Practical Application of SPARK to OpenUxAS

Initial Results

M. Anthony Aiello
Dr. Claire Dross
Dr. Patrick Rogers
AdaCore

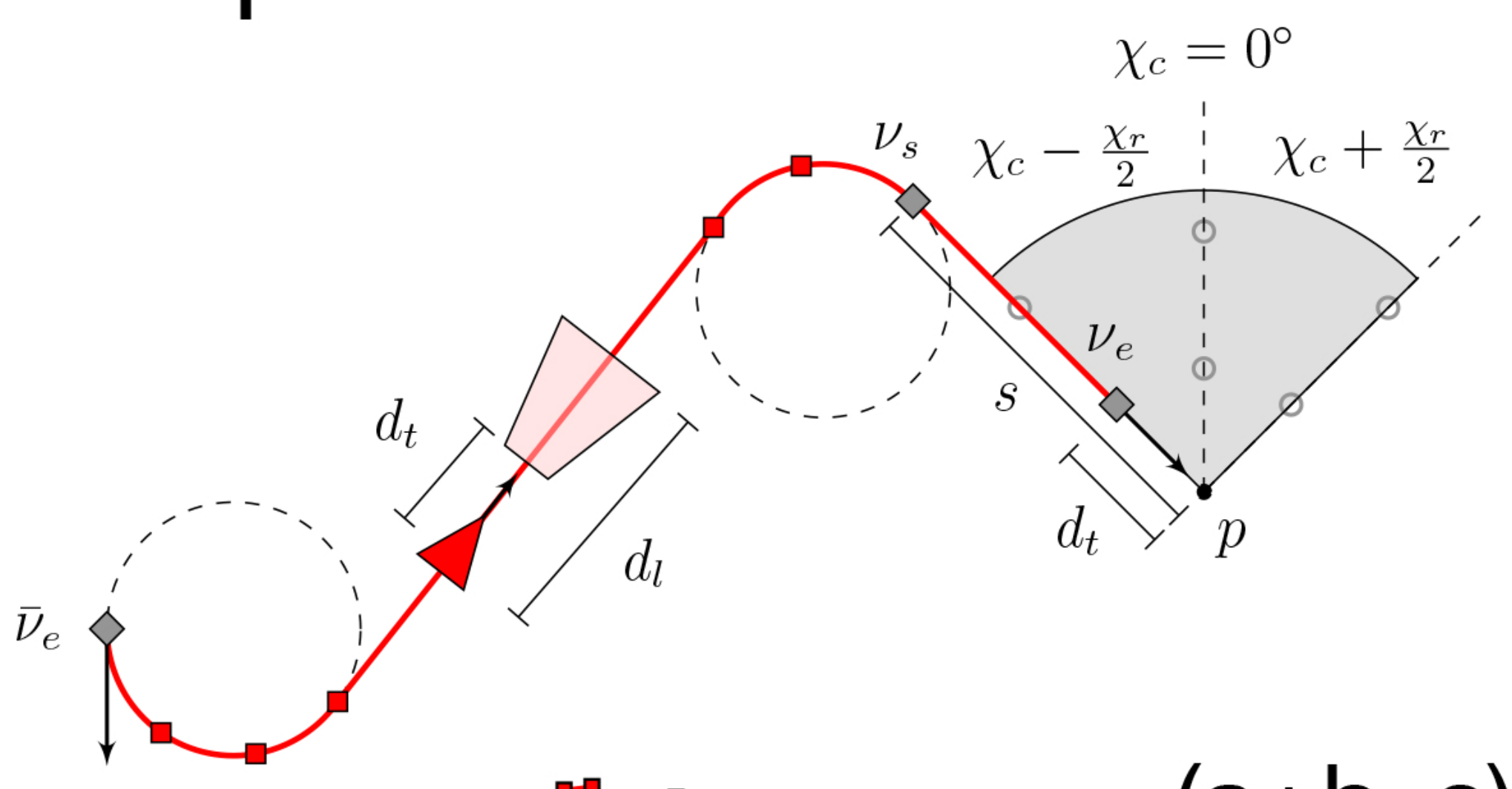
