Advanced Transportation Systems

Cyber-Physical Systems

Raj Rajkumar (PI), Ed Clarke, John Dolan, Sicun Gao, Paul Rybski,
David Wettergreen, Paolo Zuliani

Carnegie Mellon

GM

Societal & Economic Impact

- 1 million automotive fatalities in worldwide and >32,000 in the US *every* year
- Medical care, disability and property damage is $518 billion *every* year.
- 35 hours per year per person wasted in traffic delays.
- Loss of independence & self-esteem of senior and disabled citizens.

Vision

- Scientific & technological foundations for Smarter and more Autonomous Transportation
- Formal foundations for proof of correctness
- Dependable run-time infrastructure

Challenges & Approach

Real-World Conditions

Endogenous Challenges
- Sensor, actuator, processor failures
- Software failures
- Network failures

Exogenous Challenges
- Pedestrians/Cyclists
- Weather, lighting and road conditions
- Loss of GPS

Safe Driving Challenges
- Dense/volatile traffic
- Humans in the loop
- Detours/Accidents

Collaboration Challenges
- Vehicle to Vehicle (V2V)
- Vehicle to Infrastructure (V2I)
- Higher Efficiency w/ Safety

Approach

Robust Architecture

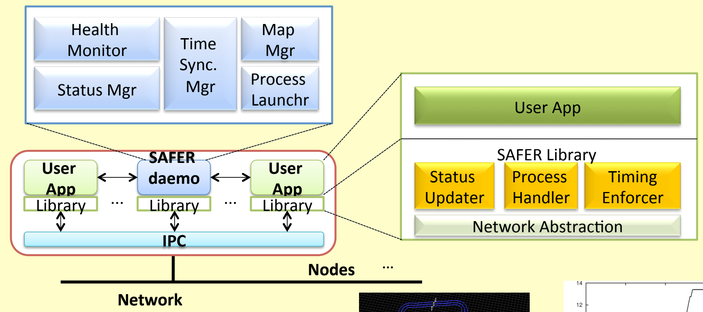
Robust Perception

Robust Behaviors

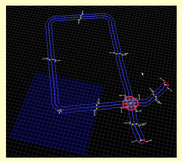
Multi-Vehicle Cooperation

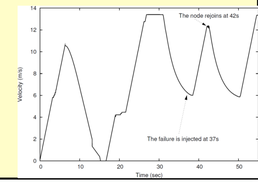
Hybrid Systems Verification

Dependable Real-Time Run-Time Infrastructure

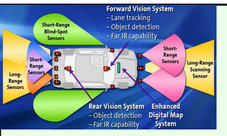


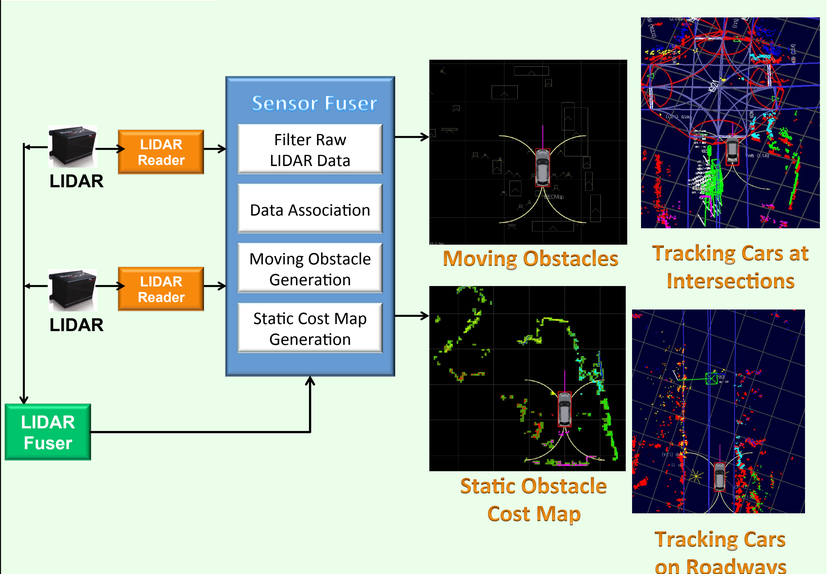
Tolerate single-point of failure
Fail-safe after second failure
Cost-effective solution
Tight end-to-end latencies





