6.0 Risks and Mitigations

This chapter addresses actual and potential safety and security risks associated with operating autonomous AVs/GVs within the new ATS. OVER fully understands that safety and security is of paramount concern to government, industry, and the general public. As such, the risks of HW/SW malfunction, explosive device, SW "hack" and other risks were considered, and solutions proposed throughout the ATS design process. Solutions include reliable and redundant HW and SW systems, comprehensive and redundant emergency systems/procedures, and hyper-secure password login processes, to name a few. These risks will always be present, as with other forms of transportation, but can be mitigated to very low, acceptable levels. When considering these risks, and any other risks, the reader should weigh those risks and compare them to the risks associated with *existing aerial and ground transportation systems*, which operators and passengers currently subject themselves to everyday. The conclusion is that the actual and potential risks can be mitigated to very low, acceptable levels, and maintained at very low, acceptable levels perpetually, which will contribute to making the concept ATS the safest and most secure mode of transportation ever devised in human history.

6.1 Hardware Malfunction

Hardware malfunctions or failures are a risk to AVs/GVs and all other forms of transportation. The risk of injury or death is relatively small in an autonomous GV because the vehicle could just roll to a stop, with only a moderate potential of crashing, but the risk of injury or death in an AV is higher, because it could fall to the ground and crash. However, current traditional aircraft (especially single engine aircraft or helicopters) are at *greater* risk of crashing if their single engine fails. These single engine aircraft, which are considered "air worthy" by the FAA, are used every day, and the pilots and passengers accept those risks every time they lift off. However, the OVER concept AVs and other electric VTOLs (eVTOLs) have electric motors instead of internal combustion or jet engines, which significantly reduces the risks of engine/motor failure due to the inherent high reliability of electric motors, and because they have fewer mechanical and electrical parts/components. The OVER concept AVs have many redundant systems (power generation, motors, computers, sensors, communications, electronics, etc.) that also mitigate and significantly reduce the risk of crash. Further, the inherent flight capabilities of a "quadcopter" type vehicle is superior to traditional aircraft, even though some concepts have no fixed wings that provide lift and glide capabilities. Even if something does fail, like a motor, an OVER concept AV can land safely, with complete control of pitch, yaw, roll, and speed. These and other factors mitigate the risks of crash due to HW malfunction/failure to a very low, acceptable level – much lower than that of traditional single engine aircraft under human pilot control.

6.2 Ice Buildup

Ice buildup on propellers presents a grave risk to the concept AVs. Ice formation on a propeller blade, in effect, produces a distorted blade airfoil section that causes a loss in propeller efficiency. Generally, ice collects asymmetrically on a propeller blade and produces propeller unbalance and destructive vibration, and increases the weight of the blades[1]. The risk of injury or death in an AV is high, because excess ice buildup could cause the AV to descend quickly and crash. The risk is mitigated to an acceptable level by using an electric propeller icing control system, similar to

[1] https://www.aircraftsystemstech.com/p/propeller-auxiliarysystems-ice-control.html

those used in traditional propeller-driven aircraft. The system would have to be modified/ customized for the AVs, to make it completely automatic and autonomous.

6.3 Fire and Smoke

Fire and smoke can present a grave risk to AV/GV passengers, whether within the cabin, the front or rear nose cone compartments, or the motor placements. The risk of fire is reduced through the use of both passive and active systems.[2] For both AVs and GVs, passive methods include the use of noncombustible materials, separation by routing, compartmentalization (use of firewalls), isolation, proper ventilation and drainage. The active methods used in both AVs and GVs are smoke detectors which function as an autonomous fire detection system that will detect smoke within the cabin or utility compartments, as well as temperature sensors for each electric motor. In case of cabin fire/smoke, a portable hand-held fire extinguisher mounted within the AV and GV cabins would be used by a passenger to extinguish the fire. AVs and GVs both have smoke detectors in the front and rear nose cone compartments, but due to the low probability of occurrence, there are no fire extinguishing systems for the utility compartments or for the electric motors.

The probability of the occurrence of a fire in the utility compartments or at any of the electric motors is *very low*. When an AV or GV is compared to a traditional aircraft, car or truck, this becomes evident. Traditional aircraft and ground vehicles carry highly flammable, explosive fuels, but the concept AVs and GVs only carry non-flammable, non-explosive bi-ION fluids. There is virtually no "fuel" to burn, and therefore a very low risk of fire. Additionally, the temperature of each electric motor is constantly monitored, and if the temperature rises past a predetermined threshold, the AV would go into alarm, and would autonomously make an emergency landing or parking event. Further, an electric motor with an "over-temp" alarm will most likely be turned OFF, in both AVs and GVs, but in an AV, the "sister" motor at the opposite corner would also be turned OFF, to maintain control of yaw. Through the use of both passive and active systems, including SW for motor control, the risk of fire is mitigated to a *very low, acceptable level*.

