**Security Concerns for the**

**Pedestrian Backup Assist System (PBAS)**

**Authors: Glen Simon, AKM Tauhidul Islam, Nick Polanco, Emily Ribando-Gros**

**Instructor: Dr. Betty H.C. Cheng**

# **Introduction**

The PBAS system has two major areas where security needs to be addressed. The first is to secure the Controller Area Network (CAN) bus, where communication is being sent and commands are being issued. If the CAN is compromised all control of the vehicle may be lost as in [1]. The next are the physical sensors around the car, this is the source of all the information and if tampered with could cause danger to the driver or pedestrians passing by.

# **2. Security Concerns**

This section describes the security concerns of the proposed PBAS system. The PBAS system depends on the correctness of the data from the sensors and the integrity of the signals among different controllers of its components. Hence, it is critical to protect the system from any malicious attack. In order to do that we first identify specific threats and assets relevant to a threat. Then, we conduct risk assessment, determine how to identify an attack and the subsequent mitigation measures.

# 2.1. Contactless Attacks on PBAS Sensors

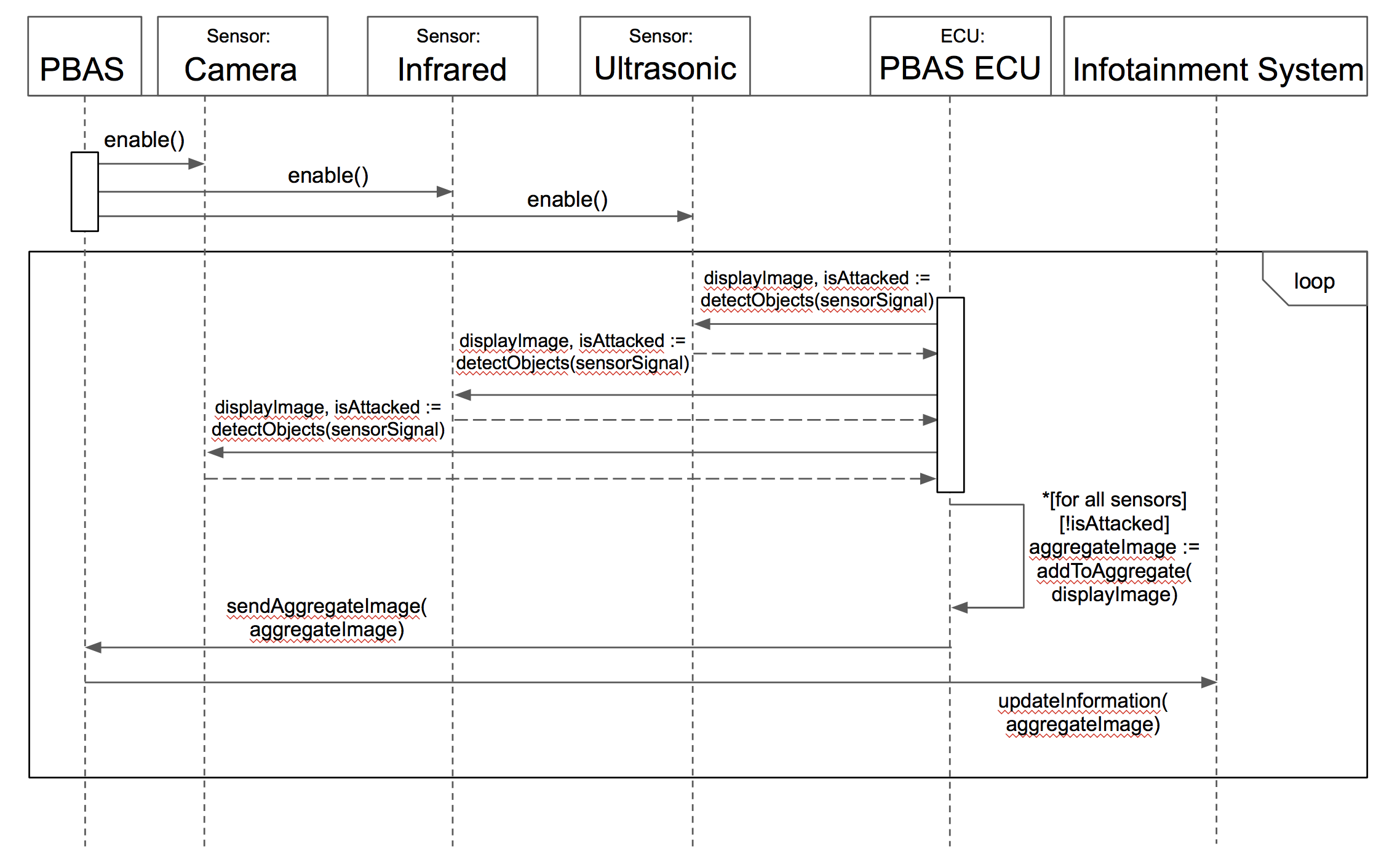
The PBAS is reliant on the accuracy of the data it receives from its many sensors. In particular, sensor signals are processed to detect obstacles and the distance from the rear of the vehicle, acting as the ‘eyes’ of the system. If the sensors are tricked or altered in any way, the system is likely to fail in obstacle avoidance. As detailed in [2], sensors can be jammed, spoofed, or quieted. Jamming is an attack method which renders the sensor useless, giving the system no useful information. On the other hand, a spoofing attack could trick the sensor into seeing an obstacle which is not in fact present or altering the distance information of an obstacle. Lastly, quieting attacks can mask obstacles so they appear as if nothing is in the way. In all of these cases, the system can exhibit undesirable behavior which could lead to loss of life.

