SAFE
Security and Freedom for Europe

Information and data protection in XR training scenarios:

straightforward solutions to comply with modern requirements.

Mr. Andrea D'ANGELO – President, Fondazione SAFE

19 October 2023, MSG-207 Symposium, Monterey (CA, USA)

Agenda

1. Overview of Fondazione SAFE
   - Who we are and what we do
   - Our activities entailing XR.
   - The Calvarina Testing & Training facility.

2. Presentation of the Paper
   - General security context
   - The use of XR and VR technology in the military context
   - Shortcomings identified so far in military applications
   - Current cybersecurity guidelines for NATO
   - Data/cyber security risks in designing a CBRN VR scenario
   - Solutions adopted by Fondazione SAFE

3. Conclusions and final considerations

Fondazione SAFE - Who are we?

Fondazione SAFE is an **independent Italian not-for-profit foundation**, established in 2018.

SAFE promotes, through its own funds and by participating in calls for projects financed by the European Union and other international donors, **high-impact** non-profit activities **in the sectors of security, defense, and rule of law**.

Project management

Capacity building and training

Technological innovation in the security and defense sectors

Monitoring and Evaluation

Fondazione SAFE - Our team

Dynamic, highly specialised team composed by a core staff of 20 people dislocated between Ravenna and Soave, a project office in Lebanon (Beirut) and a project office in Lybia (Tripoli).

40 projects implemented since 2018, 28 of which are currently ongoing

More than **70.000.000 €** of overall budget under implementation

70+ partners in project activities and part of SAFE’s network

SAFE Security and Freedom for Europe

S&T organization

Ongoing projects with XR elements (1/2)

- Development and maintenance of rescEU CBRN mobile laboratories and rescEU CBRN detection, sampling, identification and monitoring capabilities

MoSaiC

- Real-time Monitoring and Sampling of CB menaces for improved dynamic mapping of threats, vulnerabilities and response capacities

VERTIgO VR

- Virtual Enhanced Reality for interoperable training of civilian and military CBRN operators – VERTIgO

Ongoing projects with XR elements (2/2)

- NATO HFM-NMSG-354 Research Task Group on the “Study, Design, Building and Deployment of a CBRN XR Training Platform”

- SAFE self-funded initiative for the virtualization of the Calvarina facility (creation of a CBRN VR training scenario involving a clandestine facility).

The Calvarina testing & training area

- Former NATO base, offering **25.000m2 of testing & training ground** in an isolated area.
- Cleaned, restored and secured in 2020.
- Hosts **various buildings of an urban-military nature**, including two underground bunkers and a take-off/landing area for helicopters/drones.
- Currently, the only Testing & Training Facility in Italy that can be accessed by **both private and public actors**.

SAFE Security and Freedom for Europe

S&T organization

Information and data protection in XR training scenarios: straightforward solutions to comply with modern requirements

General context:

- Global crises relaunched the concept of **CBRN as a concrete threat**
- **Affordability and increased efficiency** are more and more attractive even to major military powers
- XR/VR solutions are gaining **growing attention** also thanks to enhanced realism

The use of XR and VR technology in the military context

- Armed forces are increasing introduction of XR and VR solutions.
- To date, training activities (including for maintenance of equipment) are the ones most impacted by VR/XR applications.
- The use of XR headsets during combat operations is being tested for ground troops.

IVAS system undergoing testing with the US army. Credit: Microsoft.

SAFE Security and Freedom for Europe

S&T organization

Shortcomings identified so far in military applications

1. Affordability – distributed acquisition of new technologies can be expensive.
2. Technological Maturity - the state-of-the-art of XR/VR solutions is evolving rapidly
3. Personnel - greater strain on existing IT personnel and trainers is expected at the beginning.
4. Cybersecurity - vulnerabilities of XR/VR systems are to be assessed and covered continuously.

SAFE Security and Freedom for Europe

S&T organization

Current cybersecurity guidelines for NATO

Cyberspace has been recognised among the traditional domains of operation since 2016. This includes identification and acknowledgement of malicious cumulative cyber risks.

However:

- Dedicated technical standards needs to be developed and are currently lacking (both EU and NATO)
- This evolution depends on the commitment of States to develop standards
- NATO members are ultimately responsible for their own cyber defence
- EU MS who are also NATO members must consider GDPR guidelines

Data/cyber security risks in designing a CBRN VR scenario

From the hardware perspective, wireless solutions are to be preferred for freedom of movement, but entail increased risk of:

- Eavesdropping
- Interferences
- Unauthorized accesses

A student performs a simulated pre-flight inspection on a VR system. Credit Embry-Riddle/Daryl LaBello

