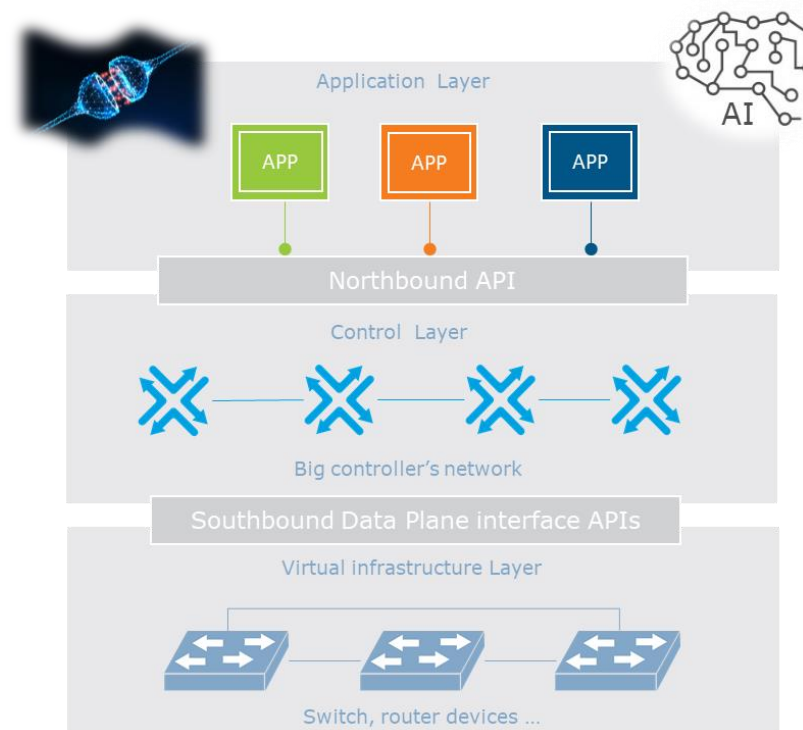
- SINAPSE AI/ML review and findings for cyber security
 - Review of ML algorithms
 - Preliminary selection of ML algorithms - selection criteria: intrusion detection
- SINAPSE approach for ML training and algorithm selection
 - Dataset pre-processing
 - ML training
 - ML selection using MCDM
 - ML algorithm validation/testing

Conclusion & Future Work

Project objectives

Intelligent & secured Aeronautical Datalink Communications network based on Software Defined Networking (**SDN**) augmented with Artificial Intelligence (**AI**)

- Predict and prevent safety services outages (e.g. ATN CPDLC)
- Optimize networking (e.g., QoS prediction and path selection)
- Intelligent Cybersecurity functions



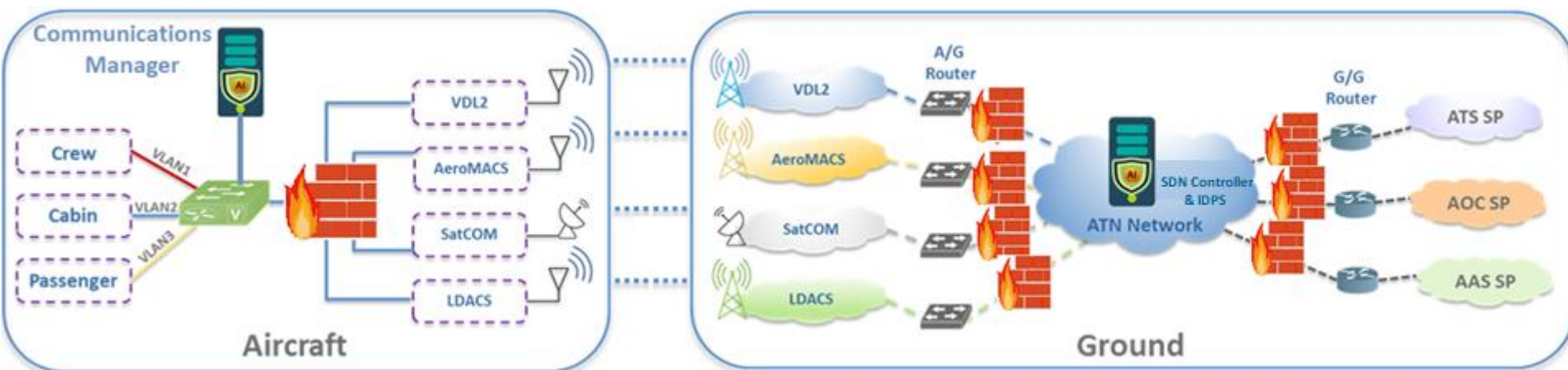
Security Architecture

Aircraft segment:

- Logical segregation of safety-critical and non-safety critical traffic domains
- Onboard router with AI-powered security gateway

Ground Segment:

- SDN controller for network management & Control
- IDPS powered by AI to secure SDN controller

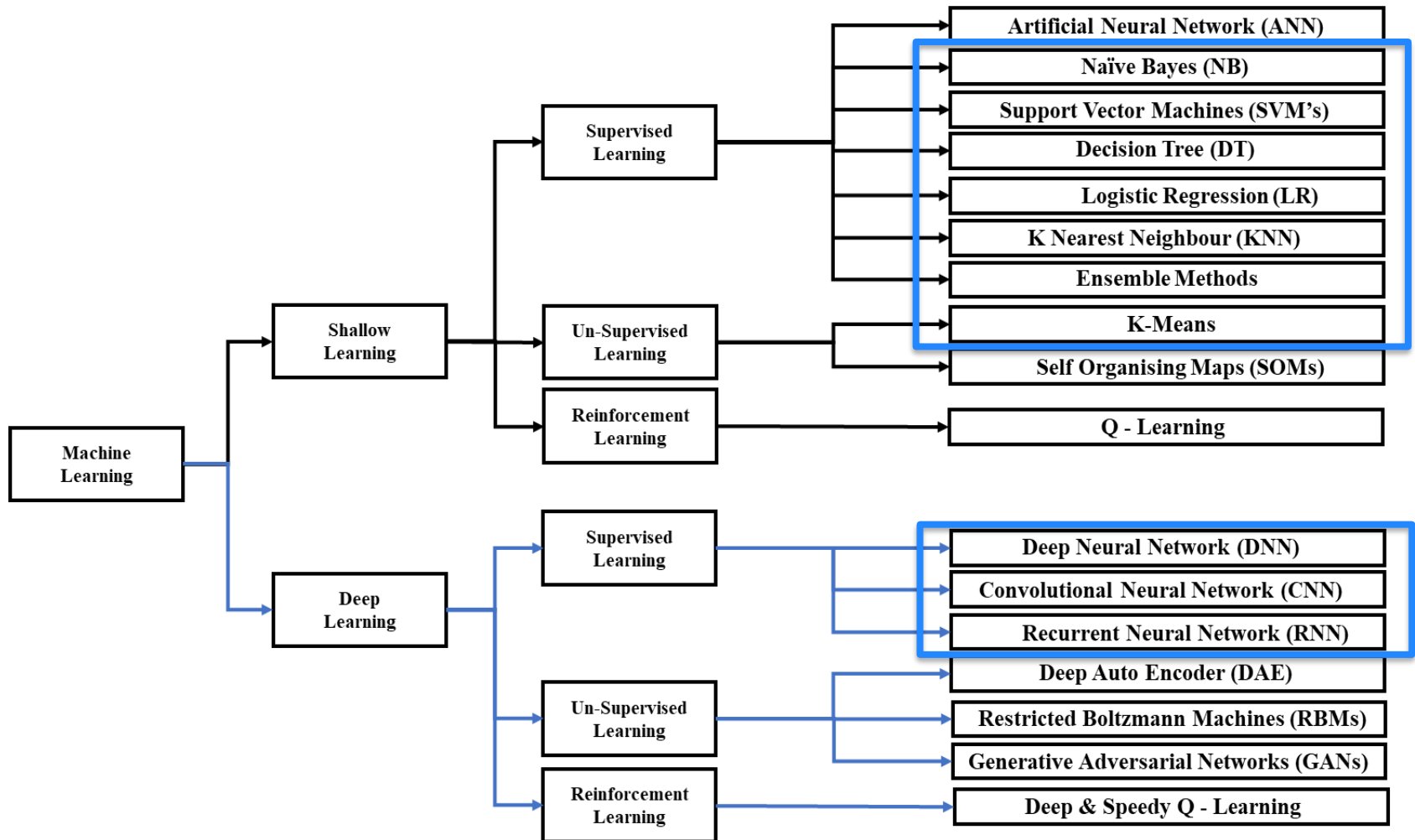