These attacks are carried out by injecting fake signals to the sensors through sound or light and in most cases only shut down the object detection system temporarily. Though these attacks may not cause any damage to the tangible assets of the system, they may endanger the safety of pedestrians and drivers in backup collisions. As for the feasibility of these attacks, these fake signals are produced by large pieces of equipment that must be in the short range of the sensors and have a high threshold of knowledge to operate. Because of these constraints, the attacker must be close to the sensors, requiring some stealth perhaps previous knowledge of the vehicle, thus making it more difficult and less successful for the attacker. However, in the case that cameras are exposed to a laser beam, parts of the cameras, particularly the CCD (charge-coupled device) and CMOS (complementary metal-oxide semiconductor) image sensors, may suffer permanent damage causing object recognition to cease indefinitely [2].

* 1. Assets
     1. Tangibles
        1. Rear-view camera and Infrared camera
        2. Ultrasonic sensors
        3. Infotainment system
     2. Intangibles
        1. Pedestrian safety
        2. Driver safety and liability
        3. Financial loss of the driver
  2. Threats
     1. Jamming
     2. Spoofing
     3. Quieting
  3. Risk
     1. When the cameras are exposed to a laser beam, parts of the cameras, particularly the CCD (charge-coupled device) and CMOS (complementary metal-oxide semiconductor) image sensors, may suffer permanent damage causing object recognition to cease indefinitely [2, Section 7.2.2].
     2. Pointing LEDs and laser beams at the camera will result in temporary blindness rendering the object recognition system useless in that time [2, Section 7.2.2].
     3. For an ultrasonic sensor, if some device generates the right ultrasound frequency it could render the sensor useless or detect fake obstacles. In addition, using some acoustic noise cancellation could quiet the signal of an object. In these cases, the ultrasonic sensor may stop the car for no reason or run in to an obstacle, perhaps even a pedestrian. This last risk can create a huge liability for the system or driver in case of a lawsuit.
  4. Detection
     1. Our object detection system should be trained to identify a jam. For example, if the camera is flooded with a bright light, led, or laser, even in the case of glare from the sun, the system should detect a sensor attack.
  5. Mitigation
     1. The main way to mitigate any of these potential threats is to have many sensors so that if one is jammed or quieted, the others may compensate for its failure.
     2. The system will display a warning to the driver to be aware of their surroundings and environment when the system is activated.
     3. In order to protect the sensors from attack, the smallest sensors should be used without sacrificing quality. Additionally, the presence of a sensor should be difficult to detect by an attacker without previous knowledge of the vehicle. (Camo sensors?)
     4. In the case that a sensor is spoofed and the car is stopped, the driver can confirm the spoof through visual inspection and proceed in the override mode of the system, ignoring false warnings.
     5. If a camera jam has been detected, sensory information is no longer used from the camera until the input is restored. Additionally, the driver is warned via the Infotainment System that the camera is experiencing low visibility and should proceed with caution.