6.4 Motor Runaway

In addition to motor failure, an AV or GV could experience motor runaway due to a short in the electrical system or motor windings, or in the case of an AV, due to a no-load situation such as a broken/missing propeller. In this situation, the speed of an AV/GV motor may be uncontrollable, and RPMs could increase to or beyond maximum limits. To mitigate such a situation, AVs and GVs will contain speed/current limiting devices (e.g. resettable circuit breakers) for each of the motor circuits (eight in an OVER concept AV and four in a GV). If either speed or current exceeds a predetermined threshold, the devices would autonomously "trip" OPEN, deactivating the motor circuit. When the voltage/current is removed from the motor winding, motor runaway will cease.

In an OVER concept AV, the motor control circuitry will also autonomously remove power from the "sister" motor on the opposite corner, turning in the opposite direction, to prevent the AV from spinning on the vertical axis. However, a consequence of these actions will be that both motors will continue to spin as a result of wind force on the propellers, since the concept vehicles contain fixed-pitch propellers with no feathering capability. After the above actions are complete, the AV will make an emergency landing. In a GV, when a speed/current limiting device (e.g. circuit

[2] https://aviation.stackexchange.com/questions/23135/how-does-a-fire-suppression-system-work

breaker) trips the circuit OPEN, voltage/current is removed from the motor winding and motor runaway will cease. The GV will make an emergency stop, as per GV operational protocols.

6.5 Explosive Device

An explosive device is another real risk to AVs, GVs and all other forms of transportation. The specific risk to AVs is two-fold: (1) that a suicide/homicide/terrorist-type bomber could board a PAV and detonate an explosive device upon landing or during the flight/trip, causing it to crash to the ground and possibly killing all; or (2) that an explosive device could be loaded on a CAV which would detonate upon landing or during flight, causing it to crash to the ground. However, either scenario could be more easily accomplished on a train, bus, taxi, or privately-owned vehicle. This risk is greatly mitigated with respect to commercial passenger/cargo aircraft, because the Transportation Security Administration (TSA) regularly inspects both persons and property prior to loading. However, such inspections do not take place for many other forms of transportation. Actually, the risk is compounded on a bus or taxi, because a homicide bomber could commandeer the vehicle, or make the driver drive to a highly populated area, where the explosion could cause even more deaths and damage to property. Similar risks exist with smaller traditional aircraft not subject to TSA screening, where an airplane is hijacked and made to fly into a highly populated area or building, similar to what happened on Sep. 11, 2001. Regardless, due to the TSA inspection procedures in place, the risk of an explosive device getting onto a commercial aircraft and then detonating is less than any form of ground transportation.

However, the OVER concept AV design and proposed ATS procedures will inherently provide safeguards against transporting suspicious persons and explosive cargo. Each passenger must request transport via iris scan identity authentication, and scan again upon boarding. If the person is wanted by law enforcement, or is on a terrorist/no-fly list, then the AV would not lift off with them aboard (depending on government policy). Additionally, AVs and GVs are not subject to hijacking because they fly/drive autonomously to the approved GPS destinations only, with no pilot/driver controls at all, so they cannot be commandeered. The concept AV and GV designs also incorporate sensors to detect explosive matter and radiation, as well as a hazardous gas sensor to detect excessive levels of oxygen (O2), hydrogen sulfide (H2S), carbon monoxide (CO), and lower explosive levels (LEL) for a variety of combustible gases. (*The exact gasses to be monitored are TBD*). An alarm from any of these sensors would prevent the AV/GV from departing, or would result in an emergency landing/stop if the alarm sounds during AV flight or GV trip. In all, the design and functionality of the concept AVs/GVs and proposed ATS protocols will mitigate the risk of explosive device detonation and excessive/hazardous gasses to low, acceptable levels – lower than virtually all other forms of ground transportation, and almost as low as traditional commercial aircraft.

6.6 Software Hack

Software hacks, to include sabotage, malware, reprogramming, over-clocking, unauthorized access to passwords, etc., etc. are perhaps the greatest risk to AVs and GVs. The primary risk is that a programmer/hacker can access the computer SW and add, change or delete programming, or add malware or other disruptive programs, where the AV/GV operation is compromised. Potential SW hack situations applicable to AVs and/or GVs include accessing the flight/drive control computer programming to:

- Commandeer one or more AVs/GVs, and crash them into an animate or inanimate object

- Commandeer one or more AVs, and make them fly around aimlessly, or stop and hover, until they run out of fuel and crash
- Commandeer one or more AVs, and fly them to another location, perhaps out over water where their power/fuel is depleted to the point that they cannot get back to a safe landing area
- Disapprove, ignore or corrupt AV/GV time-path requests
- Corrupt, revise or replace the MAP and/or the restricted airspace areas within the MAP
- Add multiple animate/inanimate objects to the MAP, which will cause AVs/GVs to avoid them, perhaps causing AVs to stop and hover indefinitely until they run out of fuel and crash.

