Towards Network Activity Visualization in Mixed Reality as Proof of Concept for Military Decision Makers

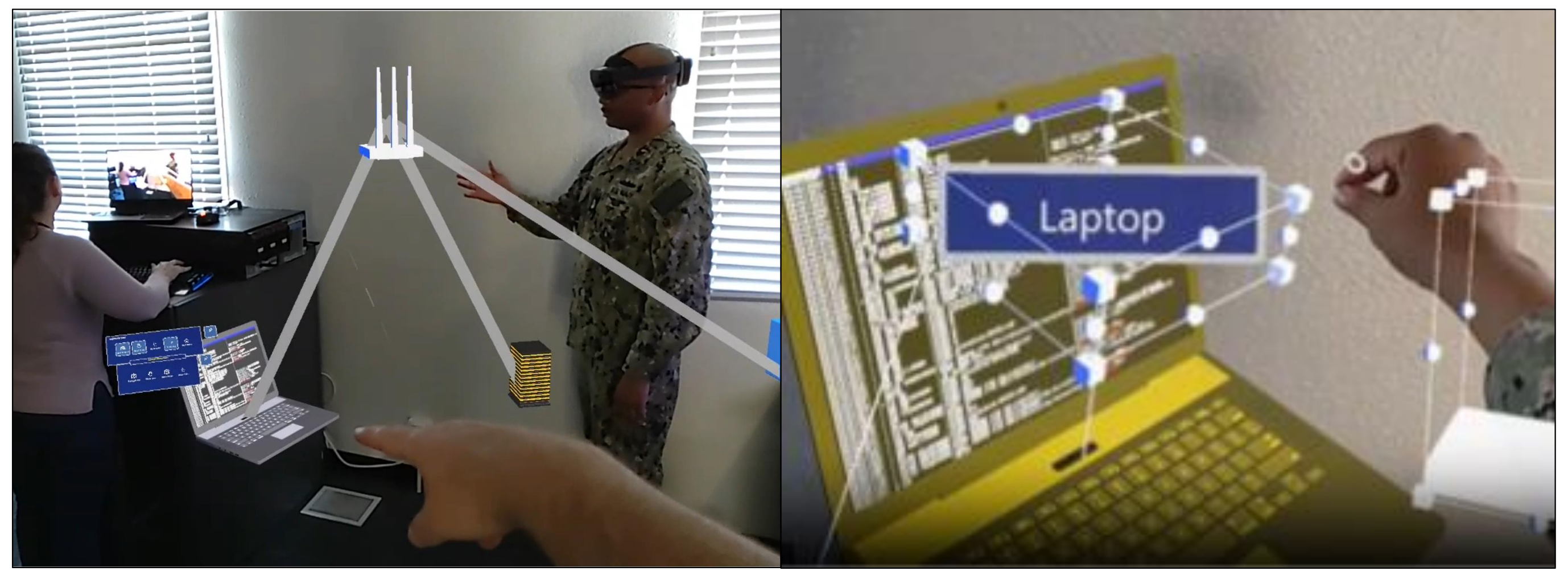
Clinton Anderson, Lawrence Kerr

Naval Information Warfare Center (NIWC) - Pacific, San Diego, CA

Background

In 2018, the United States Government Accountability Office (GAO) conducted a comprehensive review of cybersecurity in nine major defense acquisition office programs [1]. The GAO discovered that testers were able to gain control of systems without being detected using relatively simple techniques. In US Naval operations, skilled hackers can employ sophisticated tactics, making them hard to track. Therefore, improved visual communication from the GAO to program officials could have facilitated a better understanding of the deeper exploits that were dismissed, demonstrating the right tactics effectively.