# 2.1.1. Contactless Attacks Scenario

The attacks described in this section can be difficult to detect because they mimic the inner workings of the system. However, in the case of jamming, object detection can be trained to label an attack. For example, if a laser beam is directed into the camera, the feed will show a bright light covering almost every pixel. For this reason, jamming can be protected against. In particular, when the object detection system is called on each sensor’s signal a value will be returned notifying of an attack. If an attack has been detected, the sensor signal will not be trusted and is thus discarded when displaying information to the user. If the rear view camera has been jammed, only the infrared camera will be shown on the dash along with ultrasonic sensor distance information. Below is the figure describing how the system checks and protects against jamming attacks of sensors.

Figure 1: Contactless attack scenario via modification of sensor data

# 2.2. Hacking of PBAS

Hackers may send fabricated or modified signals directly to the ECUs of a component of the PBAS system. One way to carry out such an attack is to access the CAN bus remotely via a network connection as in [1]. Another way is to plug in a media device, such as a USB, to the vehicle’s entertainment system which may contain malicious files. In both cases, attackers are able to send fabricated signals to different ECUs of the vehicle, especially the ones included in the PBAS. In order to prevent these attacks, an authentication process as well as an authorized access filter should be implemented.

* 1. Assets
     1. Tangibles
        1. CAN bus ECUs
        2. Sensors and cameras
        3. Infotainment system
        4. Actuators
     2. Intangibles
        1. Pedestrian safety
        2. Driver safety and liability
        3. Financial loss of the driver
  2. Threats
     1. Hacking into the CAN bus remotely
     2. Trojan horse/virus through a media device
  3. Risk
     1. When a vehicle is hacked remotely, its control is compromised. For example, the hackers may have the option to kill the vehicle’s braking capabilities. In that case, if the PBAS senses an obstacle and sends a message to activate the brakes, this message may be intercepted. Then, the vehicle will not brake and may collide with the obstacle.
     2. In addition, there might be a ransomware attack. The hackers may deactivate acceleration of a vehicle and demand a certain amount of money to release the control of the accelerator component.
     3. If has malware entered the system via a media device or remote access, it can launch a DoS attack so that different components of the PBAS are not responsive for an indefinite period of time.
  4. Detection
     1. In order to protect from a malicious command or message from unauthorized remote access, there should an authentication check for each incoming message into the PBAS ECU. The PBAS ECU subsequently forwards only the authenticated messages to different components of the PBAS.
     2. In order to protect from an unauthorized access from an irrelevant component of the system, there should be some compartmentalization among the components of the system.
  5. Mitigation
     1. If a command or message fails to pass the authentication check, it will be discarded.
     2. If a command or message comes from an irrelevant component of the system, it will be discarded.

# 2.2.1. Hacking of PBAS Scenario

Figure 2 shows the scenario where a hacker remotely accesses the system and attempts to send a fake signal to change the actions of the PBAS. The signal is denied because the hacker fails to satisfy the authentication check.

