MASTER THESIS

Safety case for a two-wheel variant e-vehicle

Research domain
Functional safety

Topic

Context: Safety can be characterized as the capability of a system to remain outside unsafe operating zones in all circumstances. Traditional vehicles often will have a “safe” state in a passive way, e.g. when power is lost. With electrically driven vehicles the vehicle is much more controlled in an active way. Stability is then maintained by using an active control loop that keeps the vehicle in a safe zone by using sensors to read the vehicle operating conditions, applying a control law and use actuators to apply forces to e.g. the traction system (often motors connected to the wheels). This problem is in particular present when the vehicle has less than 3 wheels, as with 3 or 4 wheels the geometric distribution in space keeps the vehicle stable. With a one or two wheel vehicle, the stability can be obtained by using a gyroscopic sensor. A feedback loop controller can then actively compensate for when the point of gravity is no longer on a vertical axis versus the point where the wheel hits the ground surface. Deviations will occur to forces that are applied during driving the vehicle: traction system forces as responses of the driver commands, irregularities in the ground or external disturbances (e.g. wind, a collision). This is a classical example of the inverted pendulum problem. A major restriction is that the gyroscopic sensor based solution has a limited angle range, outside which the system becomes unstable. As a point of reference, Altreonic developed a dual control loop (with no safety support) that can keep the vertical axis upright and gives a user defined forward or backwards velocity to a one-wheel vehicle. The control loops was first developed using an RTOS simulator under Windows interacting with physical simulation model connected to a 3D visualization program Later on the control loop was converted to run on an ARM based controller. This allows to visually verifying that the control loop is functional. A second step will need to take into account safety cases and extend the physical model for it.

Aim: The master thesis will consist of the following steps:

- Apply a safety analysis to a 2-wheel variant vehicle:
  - defining the safety cases (Hazard analysis and risk assessment)
  - defining the FMEA (Failure Mode and Effect Analysis)

- Propose an adapted architecture and safety measures to cope with the detected safety cases and failures
- Implement an demonstrate the safety enabled control system on a two wheel demonstrator (= Elektor Wheelie)
    - the original controller will be used, but retrofitting a more powerful controller can be an option.
- The student will use the FLAME[1] safety engineering flow as a guideline.
- The student will be actively coached and monitored on a weekly basis.

Profile
Master of Engineering or Master of Science.

- Use of modeling tools like Vissim, Simulink,
- Programming in low level C,
- Notions of real-time control using a RTOS.

Term
Q3 2011 – Q1 2012

Supervisors

Eric Verhulst, Altreonic NV
Bert Dexters, Flanders' DRIVE

[1] FLAME = Flanders' ASIL Methodology = a safety engineering flow based on leading international functional safety standards such as ISO 26262 and IEC 61508, developed by Flanders' DRIVE, Altreonic NV and other Flemish industrial partners.