Space & Cyber Brief Series

The SGAC Space and Cyber Security Project Group provides an international forum, where members can share their thoughts, views and opinion on international space and cyber policy issues to raise awareness among the next generation of space professionals about the global scale of space activities.

2022 - #2

Author: Rada Markova | Reviewed by Dr. Nebile Pelin Mantı, Sébastien Bonnart, Aaron Pickard, Kathiravan Thangavel, Laetitia Cesari Zarkan

AI IN THE CONTEXT OF SPACE AUTONOMY

Artificial intelligence (AI) is an approach to enhance autonomy in space. AI is **not limited** to a computerized form only, e.g. in the form of algorithms, but it also **includes elements of embodiments**.

Autonomy consists of a **characteristic of a system** whereas AI deals with the evolution of machine intelligence with the goal to maintain observability and controllability, and to create machine capability.

When considered in the broader context of **space autonomy**, the technology push behind the evolution of machine intelligence is taking place in a **shared** autonomy paradigm where **the human agent remains a crucial part** of AI-based space applications deployment.

MISSION EXECUTION AUTONOMY LEVELS FOR NOMINAL MISSION OPERATIONS

E1 **Mission execution under ground control; limited on-board capability for safety issues**

- Real-time control from ground for nominal operations
- Execution of time-tagged commands for safety issues

E2 **Execution of pre-planned, ground defined, mission operations on-board**

- Capability to store time-based commands in an on-board scheduler

E3 **Execution of adaptive mission operations onboard**

- Event-based autonomous operations
- Execution of on-board operations control procedures

E4 **Execution of goal-oriented mission operations on-board**

- Goal-oriented mission re-planning

In Europe

When **designing an algorithm for space application**, the practice is to **map the engineering design** following the **standards issued by the European Cooperation for Space Standardization** (ECSS).

The ECSS defines **four mission execution autonomy levels** relative to **on-board autonomy** for executing nominal mission operations.

A central role in **characterizing the degree of autonomy** has the granularity at which **interaction between the robot and the mission control** takes place.

A **very low level of autonomy** involves a **high level of control from the ground**, i.e., manually controlled, or automated systems.

A **high level of autonomy** allows **most of the functions to be performed on-board**.

Space & Cyber Brief Series

The SGAC Space and Cyber Security Project Group provides an international forum, where members can share their thoughts, views and opinion on international space and cyber policy issues to raise awareness among the next generation of space professionals about the global scale of space activities.

2022 - #2

Author: Rada Markova | Reviewed by Dr. Nebile Pelin Mantı, Sébastien Bonnart, Aaron Pickard, Kathiravan Thangavel, Laetitia Cesari Zarkan

STANDARDS FOR ARTIFICIAL INTELLIGENCE

Space engineers strive to **accelerate AI-related technologies** to overcome the difficulties posed by sporadic and slowed communication typical for teleoperation and circumstances precluding direct human oversight of certain functions.

The ECSS addresses **mission level security of the space segment** from a high-level cybersecurity perspective by **focusing on data and networks**.

SECURITY BY DESIGN
Encompasses the **integrity and confidentiality** of each data stream produced and the **authentication and authorization** of each telecommand received.

ISO/IEC TR 24028 APPLIED TO SPACE

TECHNICAL REPORT
ISO/IEC TR 24028 (Standard)
On security, notably in the context of trustworthiness of systems providing or using AI.

Taking a holistic approach to **standardize the entire AI ecosystem**, the ISO/IEC issued a number of standards covering various aspects of AI.

ISO: International Organisation for Standardization | IEC: International Electrotechnical Commission

APPLYING TRUSTWORTHINESS APPROACHES TO AI SYSTEMS

The Standard focuses upon machine learning. According to it, AI systems can be **subject to targeted security threats**, notably data poisoning, adversarial attacks, and model stealing where typical attacks on machine learning would involve digital attacks affecting data confidentiality, integrity, and availability.

Furthermore, the Standard recommends **preventive and mitigation measures**, including **human-in-the-loop control points** and **testing and evaluating AI systems**.

KEEPING A GENERAL APPROACH

The Standard **does not address differences between various machine learning techniques**, for instance, between deep neural learning methods compared to other supervised learning approaches.

The Standard makes reference to a **general process of risk management** such as the one defined in ISO Risk management guidelines. In order to develop a strategy for risk management and **ensure the resilience of a space system**, said guidelines need to be interpreted considering the **extent of the risk specific to** AI, all used technologies and their interaction in the space system, which is, by its very nature, a cyber-physical system.

Space & Cyber Brief Series

The SGAC Space and Cyber Security Project Group provides an international forum, where members can share their thoughts, views and opinion on international space and cyber policy issues to raise awareness among the next generation of space professionals about the global scale of space activities.

2022 - #2

Author: Rada Markova | Reviewed by Dr. Nebile Pelin Mantı, Sébastien Bonnart, Aaron Pickard, Kathiravan Thangavel, Laetitia Cesari Zarkan

INTERDISCIPLINARY DISCUSSION

Building upon synergies between different industries is another way to go towards forging **cybersecurity for AI-based space applications**.

NUCLEAR AND SPACE

Anticipated that AI standardization in the nuclear sector, which is currently ***in progress***, will refer to **ITU standards related to AI**. According to the preliminary architecture of the portfolio, it will include security-related topics, such as **risk assessment of AI applications** and **data quality management** for AI for nuclear energy, which may be relevant to the space sector.

AUTONOMOUS VEHICLES AND SPACE

The way autonomy is defined by the Society of Automotive Engineers (SAE) exhibits similarities to space autonomy. Notably it could be argued that the **taxonomy** established by the SAE, which covers **6 levels of vehicle driving automation**, shares a similar paradigm with space autonomy, namely human-machine interaction that helps to outline different system capabilities corresponding to specific degree of autonomy.