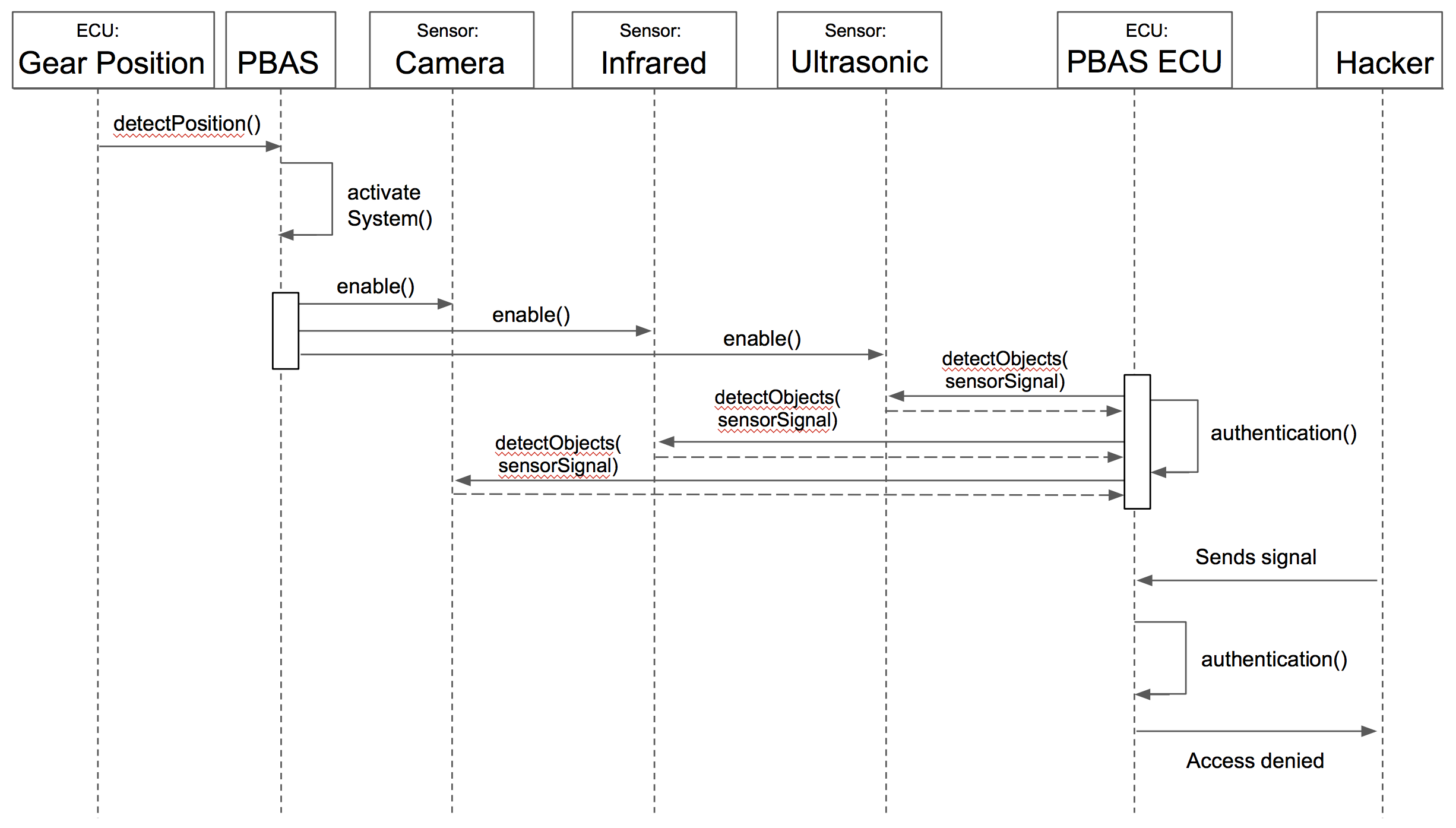


Figure 2: Attempt of unauthorized remote access into the PBAS ECU

Figure 3 shows the scenario where an attack is carried out through an infected file on a media device. In this case, the driver plugs-in a media device to the media center. The infected file accesses the infotainment system display and then sends a signal to the PBAS ECU. However, the infotainment display is not supposed to send such signals. Hence, the unauthorized access request is denied.