SDN Architecture + Security + Machine Learning

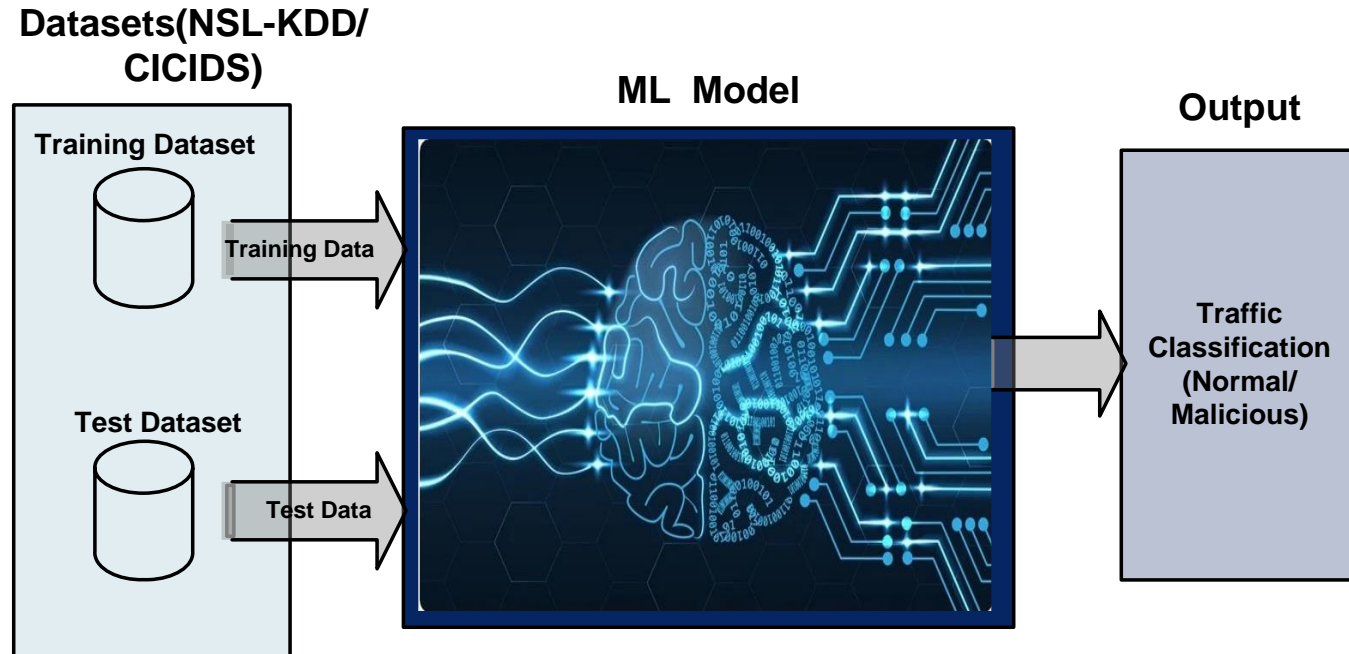
SINAPSE AI/ML review and findings for cyber security

- Intrusion detection approach
 - Intelligent attack detection
 - Traffic classification
 - Appropriate AI algorithm selection
 - Appropriate dataset selection
 - Training/testing/validation

