Slide 1 (2 min)

Introduction to Autonomous Systems

- **Definition of AS**: what is an autonomous system? What are their applications?
- **Technological benefits**: Cost reduction, risk mitigation, operation in environments without human control.
- **Critical Technologies**: Planning and scheduling, layered control, model-based reasoning, reactive behavior, behavior coordination.

Autonomous systems, DP Watson, DH Scheidt - Johns Hopkins APL technical digest, 2005 - jhuapl.edu

Slide 2 (1 min)

Integration of AS with Modern Computing

- **Integration with IoT**: enhanced communication and data gathering from a wide array of devices.
- **Integration with Big Data**: to handle large and complex datasets.
- **Integration with ML**: train models to improve planning and scheduling.

Integrations between autonomous systems and modern computing techniques: a mini review, J Chen, M Abbod, JS Shieh - Sensors, 2019 - mdpi.com

Slide 3 (2 min)

Potential advantages of using ML

- **Algorithms for difficult learning tasks**: it is necessary for autonomous systems to have improved learning abilities such as online learning and learning from imbalanced data for sensing, planning, and motion control.
- **Models for sensing problems**: investigating learning-based solutions for autonomous sensing problems.

- **Solutions for control problems**: addressing learning-based control problems in autonomous systems.

Machine learning with applications to autonomous systems, X Xu, H He, D Zhao, S Sun, L Busoniu, SX Yang - 2015 - digitalcommons.uri.edu

Slide 4 (2 min)

Federated Learning

- **What is Federated Learning**: is a specific kind of machine learning that is used in autonomous systems.
- **How the Federated Learning works**: training models across decentralized data sources while preserving privacy.
- **Advantages for Autonomous Systems**: prioritize confidentiality and privacy, security, compliance and model optimization thanks to the use of Over-the-air technology.

Integrations between autonomous systems and modern computing techniques: a mini review, J Chen, M Abbod, JS Shieh - Sensors, 2019 - mdpi.com

Slide 5 (2 min)

Safety-assurance design

- **Why safety is important**: Autonomous Systems need to sense the dynamic environment, make decisions, and plan actions, but their reliability is hindered by environmental uncertainties, interferences, hardware/software faults, and attacks. Machine learning techniques, particularly neural networks, are difficult to analyze and verify, which is critical for ensuring safety in such systems.
- **Connected and Autonomous Vehicles example**: these vehicles face many uncertainties, like sensor errors or communication problems, and with ML integration some uncertainties is added.

Safety-assured design and adaptation of learning-enabled autonomous systems, Q Zhu, C Huang, R Jiao, S Lan, H Liang, X Liu… - Proceedings of the 26th …, 2021 - dl.acm.org

Slide 6 (2 min)

Safety problems and solutions

- **adversarial attacks**: the neural network could misclassify when there is a small but intentional change in the image.
  To achieve better robustness against adversarial attacks and ensure system safety, we will need methods for quantitatively evaluating the robustness of neural networks under input perturbations, and designing
  neural networks with more robust structures.
- **timing safety**: the learning model should work not only well but also fast. Various solutions have been explored to improve efficiency, such as algorithm improvements, new network architecture designs, network pruning and quantization, knowledge distillation (where a smaller model mimics a larger one), and early-exit networks that allow the system to exit computation early. Another technique is video fast-forwarding, which skips unimportant frames to enhance efficiency.

Safety-assured design and adaptation of learning-enabled autonomous systems, Q Zhu, C Huang, R Jiao, S Lan, H Liang, X Liu… - Proceedings of the 26th …, 2021 - dl.acm.org

Slide 7 (2 min)

AMLAS

- What is AMLAS and what is its aim: is a methodology to "Assurance of Machine Learning for use in Autonomous Systems". It comprises a set of safety case patterns and processes for integrating safety assurance and generating the evidence base to explicit justify the acceptable safety of ML components in Autonomous Systems.
- How is structured AMLAS: composed by six stages, each one gives its input to the next one.
  [FOTO]

Guidance on the assurance of machine learning in autonomous systems (AMLAS), R Hawkins, C Paterson, C Picardi, Y Jia… - arXiv preprint arXiv …, 2021 - arxiv.org

Slide 8 (4 min)

AMLAS stages

- **Stage 1**: defining the scope of the safety assurance process. Creating a mapping between the system-level safety and the safety requirements for the ML components.
- **Stage 2**: developing and validating ML-specific safety requirements from the system ones.
- **Stage 3**: managing the data used for developing, testing, and verifying the ML model. Defining data requirements ti ensure the dataset is sufficient. Generating three separated datasets for development, internal testing and verification.
- **Stage 4**: developing and testing the ML model using the development data and then the testing dataset.
- **Stage 5**: verifying that the ML model satisfies the safety requirements when exposed to inputs not present during model development.
- **Stage 6**: deploying the ML model into the target system and ensuring that the safety requirements are satisfied during system operation.

Guidance on the assurance of machine learning in autonomous systems (AMLAS), R Hawkins, C Paterson, C Picardi, Y Jia… - arXiv preprint arXiv …, 2021 - arxiv.org

Slide 9 (1 min)

Conclusion and Future Directions

- **Key Takeaways**: Autonomous systems are transforming industries through enhanced capabilities and integration with modern computing. Machine learning, particularly federated learning, plays a crucial role in improving the efficiency and adaptability of these systems. Ensuring safety is paramount, especially in critical applications like autonomous vehicles, requiring robust design methodologies like AMLAS.
- **Future Focus**: Further research in safety assurance, real-time performance, and robust ML integration. Expanding applications in fields like healthcare, smart cities, and space exploration.