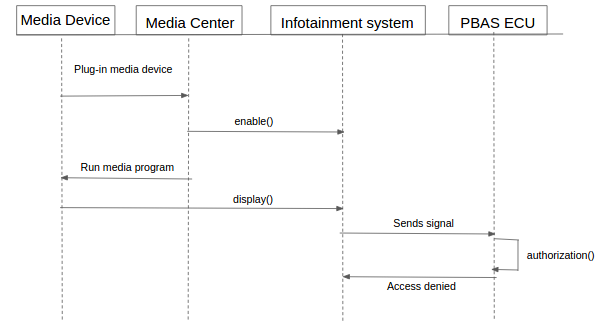


Figure 3: Attempt of unauthorized access into the PBAS through media component

# 

# **3. Goal Model**

This section describes the goal and obstacle models for the PBAS. A goal model is a hierarchical arrangement of goals or objectives for the system. The main purpose of a goal model is to demonstrate the relationships between goals and provide a realization of how the requirements can be modeled and quantified within the system. An obstacle model, is a refinement of the goal model to show how specific security concerns could impact the achievement of certain goals within the system, thus hindering some of the system functionality.

For the PBAS, the top priority goal is to prevent backup rollover accidents, as can be seen in goal (A). This goal is further decomposed into two main branches, providing warnings and the activation of the system. While the system is active, IE the override function is not engaged, the system will both limit the throttle speed and perform accident mitigation. Specifics for how these functionalities are performed are defined in more granularity as the levels of the goal model are descended.

