

HISE Seminar Black Hat Session: Make an Autonomous UGV Dangerous

Rob Alexander

Goal of the Session

In this "black hat" session, we'll be trying to come up with as many ways as possible that an autonomous vehicle could be made dangerous, either by actors who are malicious, misguided or just plain lazy, or just by bad luck and unforeseeable error.

The session is scheduled for 90 minutes. We'll spend about 60 on brainstorming attacks, then 30 on how we might counter them (e.g. through safety processes or through cleverness of design).

The Scenario

The MOD is procuring a new unmanned ground vehicle (UGV) in Afghanistan. It is primarily intended to provide convoy protection (perhaps in a convoy where most vehicles are unmanned), but will end up doing other duties as well.

The System

The vehicle is an adapted Warrior IFV (Infantry Fighting Vehicle):



- **Weight:** 25.4 tonnes
- **Dimensions:** 6.3 m by 3.03 by 2.8 m high
- Can carry 3 crew and 7 passengers
- 30mm cannon and 7.62mm machine gun (co-axial)
- Operational range 410 miles, top speed 46mph
- Basically immune to ordinary small arms (need an RPG, large IED, or antitank mine to hurt it)

Our autonomous/UGV version adds the following features:

- Can follow prescribed route plan and adapt to damaged roads, enemy movements, and traffic jams. Or just plan its own route given a destination and key waypoints
- Can merge with traffic and obey local traffic rules
- Can merge with a convoy and take up an assigned position (e.g. first, last, "next to the command vehicle")
- Main gun has assisted and full-autonomy modes: these can be configured for a wide range of Rules of Engagement (ROE), composed from features including:
 - Entity type (e.g. "human", "Challenger II tank")
 - Explicit labelling (e.g. agreed UK markings, international ambulance markings)
 - One thing attacking/threatening another. e.g. an RPG threatens the UGV itself, a rifle threatens troops or civilians.
- Different safety behaviour depending on whether has humans onboard or not (e.g. if not, it will move to create a shield for infantry)
- Fallback full-manual mode – driver and gunner take their places as if vehicle is not autonomous at all.

As for design detail, that's up to you. Assume anything that's plausible (and feel free to consider several rival designs).

Attack Angles

Include, but aren't limited to

- Design of the vehicle
- Design of support equipment (e.g. remote commander station)
- Operating arrangements and mission plans
- Situations orchestrated in-theatre (perhaps paired with design vulnerabilities)

Personas

It may help you to put yourself in the shoes of one of the following, or use them as actors in your suggestions:

- A foreign agent (or domestic anarchist) who has managed to get a job with the prime or a subcontractor and is seeking to slow down the UK's autonomous vehicle programme
- A nominally loyal employee of prime who is lazy, embittered at mistreatment by his employer, or under huge pressure to cut costs
- A subcontractor looking for a quick sale of an impressive but immature new technology
- A member of the MOD project team who's recently moved there from the Army – he is an excellent soldier but has limited technical background and has had nothing but bad experiences with "safety people".