

Secure AI Race Strategy (SARS)

Ashley Francis, Reinaldo Contreras, Jamahl Davis, Erik Pereda, Santiago Vargas

Florida International University

CIS 4951 - Capstone II

Masoud Sadjadi

December 5, 2025

Table of Contents

Table of Contents	2
I. Abstract	2
II. Introduction and Project Design	4
III. Risk Assessment	7
IV. Incident Response Plan	10
V. Conclusion	13
VI. References	15

I. Abstract

With a growing dependence on artificial intelligence, our project has decided to implement a race strategy model and demonstrate the need for vehicle security, specifically in the context of racing. This project presents both the design and implementation of an Artificial Intelligence Race Strategist model that has been enhanced with spoofing protection to prevent the possibility of dangerous injection attempts, equipping the model with reliable race decision support. Using telemetry data from the 2022 Formula 1 season, tracking both drivers from the McLaren team which are Daniel Ricciardo and Lando Norris. From here, the race strategist model would assist in the basics, assisting in pit stop maneuvers to know what tyres should be swapped out based on the weather conditions and wear-and-tear of the racecar. Afterwards, our model was equipped with an interactive spoofing detection, where users can engage with the model and inject it with evidently impossible numbers. The spoofing protection would kick in and briefly swap out the data before continuing as normal once it has detected out of bound numbers.

This model is meant to emphasise the growing need for vehicle security, especially as technology becomes more integrated in these sectors. Specifically with racing, a simple attack can brutally interfere with a driver's performance and safety, injecting values that are not real or feeding the data, sabotaging metrics. Beyond racing, this model would work brilliantly in common day commutes. Drivers could experience these same attacks at some point and would be in more danger as they can injure a greater number than those on the race track, take for instance, the Florida Turnpike, where "more than 3 million customers" utilize this major roadway as reported in 2024 (Florida Department of Transportation, 2024). Imagine the horrendous damage a simple vehicle spoofing attack can trigger, a chain reaction of catastrophic

events. In our project's intended environment, race engineering tools should be developed under new security guidelines, ensuring they are ready to prevent and mitigate these manipulation threats.

The integrated graphical user interface also serves as an educational platform, allowing users to visualize the attack attempts and how it is mitigated in a controlled environment. While it may seem a simple attack, please note these metrics would usually be displayed on the dashboard of a racecar. Spoofing attacks can contribute to physical damage beyond an annoyance, in which it may under/overreport temperatures, speed, or even oil pressure which can be the perfect disaster not to trigger the vehicle's safety measures. This leads to a string of other issues such as loss of thermal protection, miscalculated fuel flow, or even brake failure. All of which can potentially harm the driver and their fellow racers on the track. Spoofing has the ability to do both, delay safety measures or even kick them in unnecessarily.

II. Introduction and Project Design

In the world of Formula One racing, one of the more important tasks is the one of a race strategist engineer, which is to plan out the most optimal way to finish a particular Formula 1 race based on many factors, such as race weather, types of tyres, what other teams are doing in real time, current tyre wear, position of race, to be able to determine factors like what speed to travel, when to go the pit stops, as well as taking into account when any critical situations may occur, constantly in communication with the drivers on the teams when any real time decisions are made, based on data both gathered before and during a race (Astron Martin F1, 2023). When position finish times are as close as the ones in Formula 1, where finish times between two positions can be less than a second, like the finish times of Max Verstappen and Charles Leclerc at the Saudi Arabian Grand Prix in the 2022 Formula 1 season, with first and second being half a second apart, every strategy to shave off those fractions of a second is absolutely pertinent to be able to maximize the amount of points scored not just every race, but cumulatively. (Formula 1, 2022).

Through Machine Learning and Artificial Intelligence, a race strategist model, like the one that we are implementing for our project, can allow for more efficiency in making more informed decisions when communicating with the Formula 1 team drivers information like pit stop maneuvers as well as which type of tyres to use based on real time telemetry data communicated from the vehicles from the driver, such as current , already being trained and fine tuned using telemetry data from previous Formula 1 races during the season.