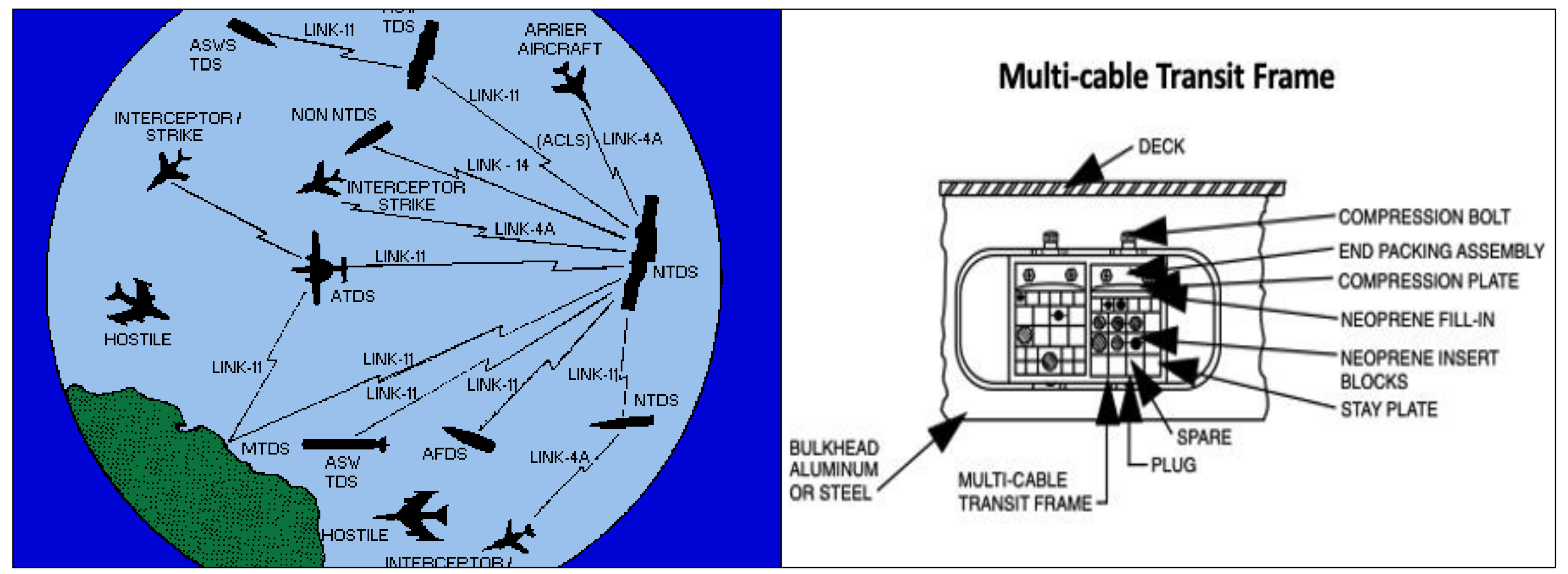
However, understanding the complexities of network traffic can be challenging for those not familiar with networking components, configurations, encryption, and how the physical environment affects connectivity. This is particularly true for time-critical operations where multiple actors with different skillsets need to collaborate effectively. While in-depth technical expertise is typically limited to enlisted members, decision-makers such as U.S. Department of Defense administrators, equipment contractors, and military officers must successfully integrate their decisions with the technical capabilities of the operational personnel. In this poster, we propose a framework that bridges the gap between technicians' explanations of complex cyber systems and decision-makers in a faster, more understandable, and more comprehensive manner compared to traditional methods like spoken word, slideshows, or graphs.



Demo from two shared mixed reality (MR) users to a screen-viewer (left)
Manipulation of a laptop model and its name tooltip using MRTK (right)

Objectives

1. Develop a framework that bridges the gap between technicians' explanations of complex cyber systems and decision-makers' insight
2. Create a shared, real-time, mixed reality app that depicts traditionally intricate network systems in a digestible and easy-to-analyze format



