ENCODE aimed to advance the commercial opportunities of operating a teleoperated fleet of commercial vehicles safely and efficiently, with ANGOKA onboarded as cybersecurity lead to implement measures that embedded trust and resilience within the teleoperated networks and ensured continuity of service.

In project partner Coventry University's threat assessment, teleoperations and CAN Bus were identified as the elements with the highest risk from several possible cyber threats to the vehicle network and the operations. Exploiting them can see hackers gain unprivileged access via vehicle communications channels, misconfigure the vehicles, and even disrupt service entirely to cause economic and operational damage to the teleoperator.

One of the attack scenarios explored by the project's consortium was the risk of spoofing a remote teleoperator, a threat that could jeapordise the safety and efficiency of an entire vehicle fleet. In this instance, an attacker compromises the VPN connection between the teleoperation system and the vehicle and masquerades as the teleoperator, disrupting the operation as they remotely intercept and modify vehicle commands.

In normal operations, the teleop would send a 'brake' command for the vehicle to slow down when it reaches a pedestrian crossing. The vehicle would reply with the status message of 'braking' and action the command. However, an attacker acting as the teleops could replace these messages with false information and command the vehicle to accelerate, which would appear as a legitimate message on the network and be actioned by the vehicle. Such a change could have devastating consequences, threatening the safety of not only the vehicle but the environment and infrastructure around it.

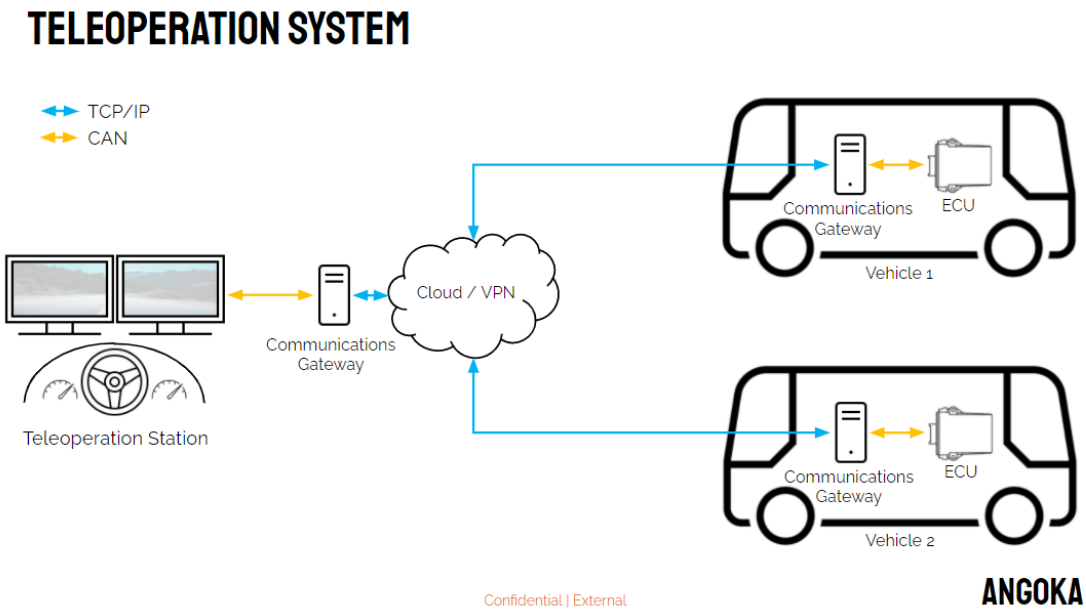


*Image 1: teleoperations systems*

ANGOKA's device authentication units (DAUs) were implemented to secure the communications channels and safeguard against potential cybersecurity threats. Deploying ANGOKA's DAUs at critical touchpoints of the teleoperation system and the vehicle network created a secure device private network (DPN). The DPN established a trusted network between the vehicles and the teleop station, regardless of the communication medium or communication infrastructure.

With ANGOKA's technology, trust is established through continuum authentication of the participating vehicles and teleop stations and their communications during an active teleoperation session. The immutable identities the DAUs generated dynamically for the DPN, and its participating vehicles and teleop station, ensured the DPN's advanced resilience against spoofing, man-in-the-middle and DoS attacks. Additionally, the DPN will report any malicious attempt to disrupt the vehicles or the teleoperation.

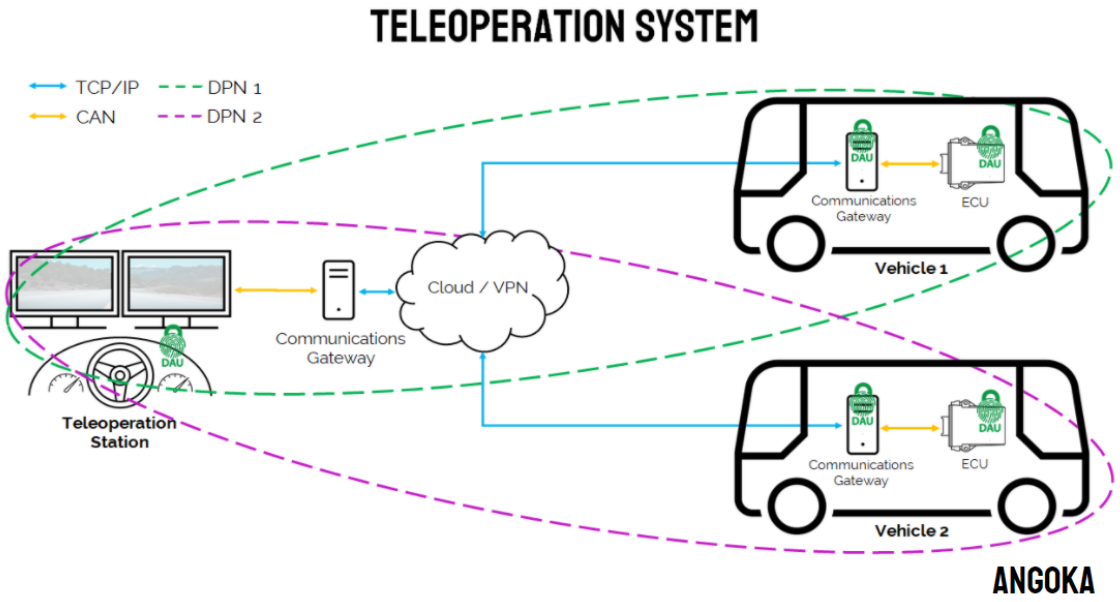


*Image 2: teleoperations systems embedded with ANGOKA solution*