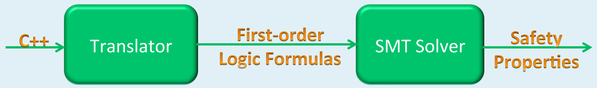
Sensor Processing





Formal Code Verification

Using bounded model checking, invariant checking

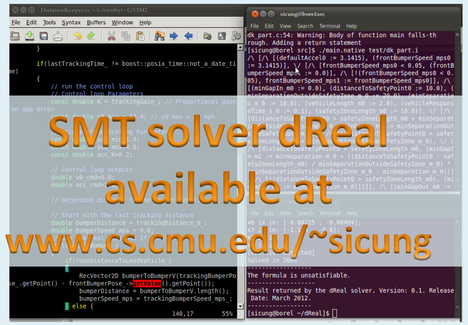


Original Code: (DistanceKeeper.cc)

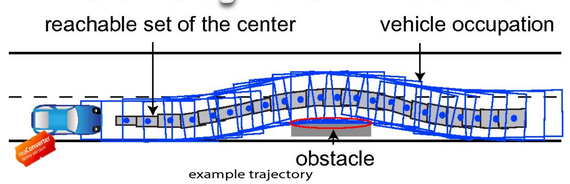
```
// compute the minimum gap as a smooth transition from inside to outside safety zone
double minGapIn_m = 0.0;
double distanceToSafetyPoint = 10.0;
double minSeparationOutsideSafetyZone_m_ = 20.0;
double minSeparation_m_ = 10.0;

if(distanceToSafetyPoint > safetyZoneLength_m + minSeparationOutsideSafetyZone_m_)
{
   minGapIn_m = minSeparationOutsideSafetyZone_m_;
} else if (distanceToSafetyPoint > safetyZoneLength_m) {
   // scale from outside to inside as we approach the safety zone
   minGapIn_m = minSeparation_m_ +
      (distanceToSafetyPoint - safetyZoneLength_m) /
      minSeparationOutsideSafetyZone_m_ *(minSeparationOutsideSafetyZone_m_ - minSeparation_m_);
} else {
   minGapIn_m = minSeparation_m_;
}
```

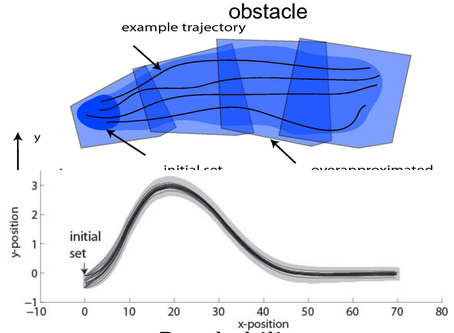
Output Logic Formula:

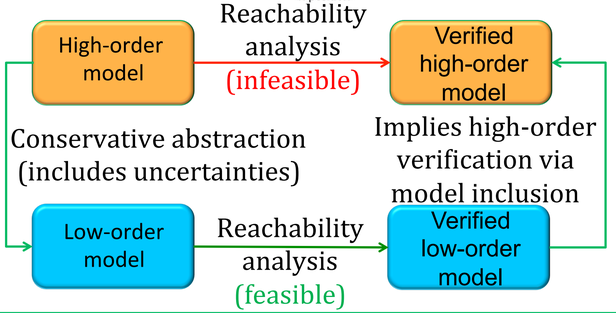
```
[sicung@borel test]$ ../main.native dk_part.i
/\ [/\ ((minGapIn0 := 0.0), (safetyZoneLength0 := 10.0), (distanceToSafetyPoint0 :=
 20.0), (minSeparation0 := 10.0)), \/ [/\ (distanceToSafetyPoint0 > safetyZoneLe
ngth0), (minGapIn1 := minSeparationOutsideSafetyZone0)], /\ [!(distanceToSafetyPoint0 > safet
y0), \/ [/\ (distanceToSafetyPoint0 > safetyZoneLength0), (minGapIn1 := minSeparati
on0 - (minSeparationOutsideSafetyZone0 - (minSeparationOutsideSafetyZone0 - mi
n(safetyZoneLength0), (minGapIn1 := minSeparation0)))]], true]
{
distanceToSafetyPoint: 0,
minGapIn: 1,
minSeparation: 0,
minSeparationOutsideSafetyZone: 0,
safetyZoneLength: 0
}
```



Safety Verification







Road State Classification