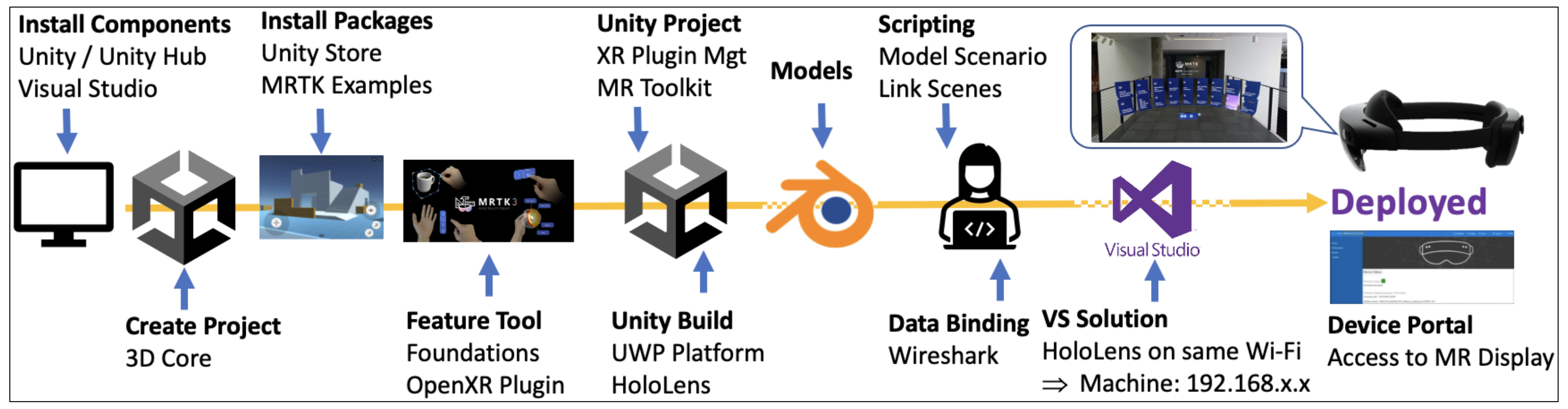
Multicomponent Naval Tactical Data System that can be expanded on in 3D (left) [2]
Traditional 2D orientation from tech manuals makes door structure unclear (right) [3]

Methods – Tools and SDKs

- Unity Hub, Unity Game Engine
- Universal Windows Platform
- Microsoft Mixed Reality Toolkit
- Open XR Plugin
- Microsoft HoloLens 2
- Wireshark Network Analyzer
- Microsoft Device Portal
- Blender 3D Modeling Software

Methods – Prototype Development

1. **Install Packages with Unity Game Engine using Unity Hub**
   - Create project with latest Unity 3D Core package using Unity Hub
   - Install packages: current Microsoft Visual Studio C#, OpenXR Plugin
2. **Install Mixed Reality Toolkit using MRTK Feature Tool**
   - Use the MRTK Feature Tool to install MRTK Toolkit using Examples Hub as a base
   - Create and import models using Blender 3D Modeling software (**see below**)
3. **Create Simulated Environment with Modeled Network Components**
   - Read Wireshark columns to convert internet protocol (IP) sources and destinations into "Network Object" prefabs imported from Blender models
   - Use Scripts to create descriptions and troubleshooting steps for components
4. **Build Application to Microsoft HoloLens or Emulator**
   - Build using Visual Studio solution to mixed reality device
   - Use Mixed Reality Device Portal to have multi-users view the same application concurrently on multiple HoloLens devices or a separate computer screen on the same wireless network