ML Algorithms



ML Model and Performance Metrics



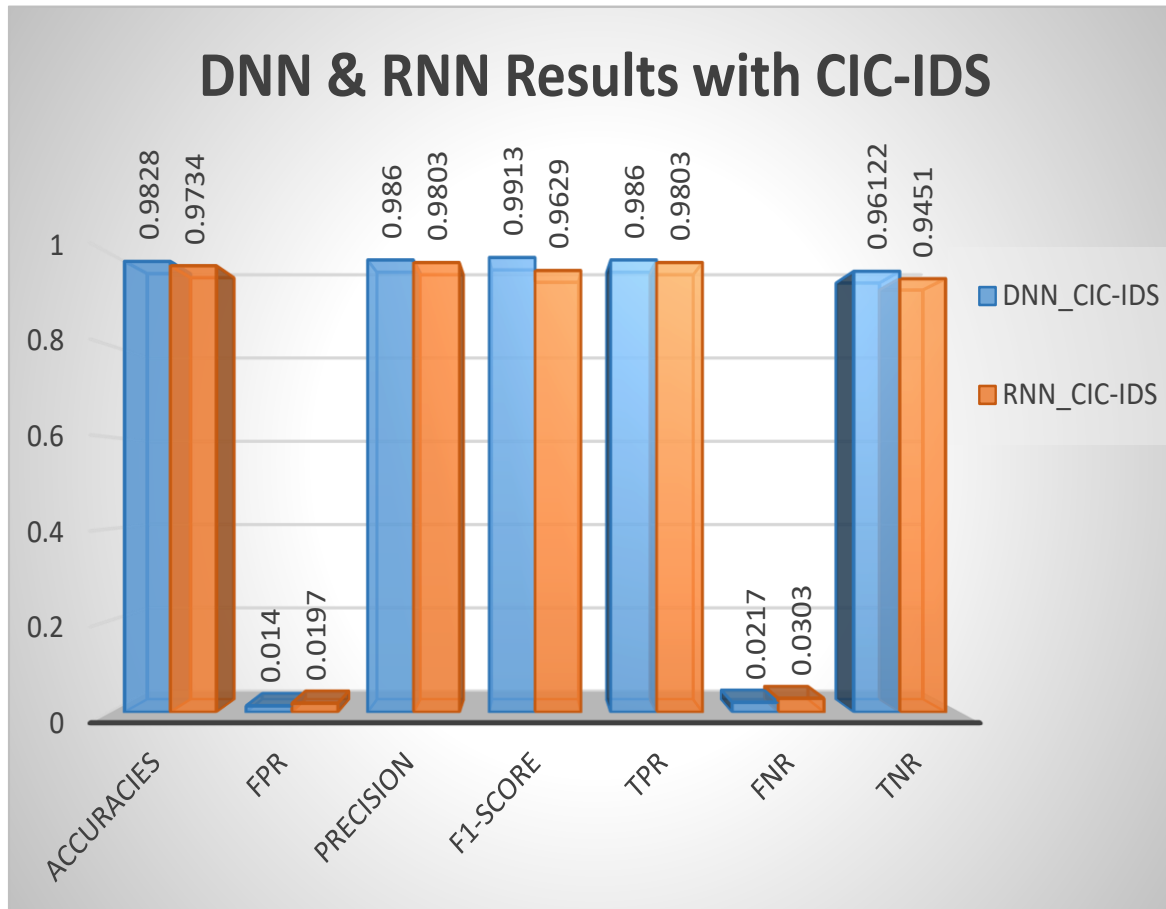
- **Output (Classification)**
 - Malicious Traffic
 - Non-Malicious Traffic
- **Performance Metrics**
 - Accuracy
 - False Positive Rate
 - Precision
 - F1 Score
 - True Positive Rate
 - False Negative Rate
 - True Negative Rate

Performance evaluation of all ML algorithms using NSL-KDD with MADM

MDMA scores using complete NSL-KDD

	A (+)	FPR (-)	P (+)	F1 (+)	TPR (+)	FNR (-)	TNR (+)	Scores	Rank
NB	0.9228	0.1103	0.9033	0.9227	0.9899	0.7867	0.9978	21.3288	9
SVM	0.9302	0.1336	0.9826	0.9521	0.9233	0.8715	0.8919	23.4400	6
DT	0.9273	0.0842	0.9543	0.9487	0.9431	0.4572	0.8267	24.1331	5
LR	0.9295	0.1269	0.9805	0.9516	0.9241	0.8896	0.8860	23.4146	7
KNN	0.9452	0.2825	0.9946	0.9582	0.9241	0.8902	0.9503	24.6198	4
Ensemble	0.9005	0.0998	0.9754	0.9338	0.8954	0.4010	0.8544	21.8578	8
CNN	0.9552	0.2825	0.9949	0.9655	0.9375	0.2583	0.9503	25.4966	3
DNN	0.9987	0.6982	0.9899	0.9923	0.9879	0.9851	0.8456	27.7903	1
RNN	0.9832	0.7036	0.9033	0.9555	0.9291	0.9016	0.0110	26.0445	2