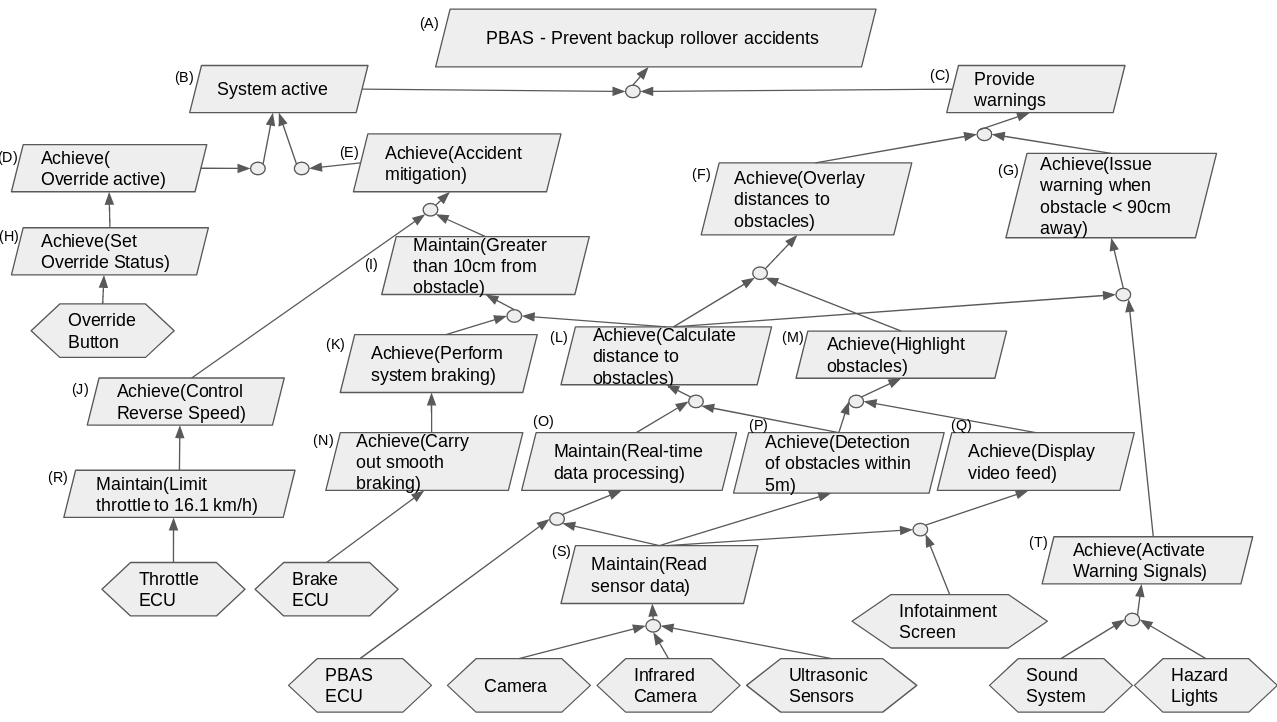


Figure 4: PBAS KAOS goal model

3.1 Obstacle Models

This section covers two possible obstacle models for the PBAS, which relate to the security concerns described in the previous sections. Obstacle models help pinpoint weaknesses in the designed system and can be used to create a refined goal model that is strengthen against the defined security concerns.

3.1.1 Obstacle Model for Contactless Attacks on PBAS Sensors

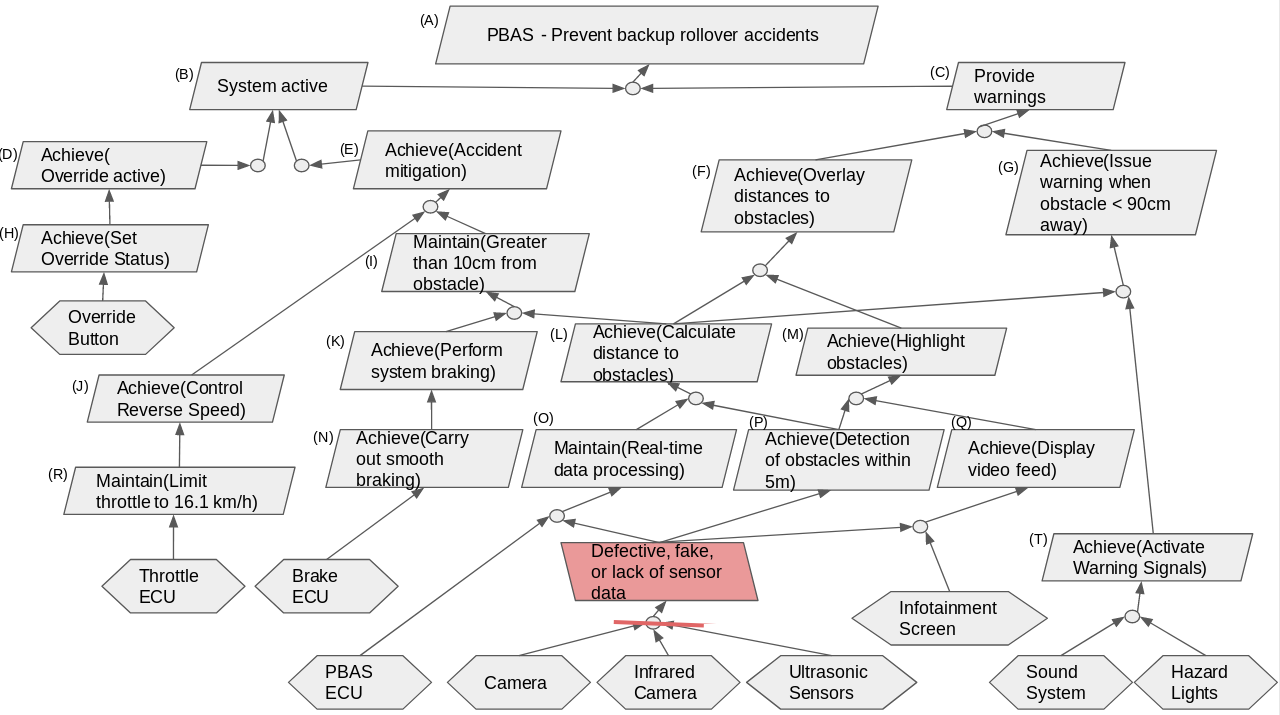


Figure 5: PBAS KAOS obstacle model showing a possible weak point to contactless attacks on PBAS sensors