Additionally, autonomous space applications and autonomous vehicles are comparable due to the **complexity of their technical systems** and the many resulting interactions where **the system's behavior is susceptible to changes in the environment**.

Hence, the cybersecurity approach towards AI employed in the autonomous car industry, which consists in **implementing security solutions to secure AI in relation to other components and services of the system**, could be relevant to the space industry.

In the context of autonomous vehicles, cybersecurity threats and vulnerabilities are often **addressed under the angle of safety**, notably where intentional attacks aim to interfere with the AI system and disrupt safety-critical functions. Cybersecurity is thus part of the broader framework of **road vehicles safety**. When considered in the context of advanced functionalities included in vehicles throughout AI methods, **safety is of paramount concern for the road vehicles industry**.

Building upon this model, cybersecurity vulnerabilities of space applications of AI could be addressed by **integrating threat modelling within the formal verification process** typically deployed to **ensure and validate functional and safety properties** of the space systems.

Space & Cyber Brief Series

The SGAC Space and Cyber Security Project Group provides an international forum, where members can share their thoughts, views and opinion on international space and cyber policy issues to raise awareness among the next generation of space professionals about the global scale of space activities.

2022 - #2

Author: Rada Markova | Reviewed by Dr. Nebile Pelin Mantı, Sébastien Bonnart, Aaron Pickard, Kathiravan Thangavel, Laetitia Cesari Zarkan

FUNCTION-SPECIFIC AI

Autonomy in space systems can be addressed at **the system (or generalist AI) and the function-specific levels.**

Integrating autonomy at function-specific level is more common.

To address AI **at the functional level** within space components and see **how it interacts with other components of the system**, a **reference architecture** can be used. Unlike other situations where it has been applied, here **reference architecture** relies upon a high-level specification of space systems and **consists of an initial cyber security analysis preceding low-level security analysis**.

Certification may play a **crucial role in formalizing AI reliance and interoperability**, which then could contribute to its **wider acceptance and applicability**. However, typical certification procedures for traditional software cannot be applied in a straight-forward manner to AI, notably machine learning. Hence, certifying AI would call for review of major certification topics.

RELEVANT STANDARDS

- **Technical Report, ISO/IEC TR 24028**, "Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence" First edition 2020-05.
- **ISO 31000:2018**, provides a common approach to manage any type of risk faced by organizations and could be customized to any organization and its context. It is not industry or sector specific.
- **ISO 26262 -1:2018** on functional safety.
- **SOTIF ISO/PAS 21448:2019** Road vehicles – Safety of the intended functionality.
- **F.AICO-GA, ISO/IEC SC42**, technical specifications for artificial intelligence cloud platform: general architecture.
- **F.748.12** (ex. F. AI-DLFF) approved 2021-06-13, Deep learning software framework evaluation methodology.
- **ECSS-E-ST-70-11C**, European Cooperation for Space Standardization, Space engineering, Space segment operability, 31th July 2008.

Space & Cyber Brief Series

The SGAC Space and Cyber Security Project Group provides an international forum, where members can share their thoughts, views and opinion on international space and cyber policy issues to raise awareness among the next generation of space professionals about the global scale of space activities.

2022 - #2

Author: Rada Markova | Reviewed by Dr. Nebile Pelin Mantı, Sébastien Bonnart, Aaron Pickard, Kathiravan Thangavel, Laetitia Cesari Zarkan

FURTHER READING AND RESOURCES

- Jan-Gerd Mess, Frank Dannemann, Fabian Greif, 'Techniques of Artificial Intelligence for Space Applications - A Survey', (2019) European Workshop on On-Board Data Processing.
- Stephanie Sze Ting Pau, Judith-Irina Buchheim, Daniel Freer, Guang-Zhong Yang, 'Future of human-robot interaction in space', pp. 359 in Yang Gao (eds), Space Robotics and Autonomous Systems technologies (IET, 2021).
- Daowei Bi 'Develop International Standards on AI for Nuclear Energy' (2021) AI for nuclear energy, ITU.
- Society of Automotive Engineers (SAE), 'Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles' (2018).
- Jenay M. Beer, Arthur D. Fisk, Wendy A. Rogers, 'Towards a framework for levels of robot autonomy in human-robot interaction' (2014), Journal of Human-Robot Interaction.
- Alexander Poddey, Tino Brade, Jan E. Stellet, and Wolfgang Branz, 'On the validation of complex systems operating in open contexts' (2019).
- European Union Agency for Cybersecurity, Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving, February 2021.
- ENISA, Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving, February 2021.
- Carsten Maple, Ugur Ilker Atmaca, Gregory Epiphaniou, Gregory Falco, and Hu Yuan, 'Cyber security of New Space systems' in Yang Gao (eds), Space Robotics and Autonomous Systems technologies (IET, 2021)', p. 427.
- Issa A. D. Nesnas, Lorraine M. Fesq, Richard A. Volpe, 'Autonomy for space robots: past present and future' (2021), Current Robotics Reports.
- Lars Kunze, Nick Hawes, Tom Duckett, Marc Hanheide, Tomas Krajnik, 'Artificial Intelligence for Long-Term Robot Autonomy: A Survey' (2018) IEEE Robotics and Automation Letters.
- Matthew Bradbury, Carsten Maple, Hu Yuan, Ugur Ilker Atmaca, Sara Cannizzaro, 'Identifying Attack Surfaces in the Evolving Space Industry Using Reference Architectures' (2020) IEEE Aerospace Conference.
- Philip Matthias Winter et al. 'Trusted Artificial Intelligence: Towards Certification of Machine Learning Applications' (White Paper, 2021).