Results for DNN and RNN



Targeted individual attack validation

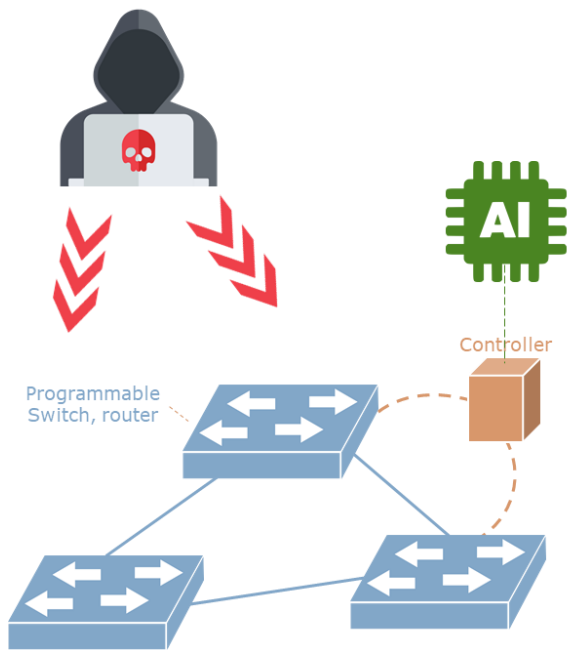
- DoS attack
- Probe attack
- User-to-Root attack
- Remote-to-Local attack
- Portscan attack
- Bot attack
- Infiltration attack
- Brute-Force attack
- SQL Injection attack

Conclusion

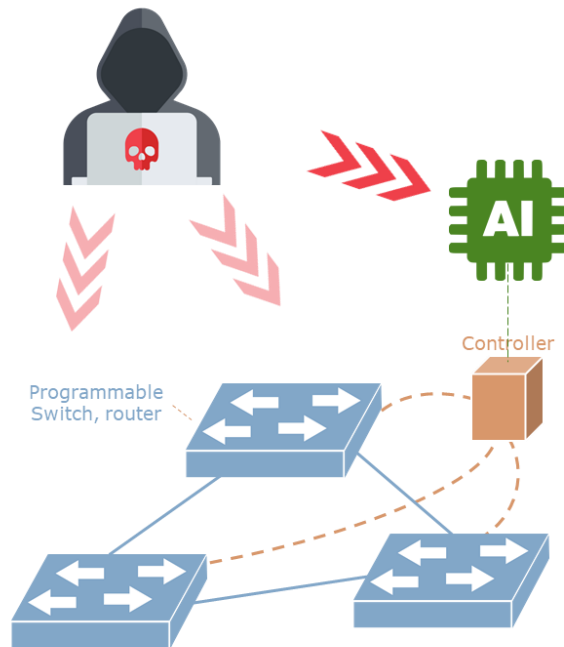
- For Small dataset
 - SL (Naïve based, SVM, KNN etc.) algorithms performed better than DL (DNN & RNN & CNN etc.)
- For Larger dataset
 - DL algorithms outperformed SL ones
- MADM method was used to rank machine learning algorithms
 - The best two shortlisted algorithms : DNN and RNN
- DNN compared to RNN using CIC-IDS datasets
 - Both algorithms showed sufficiently improved results (accuracy >0.98)
 - **DNN** performed slightly better than RNN