3.1.2 Obstacle Model for Hacking of PBAS

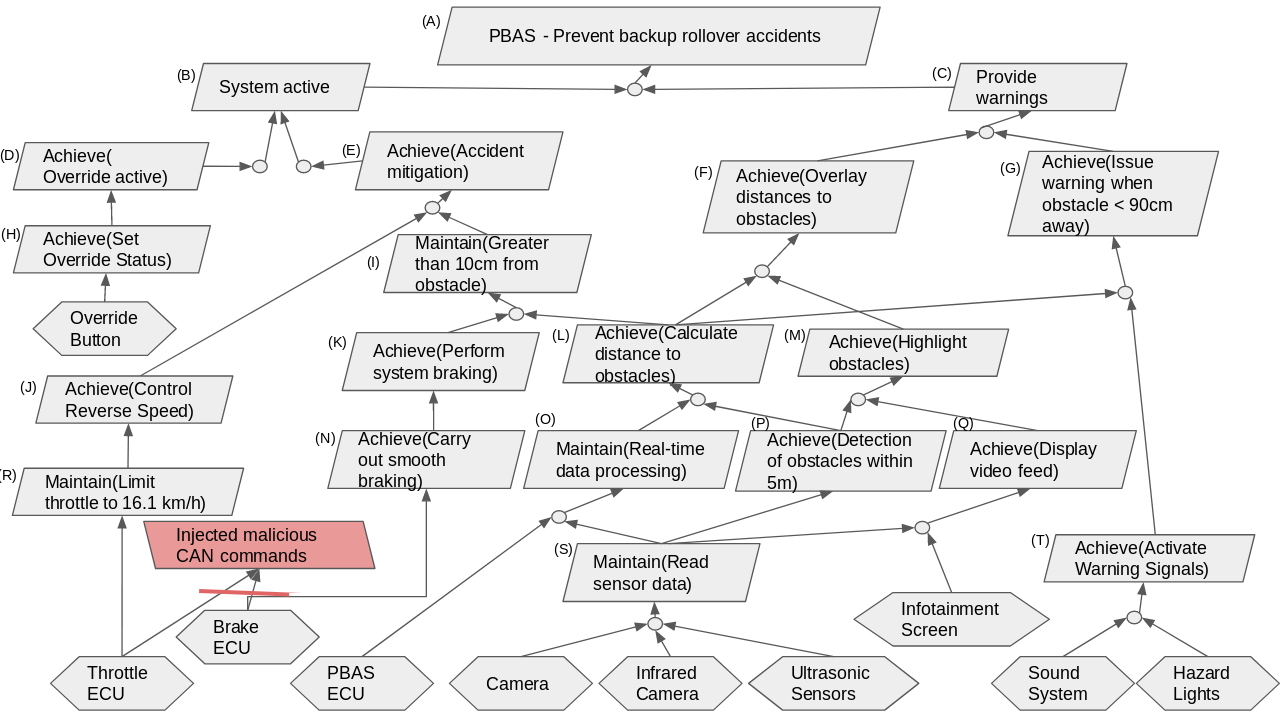
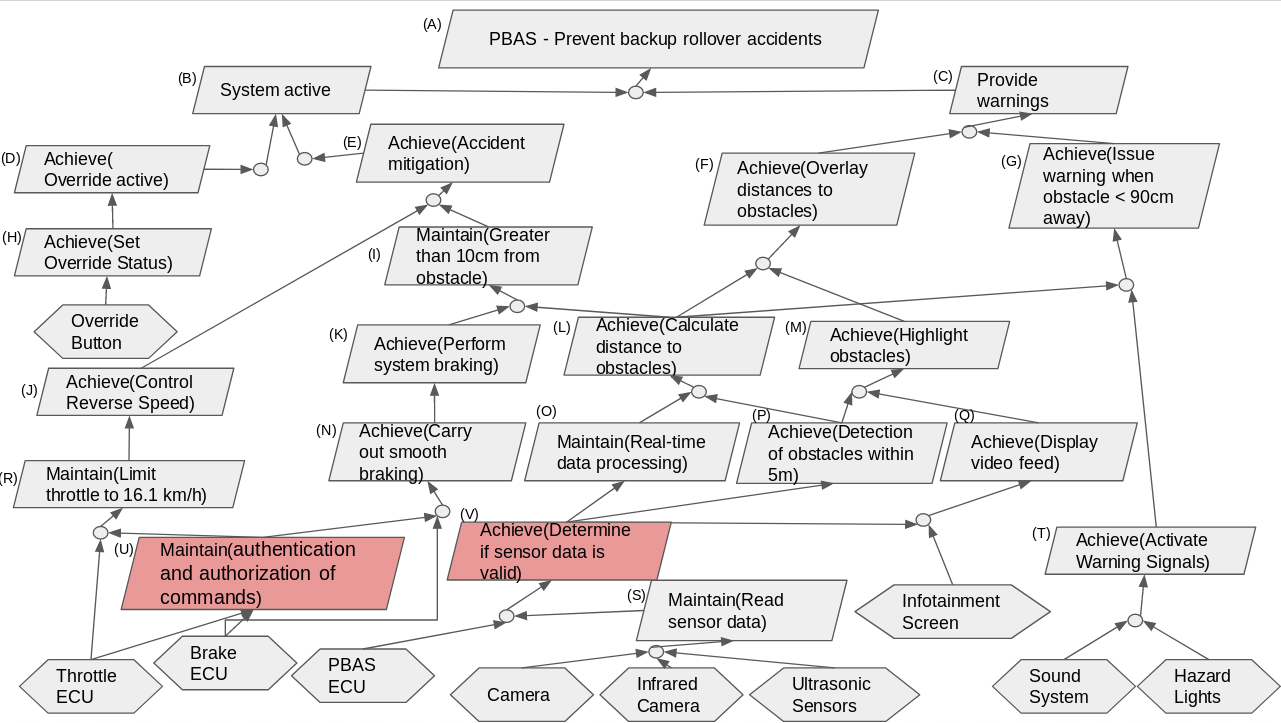