Proposed mitigation efforts to prevent such hacks are many. Threats can be overcome by implementing high-security network communication protocols, using 2048-bit encryption; randomly generated, multi-character passwords for each and every AV/GV and GM Control transmission, and by implementing a new communications protocol (instead of TCP/IP). This new protocol could use a unique "packet" design/configuration that accommodates *all data* transmitted by AVs every 1-2 seconds during flight – into a single, variable length packet. (Routers and switches may be able to process the new "packets" with program modifications). Additionally, if necessary, the ATS could use communication protocols similar to those used by our government and military such as the Secret Internet Protocol Router Network (SIPRNET) used for "Secret" communications, or the Joint Worldwide Intelligence Communications System (JWICS) used for "Top Secret" communications. The American taxpayer paid to develop these protocols, and should be able to incorporate the technology into the ATS, if at all possible – without disclosing secret/top-secret HW/SW.

Further, all upgrades, revisions, changes, tests, etc. to the flight and drive control computer programming should be accomplished through a USB flash-drive (or the like), while on the ground, in a secure maintenance facility – not over a network. Only authorized technicians with appropriate background investigation and "clearance" may access the flash-drives, as well as the USB ports on the AVs/GVs, physically located within the covers and inaccessible to operators/passengers.

6.7 Bug Bounty Program

Another proposed mitigation effort to thwart malicious hacking is to use a "*Bug Bounty Program*"[3] similar to the approach taken by the Department of Defense (DoD), Google, Uber and others. An Air Force representative stated that "*bug bounty programs are an industry standard practice that helps better secure an organization's internet presence. These programs crowdsource sanctioned hackers to identify vulnerabilities within systems, which then allows the organization to quickly remedy those vulnerabilities*." The first two DoD bug bounty programs were "Hack the Pentagon" and "Hack the Army", where 138 and 118 security gaps were identified and resolved, respectively. The DoD's third bug bounty program "Hack the Air Force" was conducted in 2017, where 30 vulnerabilities on the service's networks were identified and resolved. The Air Force awarded the hackers who discovered the vulnerabilities more than $130,000 in prize money.

For the ATS, a bug bounty program could be used to seek out vulnerabilities not only during SW development, but perpetually thereafter. Its anticipated that the ATS SW would initially be used in a "test-range", where the SW would control prototypes initially, and then all newly

[3] https://fedtechmagazine.com/article/2017/11/teenage-hacker-gives-cybersecurity-advice-dod-and-other-agencies

manufactured AVs/GVs prior to commencing commercial operations. During the initial testing of both the SW and prototypes, and perpetually thereafter, monetary rewards could be offered to any sanctioned programmer/hacker, perhaps from anywhere in the world, who could gain access to the test-range network, SW program or MAP, and/or commandeer one or more AVs/GVs. Monetary rewards could be offered to those who identify security gaps, such as $25,000 to gain access to the SW, $50,000 to commandeer a single AV/GV, and $100,000 to commandeer all AVs or GVs. In addition to the monetary reward, hackers would gain public notoriety (award), and possibly offered full-time employment with the JVLLC, SLLCs, or other manufacturers.

Such a perpetual financial/reward program would create a huge group of expert sanctioned programmers/hackers who would continually seek out any vulnerabilities for both recognition and reward. All such revealed vulnerabilities would be resolved/blocked by JVLLC employees, one by one, to prevent reoccurrence. The identified threats would be patched/resolved in the test range HW/SW, and then applied to the final operational ATS HW/SW, resulting in a very secure final operating system. Any attempt to gain access to the real-world ATS HW/SW which controls real-world AV/GV operations would be illegal, investigated by law enforcement, and prosecuted to the fullest extent of the law. (*Note: The two separate HW/SW systems, one for the test range and one for commercial operations, would be operated and maintained perpetually*).

The idea here is that most programmers/hackers would not want to deliberately crash operational AVs/GVs, or the operational ATS, which their friends and family will use. To the contrary, most programmers/hackers would welcome the monetary reward and notoriety for identifying and helping to resolve any vulnerabilities, and thereby thwart any “real-world” efforts that terrorist-type programmers/hackers may use.

The JVLLC test range would evolve from testing prototypes, to testing/proving newly manufactured or repaired AVs/GVs prior to entering/reentering operations. SLLC test ranges would only test/prove newly manufactured or repaired AVs/GVs prior to entering/reentering operations in their areas of operation. Each vehicle would be tested/proven in a test range for at least 24 continual hours after being manufactured or repaired, subjecting each AV/GV to a comprehensive array of standard flight/trip scenarios and emergency situations. These tests would be conducted using the test range network HW/SW – completely separate from the real-world operational ATS. Only after successful completion of all tests would an AV/GV enter real-world ATS operations, on the real-world network. Test range operations would continue, 24x7x365, perpetually.