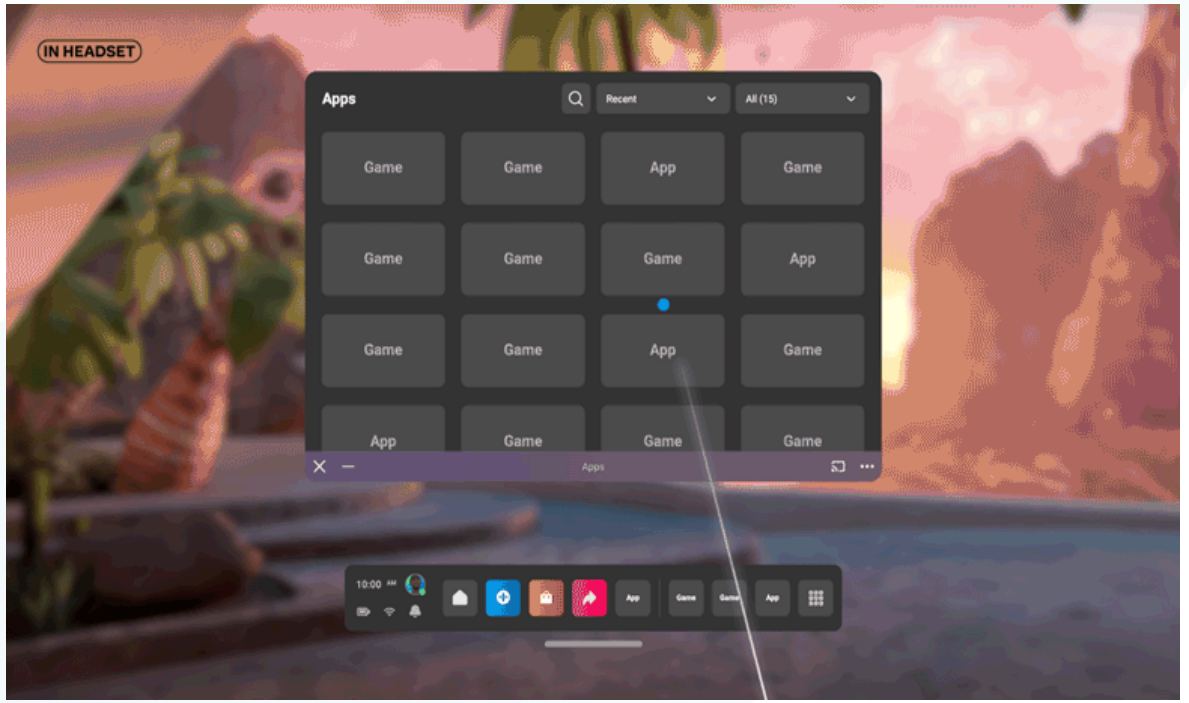
SAFE Security and Freedom for Europe

S&T organization

Data/cyber security risks in designing a CBRN VR scenario

From the software perspective, the following elements are to be considered:

- Presence of sensitive data and content regarding the settings of the scenario
- Appropriate encryption level to access the library/launch the software
- Third party software monitoring to avoid unauthorised data transmission



Example of built-in lock system to access files/apps.
Credit: META

Data/cyber security risks in designing a CBRN VR scenario

Additional key elements regarding the settings of the scenarios:

- When operating in a scenario entailing classified data for its setting, cybersecurity measures must be addressed properly.

- Even when operating in a scenario setting that does **not** entail **classified information** for its development, the **procedures** undertaken by the trainees **may be sensitive**.

Data/cyber security risks in designing a CBRN VR scenario

Generation of aggregated trainees' data and cyber/data security issues:

- The generation of an automated **After Action Report** (AAR) always brings data protection issues for the trainees and possible data classification concerns.

- Even if anonymised, **aggregated data** coming from several AARs must be considered **classified** as it potentially highlights **gaps in** trainees' **preparation** – and MS defence.

SAFE Security and Freedom for Europe

S&T organization

Data/cyber security risks in designing a CBRN VR scenario

When it comes to network setup, different solutions involve different limitations:

- Internet-connected: is the most exposed to risks such as unauthorized/involuntary upload or transfer of information during the development phase, data breaches, and unauthorized access.

- Intranet-connected: mostly vulnerable to insider attacks, robust security measures to prevent unauthorized access must be put in place.

- Standalone offline: it greatly reduces the risks associated with network connectivity. It allows the whole system and associated scenarios to work isolated from the external environment.

Solutions adopted by Fondazione SAFE in the context of EU and NATO RTG sponsored activities

Hardware

- Integrity of headsets (conducted by the scenario developers)
- Password protection that requires hard reset for removal, making the headset data secure
- Physical security of the headsets guaranteed both inside and outside the HQ

Testing of the CBRN VR solution at SAFE Testing & Training facility.
Credit: SAFE

Solutions adopted by Fondazione SAFE in the context of EU and NATO RTG sponsored activities

Software

- Password prompt triggered while accessing scenario
- BIOS encryption, SSD encryption and user and password
- Generation of anonym AARs to comply with data protection
- To avoid the generation of classified aggregated data, XR can be used instead of pure VR

Solutions adopted by Fondazione SAFE in the context of EU and NATO RTG sponsored activities

Network

- Use of trusted and heavily protected networks if and when necessary.
- Offline, standoffs versions are to be preferred in any other case.
- Use dedicated hardware to host all the software related to the XR/VR solution, as to minimize network's access from different devices

SAFE Security and Freedom for Europe

S&T organization

Conclusions and final considerations

1. Growing interest in XR/VR solution for armed forces around the world
2. Need to urgently define specific NATO technical standards and centralise the effort
3. Creative and low-cost solutions can be put in place as stop-gap measures
4. The technical aspects must be substantiated by the spread of a cybersecurity culture at all levels

SAFE

Security and Freedom for Europe

Mr. Andrea D'ANGELO – President, Fondazione SAFE
andrea@safe-europe.eu