However, being in possession of not only real time telemetry data from Formula 1 cars, which are going at an average of 230 miles per hour, or 370 kilometres per hour, pushing themselves along with the forces of nature as they maneuver the high speeds of each the turns

and terrain changes between each race, but also having the power to directly influence what decisions an F1 driver ultimately takes, such as which tyres to use, speed, when to fuel and change tyres, angles at which to take turns, and more, can pose a major security risk, due to factors like spoofing telemetry data, manipulating data in which AI strategist uses, as well as compromising the actual communication that is maintained with the actual sensors of the car and the race strategy engineer (F1, 2025). For example, modern vehicles, which rely on a multitude of sensors in order to not only provide comfortable user experience but fulfill in carrying out basic functions and major features of a vehicle. For example, vehicles with capabilities of full autonomy, like those manufactured by Tesla Motors or self-driving taxis like the ones provided by Alphabet Inc. Subsidiary Waymo rely on key sensors like cameras and global positioning system (GPS) as well as Artificial Intelligence algorithms to be able to not only find the optimal route to get to a destination, but to also ensure the safety of not only the passengers, but surrounding drivers and pedestrians, by following all road laws, safety / speed limit signs, and keeping a safe distance between neighboring vehicles, and always yielding (Tesla, 2025).

When the AI system tells the car to make a certain decision that may appear wrong, whether it is because the sensors have read false data that the AI believed to be true, the sensors may be broken or not having communication or because the AI is making mistakes, it could lead to damages to not only the vehicle, the passengers, as well as surroundings, ranging from minor to catastrophic, such as when a Tesla Model Y running its full self-driving feature directly rear-ended another vehicle at a high speed, due to poor camera readings due to the sun's strong glare, leading to a unintentional and undeserved fatal casualty as a result (Anon, 2025). This same level of risks can affect Formula 1 drivers in the same way, because if tyre, fuel, speed, weather, oil pressure, temperature data are misleading due to different factors, any wrong move

by the driver or any false reading can cause catastrophic impacts, to not just the driver themselves, but the surrounding drivers (Hull & Trudell, 2025).

In order to bring awareness to mitigate potential security risks that can arise from the direct communication between the race strategist and the Formula 1 driver on the wheel, this capstone project focused on providing a simulation of spoofing telemetry data, as well as implementing an interactive spoofing detection protection method, which can identify poor or misleading data, and swap the data to continue as normal, simulating a scenario similar to what would actually occur in a real Formula 1 race, in the same position that typical race strategist engineer would be in. The data that was used to train the Large Language Model (LLM) used was from the 2022 Formula 1 racing season, from the McLaren racing team.

III. Risk Assessment

The safety of the pilot and the vehicle will always be in great danger due to the poisoning of false data. Today's vehicles rely heavily on wireless telemetry, Bluetooth sensor connectivity, and real-time AI-recommended strategies.

Spoofing attacks generate incorrect information and readings such as speed, tire temperature, brake pressure, engine problems, and also send falsified values to engineers and AI systems. In motorsports such as Formula 1, these types of attacks are very dangerous because the cars travel so fast that a small detail can cause significant damage to either the driver or the vehicle. It is recommended that drivers accelerate only when the tires can no longer keep up.