Security Architecture Evolution

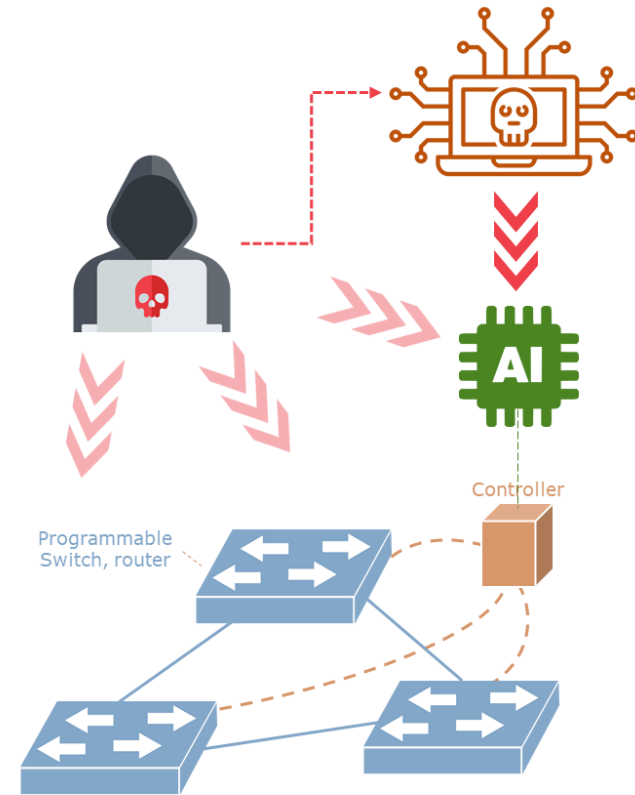
Level 1 – Securing the SDN Controller using **AI**



Level 2 – Securing **AI** from Cybersecurity Attacks



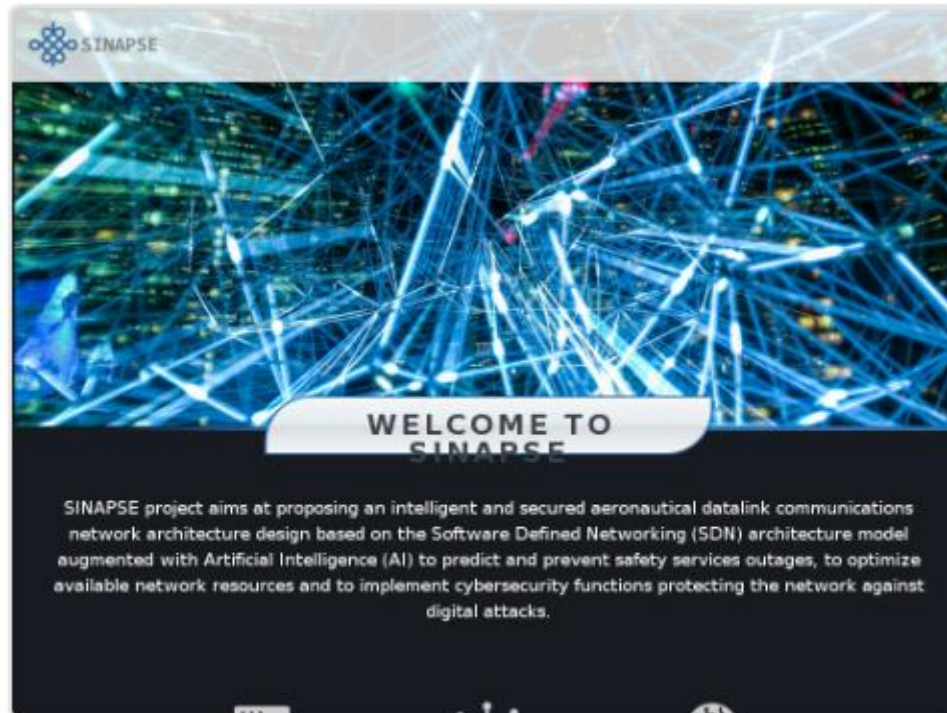
Level 3 – Protecting **AI** against **malicious AI** powered Cybersecurity Attack



Getting in touch with us



<http://sinapse-s2021.eu>





SINAPSE Project

Thank you very much for your attention!



This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2021 research and innovation programme under grant agreement No 783270



Founding Members



The opinions expressed herein reflect the author's view only.

Under no circumstances shall the SESAR Joint Undertaking be responsible for any use that may be made of the information contained herein.