Dr. Laura Humphrey
James Hamil

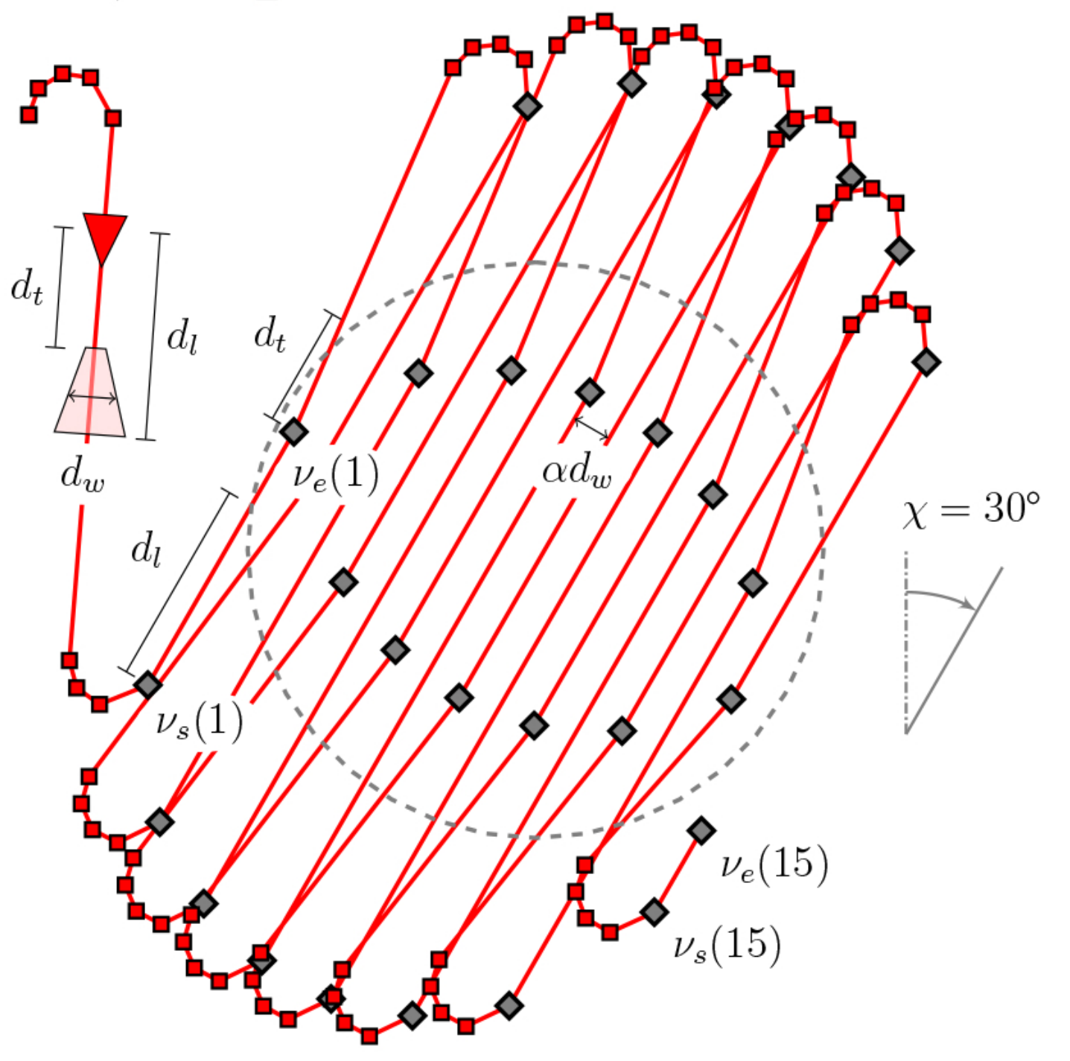
Goal

Establish a foundation for platform-wide proofs of functional, safety and security properties.