Risk Matrix		Severity				
		Negligible	Minor	Moderate	Major	Catastrophic
Probability	Frequent					
	Likely					R6
	Moderate			R5,R7	R3	R4
	Unlikely					R1, R2
	Very Unlikely					

ID	Date	Description of Risk	Probability	Impact	Severity	Mitigation
	Raised		(1–5)	(1–5)		

Secure AI Race Strategy

R1	12/2/25	Bluetooth spoofing producing incorrect information such as speed	4	5	20	-Encrypted Bluetooth -MAC filtering -Anomaly detection - Short pairing windows
R2	12/2/25	The AI model receives incorrect information during the race, such as engine statistics and tire temperature.	4	5	20	-AI anomaly detection -Zero-trust access -Validation of data ranges
R3	12/2/25	False odometer readings can request pit stops or make them longer.	3	4	12	-Threshold validation -Cross-check with secondary sensors
R4	12/2/25	Recommendations manipulated by attackers, harming the career strategist algorithm	3	5	15	-Secure storage -RBAC -Version control
R5	12/2/25	Wireless interference or forced connections.	3	3	9	-Redundant communication channels -Pre-race wireless integrity checks

R6	12/2/25	Delayed safety flags and fake overheating alerts.	2	5	10	-Multi-source telemetry verification -Real-time sanity checks
R7	12/2/25	Delayed patching puts the algorithm and telemetry at risk.	3	3	9	-Patch schedule enforcement -Automated updates -Integrity monitoring.

IV. Incident Response Plan

The incident response plan outlines the procedures for detecting, defense, recovery, and prevention should anything go wrong. In this specific context, if the injections actually make it through to the AI system or if there is a compromise somewhere along the system. This might even be something such as a wireless attack where all the systems of the AI would be greatly sabotaged and undergo a complicated recovery as the race could not be easily stopped to account for these types of situations since they are a use-at-your-own-risk situation. The important problems that should raise a concern are as follows;

- Bluetooth spoofing
- Telemetry falsification
- AI strategy manipulation
- Data poisoning
- Wireless connection hijacking

These incidents should be immediately identified with the appropriate measures be implemented but do note these attacks only make up a portion of what one can anticipate happening. In any case, the foundational procedure should entail of detailed documentation, noting the exact date, time, involved systems, individuals, and anything else that may be relevant in the report so the security team can perform a complete trace and audit to pinpoint exactly where things all went wrong. After completing so, please follow the outlined lifecycle plan implemented.

A. Identification

- Impossible value changes like speed from 54 mph to 390 mph in a matter of seconds.
- AI model flags injected values as out-of-bound.
- Telemetry misalignment between car sensors and pit data.
- Bluetooth pairing request from an unknown MAC address.
- Engineer dashboards showing discrepancies between redundant sensors.
- Race strategy is extreme or something like mathematically inconsistent decisions.
- AI anomaly detection logs the incident.
- The engineer manually validates values using fallback dashboards.
- Connection integrity is checked for spoofing signatures.

B. Containment

1. Immediately terminate the compromised Bluetooth session.
2. Radio driver to pull in for an emergency pit stop.
3. Switch telemetry to a secondary encrypted channel.
4. Freeze AI strategist outputs until values stabilize.
5. Lock system access to strategy commands.

Secure AI Race Strategy

- Disable previously paired Bluetooth keys.
- Regenerate encryption keys for race telemetry.
- Block spoofing MAC addresses and frequency signatures.
- Enable strict pairing window.
- Implement zero-trust validation for all incoming telemetry.

C. Elimination

- Perform scans of telemetry pipeline for altered firmware.
- Remove malicious configurations or spoof-injected datasets.
- Delete corrupted AI data if contamination is detected.
- Reset all Bluetooth in the car and pit equipment.

D. Recovery

- Establish secure telemetry channels.
- Enable AI strategist only after the incident is solved.
- Test all sensors like:
 - Speed
 - Tire temp
 - Engine temperature
 - Brake pressure
- Reconnect wireless using new authentication keys.
- Track the car only after engineers confirm safe operation.

E. Lessons Learned

- Develop new detection rules from attack data.
- Provide engineers with playback visualization of spoofing attempts.

Secure AI Race Strategy

- Update algorithm thresholds and anomaly detection to identify subtle attacks.
- Patch any exploited vulnerabilities.
- Document the entire event within team logs
- Post-race analysis reports.
- Integrate attack signatures into future simulations for training.

