**Resilient Control System Assurance Specifications for LandShark Platform**

**Part A: Resilient Control System Description**

**Part B: Assumptions on Platform**

**Part C: Assumptions on Environment**

**Part D: Guarantees Provided**

**PART A : Resilient Control System Description**

The resilient cruise controller node developed by the University of Pennsylvania uses measurements from 3 sensors (left encoder, right encoder, and GPS), and controls the actuators to reach and maintain a desired reference speed, even in the event of a malicious attack that compromises one of the sensors. The controller consists of an attack-resilient state estimator, which is used to evaluate the speed of the vehicle, and a standard PID controller that utilizes the difference of the desired and actual vehicle speed to provide appropriate command inputs.

**1) General Architecture**

- Resilient state estimator (RSE)

- model-based L1/L2 approach to resilient state estimation;

- it assumes a known model and sampling rate.

- Quadratic programming implementation;

- iterative interior-point search;

- bounded execution time.

- Controller

- PID controller;

- tuned for a constant sampling rate,

- low-gain control approach.

**2) Code generation / ROS integration**

- C++ PID controller and RSE wrapper generated via Simulink Coder;

- C-based RSE generated via CVXGEN;

- Integration of code;

- C-based RSE inserted into RSE wrapper;

- C++ controller/RSE integrated into ROS wrapper.

**Part B: Assumptions on Platform**

**1) Information flow**

- All the ROS nodes associated with the sensors connected on the robot reliably advertise their information to the ROS Master and in turn, the UPenn RSE is assumed to always be able to subscribe and get data from all the sensor nodes of the system.

- The same observation applies for advertising data to the actuators: the control signal generated by the PID is assumed to be reliably propagated to the actuators of the robot.

**2) Expected rates**

We tested our controller under the following conditions

- The encoder measurements are delivered at the average rate of 50 Hz with a minimum rate of 49.5 Hz and a maximum rate of 50.1 Hz.

- The GPS measurements are delivered at the average rate of 10Hz with a minimum rate of 8Hz and a maximum rate of 19Hz.

- The input commands are delivered to the actuators at a frequency of 50 Hz.

**3) Bounded measurements**

We tested our controller under the following conditions

- The maximum expected encoder counts increment every time the sensor gets a new measurement is less than 21 counts.

- The maximum difference between left and right encoder measurements is 1 count.

- The measured velocity of the robot while on flat surface is always less than 1.25 m/s.

**3) Assumptions on the implementation**

- The UPenn node must be run after all the sensor nodes are on and are broadcasting data.

**4) Bounded jitter**

- Bounded difference between actual and theoretical sampling;

- errors caused by non-uniform execution of control-related tasks.

**5) Bounded measurement error for un-attacked sensors**

- Bounded difference between measurement provided and its true value;

- errors caused by analog-to-digital conversion and rounding.

**6) Bounded mathematical errors**

- Bounded difference between analytical and numerical mathematical operations.

**7) Bounded control signal error**

- Bounded difference between the generated and applied control.

**Part C: Assumptions on Environment**

**1) Bounds on environment**

- the robot must be operated in environments and under conditions whose dynamics are similar to the modeled dynamics;

- the absolute difference between the effects of the simulated environment and true environment must be bounded.

The following are some examples of environment boundaries:

**1.a) Bounds on surface grade**

- the robot must be operated on near-level surfaces;

- level-surface +/- small deviations.

**1.b) Bounds on traction**

- the robot must be operated on surfaces with minimal “slippage”;

- bounded skidding while in forward motion.

**1.c) Bounds on external forces**

- the robot must be operated in environments with bounded external forces;

- the horizontal forces must be bounded (i.e., obstacles, wind, etc.);

- the vertical forces must be bounded (i.e. additional mass).

**Part D: Guarantees Provided**

1. **The RSE guarantees a correct vehicle speed estimation when less than 2 sensors (i.e., 0 or 1) are under attack.**

**-** For instance, either one of the encoders, or the GPS, can be under attack while the other sensors are not compromised, thus, the controller will be able to estimate the real speed of the vehicle.

**2) speed estimation**

- the absolute difference between true speed and estimated speed is bounded.

- During the tests run at UPenn, using noisy measurements from the encoders and the GPS, on flat tiled and grass surfaces, we observed a correct velocity estimation with error under 10%.

**3) steady-state speed control**

- the absolute difference between true speed and desired speed is bounded after some time *T*.

**4) transient speed control**

- the absolute difference between true speed and desired speed is exponentially decaying from time 0 to *T*.