Install Components
Unity / Unity Hub
Visual Studio

Install Packages
Unity Store
MRTK Examples

Unity Project
XR Plugin Mgt
MR Toolkit

Models

Scripting
Model Scenario
Link Scenes

Deployed

Create Project
3D Core

Feature Tool
Foundations
OpenXR Plugin

Unity Build
UWP Platform
HoloLens

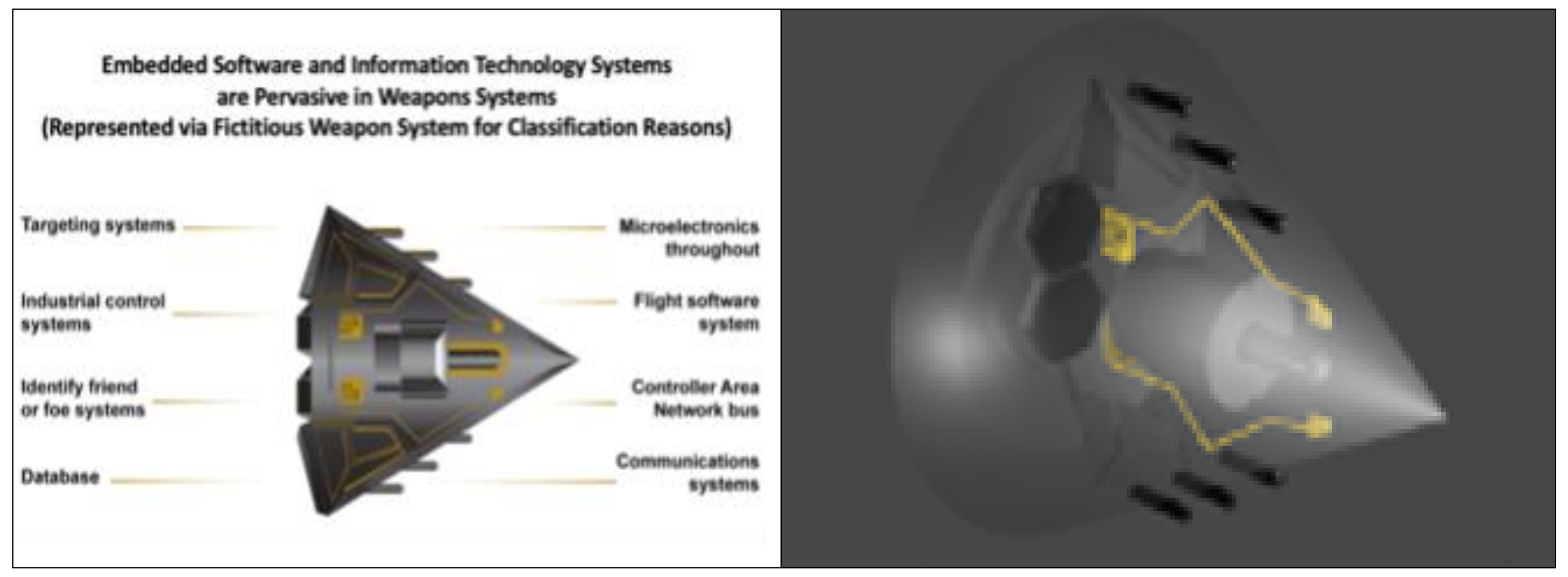
Data Binding
Wireshark

VS Solution
HoloLens on same Wi-Fi
⇒ Machine: 192.168.x.x

Device Portal
Access to MR Display

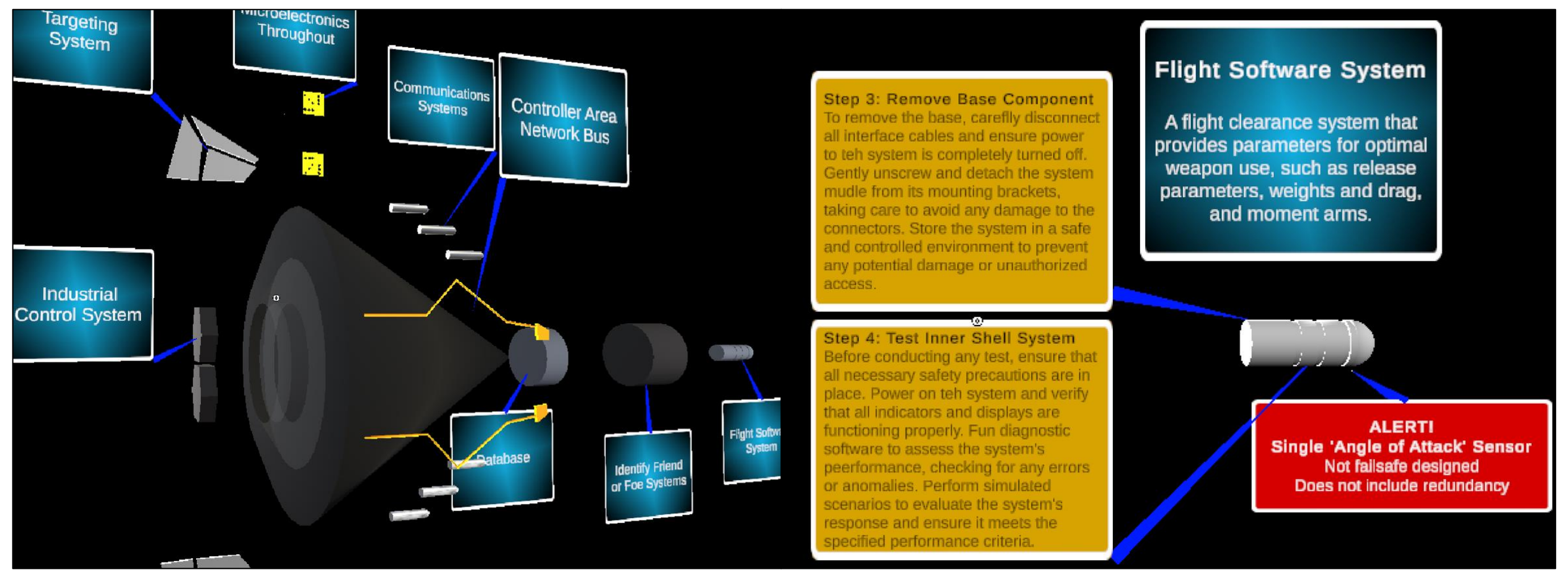
Methods– "Network Object" Model Development

1. **Model Object in Blender**
   - Item constructed from horizontal/vertically image file of desired component
   - Materials colored and provided 3D projections to distinguish features
   - Child components created based on desired animation sequences


Embedded Software and Information Technology Systems are Pervasive in Weapons Systems
(Represented via Fictitious Weapon System for Classification Reasons)
Targeting systems
Industrial control systems
Identify friend or foe systems
Database
Microelectronics throughout
Flight software system
Controller Area Network bus
Communications systems

Fictitious weapon shown in the Government Accountability Office (GAO) paper (left) [1]
Weapon modeled in Blender. Casing is transparent, items colored for contrast (right)

2. **Create "Network Object" Unity Prefab**
   - Blender object imported with completed component as parent, separate children
   - Animated in separate scene with six-second Unity Timeline animation clips
   - Prefab created in main scene with OnClick() methods to open clips and steps