Creating a detailed report like this can help mitigate what went wrong so that prevention methods are created more efficiently, adapting to sophisticated attacks (which will only become worse as time goes on). At some point in the compromise, reverting to older versions of systems where it was not so readily available by the click of a figure might be in the best interest of a security posture. For instance, there will definitely be a large bandwidth available between the drivers and where the race engineers are stationed, so that is a large attack vector hackers might see that as. Brainstorming a solution that maybe only updates the engineers position each time they pass close would be more secure, but does slow down the suggestion phase on the engineers' behalf and defeats the whole purpose of the model. It is all a learning phase.

V. Conclusion

After the development of Secure AI Race Strategy (SARS) model, we believe to have demonstrated the potential of an artificial intelligence-driven race strategy model that was secured through our spoofing protection model. This process highlighted the importance of protecting systems across attacks as simple as data manipulation, specifically spoofing attacks. The use of historical data from the 2022 season in order to create our model solidified the outcomes the race strategy model produced as it ensured the model had realistic values to go off of and was trained on what to expected within the Formula 1 environment. While our model did not predict intricate things, the basics like tyre swaps and pitstops were sufficient to at least create a strategy of pitstop timing from that, combined with the weather conditions at the time.

The interactive graphical interface allows users to see the attacks for themselves, providing that our AI model stays afloat and does not suggest strategy or changes based off the inputted data. This was seen in our demonstration video. Even beyond the racetrack, the implications of this work can be applied to the common day vehicles where nearly 75% of vehicles utilize some type of technology that can be tinkered with if the right tools are nearby. This project represents a foundational step towards a balanced duo of security and AI powered solutions, the growing emphasis to highlight additional research on what these models are capable of and can be suspect to is imperative to ensuring success.

In the future, it would be greatly beneficial to include protection models for all possible cyberattacks to harden our security systems. This would be great as it would provide a peaceful state of mind to everyone on and off the track, the impact of these systems extends beyond the track but if anything happens would be the governing bodies (in this case, Fédération Internationale de l'Automobile), the devastated teams, and more importantly, the families that

Secure AI Race Strategy

lost a talented loved one. Creating these systems is more than just about making them more efficient, safety will always remain a number one priority in anything that is ever created and we should never lose sight of that.

VI. References

Aston Martin F1. (2023, July 9). *Aston Martin F1 Team*. Astonmartinf1.com.

<https://www.astonmartinf1.com/en-GB/news/feature/so-you-want-to-be-an-f1-strategy-engineer>

F1 - The Official Home of Formula 1® Racing. (2022). Formula 1® - the Official F1® Website.

<https://www.formula1.com/en/results/2022/races/1125/saudi-arabia/race-result>

Florida Department of Transportation. (2024 6). *2024 Fiscal Year System TEAR Combined*.

Florida's Turnpike System; FDOT.

https://floridasturnpike.com/wp-content/uploads/2025/02/~2024_System%20TEAR%20Combined_F3.pdf

Formula 1. (2025). *Everything You Need to Know about F1*. Formula 1.

<https://www.formula1.com/en/latest/article/drivers-teams-cars-circuits-and-more-everything-you-need-to-know-about.7iQfL3Rivf1comz dqV5jwc>

GPS-IDS: An Anomaly-based GPS Spoofing Attack Detection Framework for Autonomous

Vehicles. (2025). Arxiv.org. <https://arxiv.org/html/2405.08359v2>

Hull, D., & Trudell, C. (2025, June 4). *Musk Touts Austin Robotaxis, But Tesla Crash Shows*

FSD Limits. Bloomberg.com; Bloomberg.

<https://www.bloomberg.com/features/2025-tesla-full-self-driving-crash/>

Tesla. (2025). *Full Self-Driving (Supervised) | Tesla*. Tesla. <https://www.tesla.com/fsd>