Figure 6: PBAS KAOS obstacle model showing a possible weak point to hacking of the PBAS

3.2 Refined Goal Model to Accommodate Security Concerns

Once security concerns are identified and defined for the system and their corresponding obstacle models are created, a refinement to the original system’s goal model can be made to strengthen it against these security concerns. Below is a refined goal model for the PBAS to better handle both contactless attacks on PBAS sensors and hacking of the PBAS.

Figure 7: PBAS updated KAOS goal model refined to handle security concerns

# **4. Security Policies**

The policies of the PBAS system aim to cover both the the threats to pedestrians’ and drivers’ safety. Since the system is designed to avoid backup collisions, the collision avoidance policy is treated separately from the vehicle security policy. Furthermore, the vehicle security policy details the intolerance to ‘hacking’ of the system.

4.1. Collision Avoidance Policy

The PBAS is responsible for assisting drivers while backing up a vehicle. The system should be developed with the current best practices in software engineering, object detection, and real-time systems to ensure the driver is supplied with all needed information quickly while backing up. The developers of this system are responsible for ensuring the behavior of the system is consistent with the requirements outlined in the Software Requirements Specification document. The mitigative features will only be active in the case of a perceived future collision by the system and the override is not currently enabled. Furthermore, the features of the system should never be interrupted when active. Specifically, the hardware components of the system should be supplied with protective gear to exhibit resilience to extreme circumstances.

4.2. Vehicle Security Policy

The services of the PBAS are only accessible or modifiable by the system internally or the developers or manufacturers of the system. The information contained in the PBAS should never be accessed, modified, fabricated, or interrupted by a party other than the developers or manufacturers. Information of the system will only be accessed in case of an update or investigation by only the developers or manufacturers. Communication with the ECUs of the system will be secure and minimal in regard to the features of the system.

# **5. References**

[1] “Hackers Remotely Kill a Jeep on the Highway - With Me in It,” Andy Greenberg, Wired, July 21, 2015.

[2] “Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle,” Chen Yan, Wenyuan Xu, and Jianhao Liu, 2016.