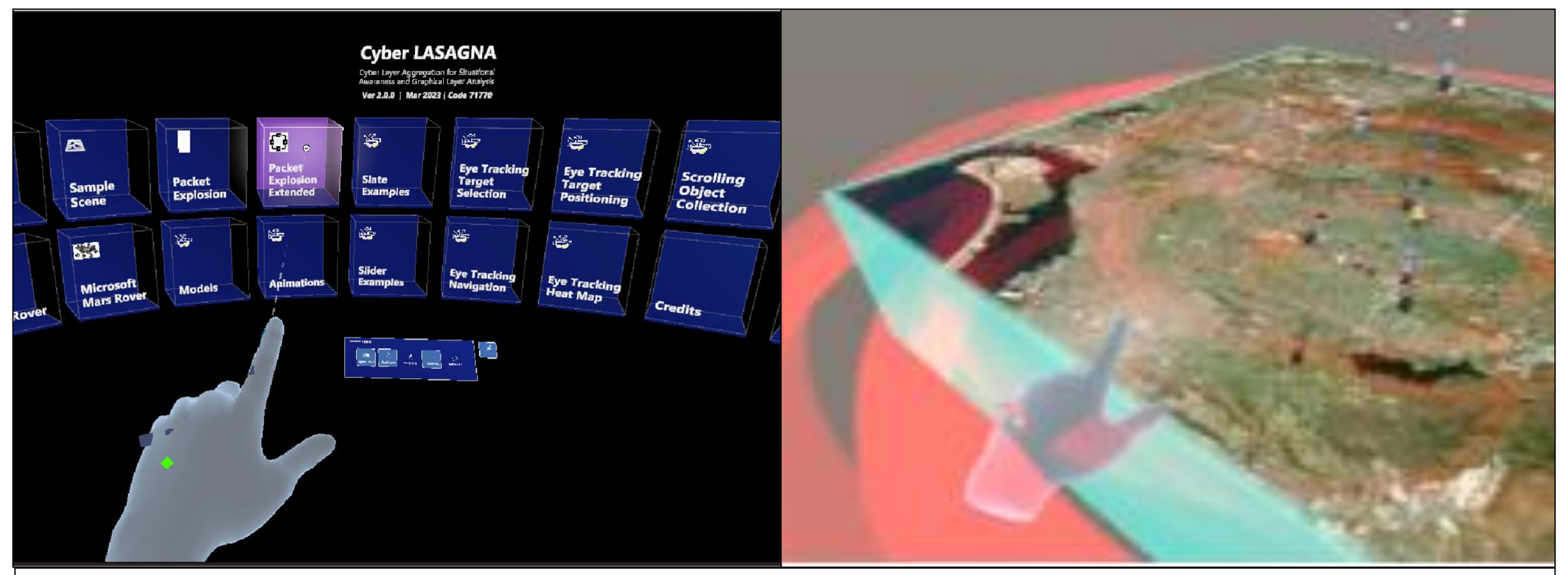

Targeting System
Microelectronics Throughout
Communications Systems
Controller Area Network Bus
Industrial Control System
Database
Identify Friend or Foe Systems
Flight Software System
Step 3: Remove Base Component
Step 4: Test Inner Shell System
Flight Software System
A flight clearance system that provides parameters for optimal weapon use, such as release parameters, weights and drag, and moment arms.
ALERT!
Single 'Angle of Attack' Sensor
Not failsafe designed
Does not include redundancy

"Network Object" Weapon prefab expanded in Unity with tooltip labels (left)
Description (blue), Repair steps (orange), and Alert (red) provided on item click (right)

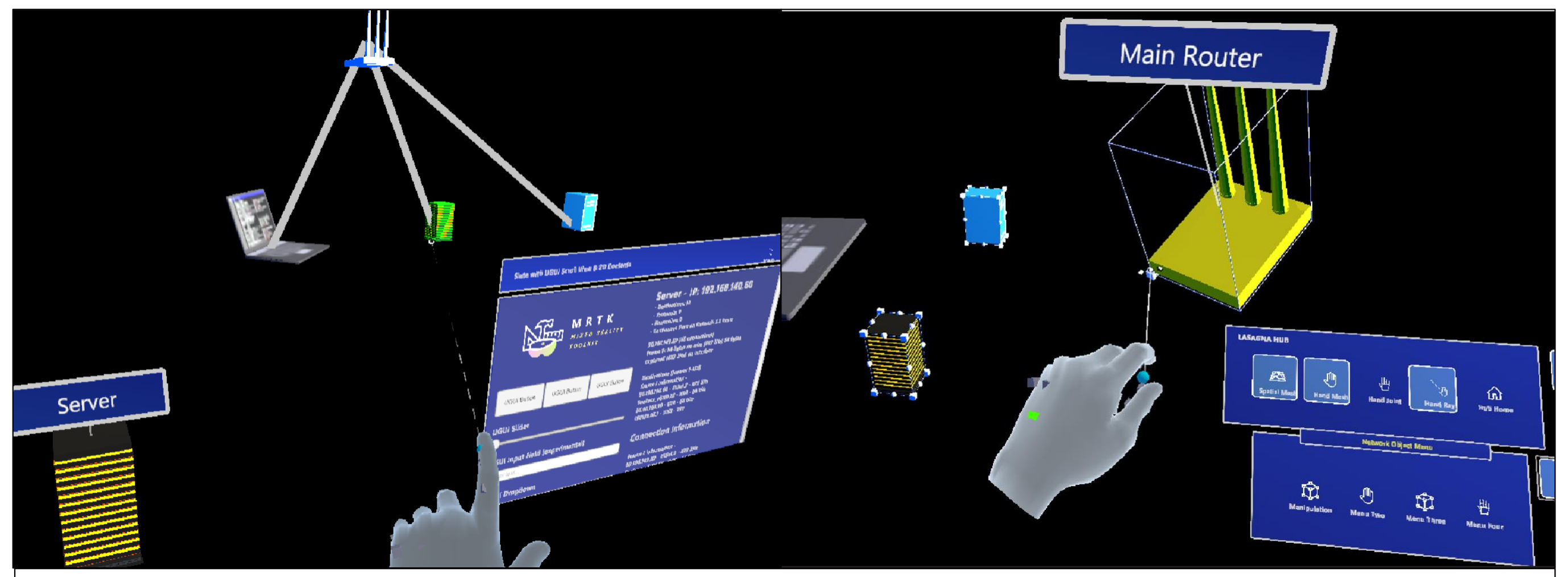
Results – Dynamic Cyber-Networking Environment