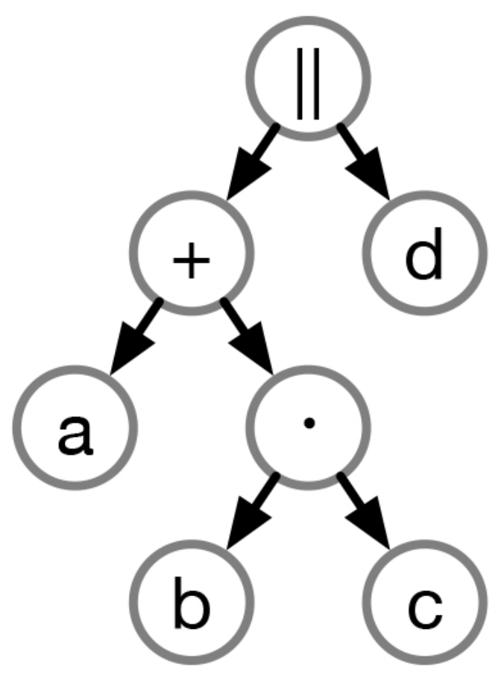
What is OpenUxAS?

A platform for autonomous cooperative control.

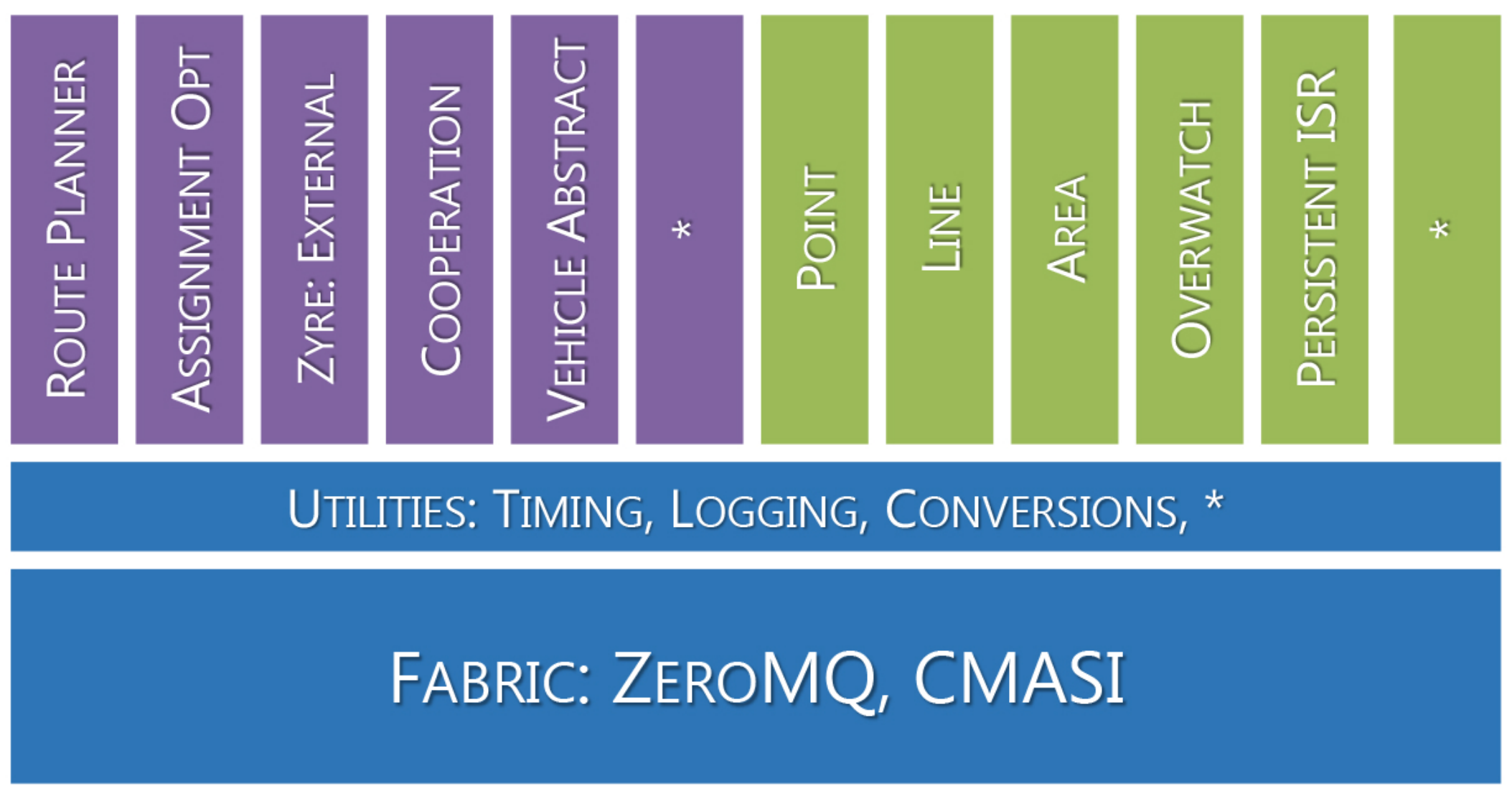




(a+b·c) || d



Tasks Process Algebra Task Assignment



Route Planner | Assignment Opt | Zyre: External | Cooperation | Vehicle Abstract | * | Point | Line | Area | Overwatch | Persistent ISR | *

Utilities: Timing, Logging, Conversions, *

Fabric: ZeroMQ, CMASI

- *service-oriented architecture*
- *67k lines C++ code*
- *custom message set (LMCP)*
- *ZeroMQ pub/sub*

What is SPARK?

A programming & specification language with proof tools.

```
procedure Increment
  (X : in out Integer)
with Global   ⇒ null,  ←———————— data dependencies
     Depends  ⇒ (X ⇒ X), ←—————— flow dependencies
     Pre      ⇒ X < Integer'Last,
     Post     ⇒ X = X'Old + 1;  ← functional contracts
```

```
procedure Increment (X : in out Integer)
is begin
  X := X + 1;  ←——————————— absence of run-time
end Increment;                  errors
```

Learn more: learn.adacore.com

What We Did

Rewrite the Automation Request Validator Service in Ada and SPARK.

Base Classes

- *30 packages*
- *7,015 lines Ada*

LMCP

- *202 packages*
- *32,831 lines Ada*
  (mostly auto-generated)

SPARK

- *11 packages*
- *1,794 lines SPARK*

All keep-out areas must be defined in the operating region.

```
function All_Elements_In (V : Vector; S : Set)
  return Boolean
is
  (for all J of V ⇒ S.Contains (J));

function Check_For_Keepout_Zones
  (Id               : Int64;
   Operating_Regions: Operating_Region_Maps;
   KeepOut_Zones    : Int64_Set) return Boolean
is
  (All_Elements_In
   (Get_KeepOutAreas
     (Element (Operating_Regions, Id).Content),
    KeepOut_Zones));
```

The full property contains 10 predicates and is 79 lines long. The validation procedure is 471 lines long.

Proved Correct

What Comes Next

Expand Ada and SPARK work to enable platform-wide proofs.

- *expand Ada and SPARK rewrite of base classes*
- *formalize additional service contracts*
- *formalize compositional properties of the architecture*
- *investigate security properties from the system level to the code level*
- *incorporate SPARK support for ownership pointers*

distribution unlimited; approved for public release; case number 88ABW-2017-1985
supported by the USAF under contract 18-S8401-17-C1