LASAGNA describes complex objects in an accessible manner, enhancing descriptions of intricate network communication among multiple actors. One example is the intersystem communication employment shown in **Objectives**, showcasing data links like Link-11 and Link-14 shared among aircraft, ships, and facilities.

1. **Shared 3D Visualization Environment**
   - Technician uploads network traffic data, such as logs, Wireshark data, or manually
   - Real-time delivery can be shared among multiple testers, operators, and decision-makers in a pipeline, and can be viewed on several MR devices and a 2D screen
2. **Instructional and Troubleshooting Steps**
   - Provides ability to detail explanations of components, troubleshooting instructions, alerts, and showcase components without jargon in a large networked system



LASAGNA Software Hub based on native MRTK Example Hub (left)
Geography Scene with emanating signal displacement to show network strength (right)



Network connecting lines, model expansion of yellow server showing data on slate (left)
Users move, scale, and rotate items. Object menu specific to scene and model (right)

Conclusions

- Created prototype of "LASAGNA," a shared mixed reality visualization tool that facilitates the understanding of cyber-related network configurations
- Prototype models were developed with broad applicability, replacing traditional manual or slideshow-rendered images, enabling technical experts in the military to enhance their system descriptions for senior officers, administrators, and testers

Future Objectives

- LASAGNA can be extended for use as a daily malware detection system, aiding IT watch standers in quickly assessing ship computers during the last hour of their shifts
- Can also be utilized for capture the flag scenarios and IT equipment training tutorials
- A well-designed framework, as well as user study and analysis to include the present system, can be adapted to various schematic and drawing types across different fields. This includes applications such as damage control in firefighting, electric plant reconfiguration, supply equipment logistics, and the operation of mechanical systems

References

[1] U.S. Government Accountability Office. (2019). Weapons System Security: DoD Just Beginning to Grapple with Scale of Vulnerabilities. Retrieved from https://www.gao.gov/assets/gao-19-128.pdf

[2] U.S. Navy. (n.d.). NEETS Module 17 Radio Frequency Communication Principles (Figure 5-13: Intersystem communication employment). Retrieved from http://www.tpub.com/neets/book17/77b.htm

[3] U.S. Navy. (n.d.). Chapter 3: Ship Compartment and Watertight Integrity (Figure 3-16: Multi-cable transit frame). In Damage Controlman Online Training Course. Global Security. Retrieved from https://www.globalsecurity.org/military/library/policy/navy/nrtc/14057_ppr_ch3.pdf

Acknowledgements

Funding provided by Naval Information Warfare Center Pacific NISE

November 2023 • Approved for Unlimited Distribution (Dist A) under RSTI-8422. Contact: clinton.j.anderson.civ@us.navy.mil