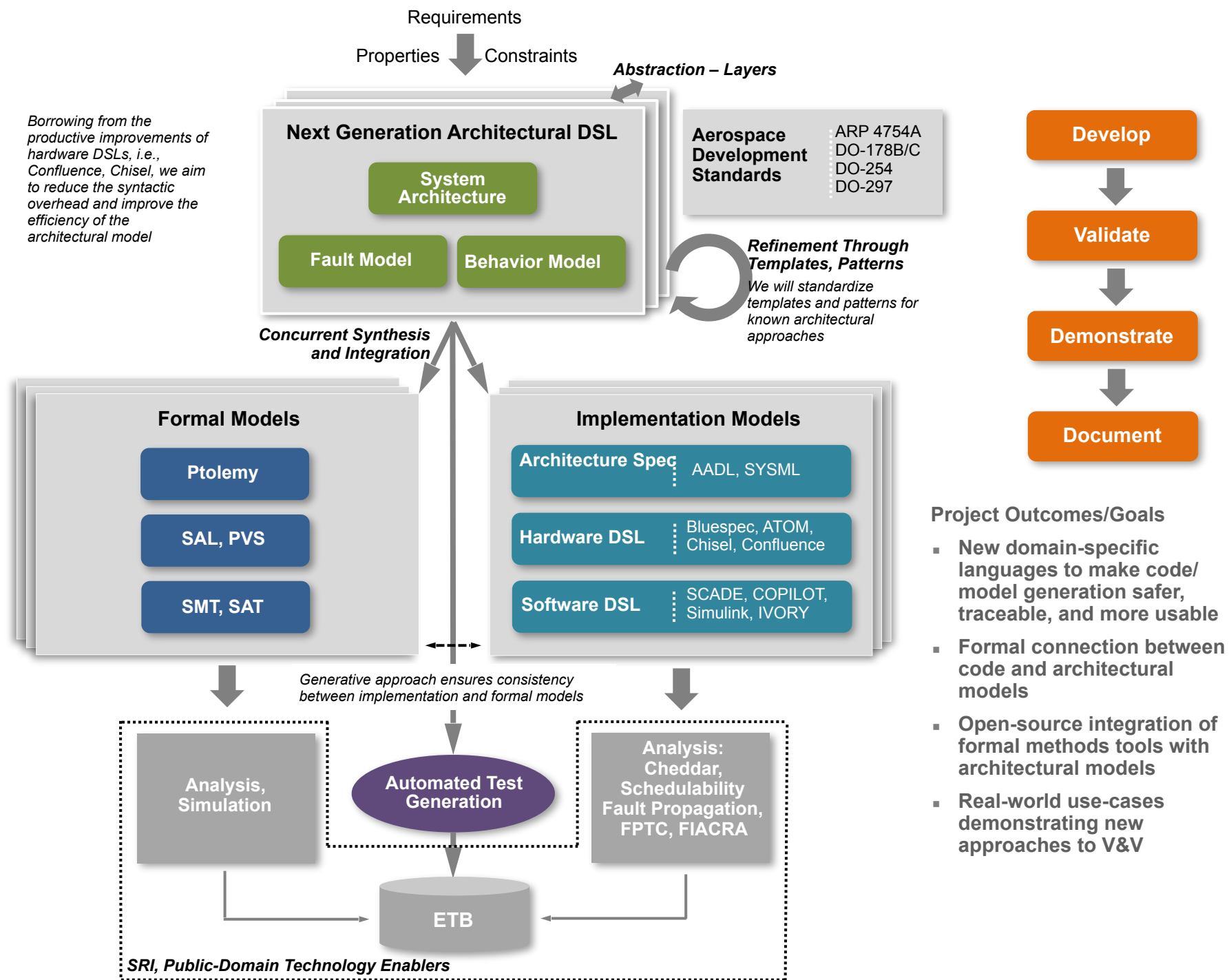


# AFFIRM Year 2

August 9, 2016 - NASA Langley Research Center

# Framework



# AFFIRM Year 1

- Determining what abstractions are appropriate and necessary in the ADSL
- Exploration of the case studies, primarily OM(1) and WBS
  - communication, timing, faults
  - not concerned (yet) with verification
- Researching related work, modeling languages and paradigms, etc.

# AFFIRM Year 2

- Experiments toward translating system specifications in an architectural DSL into transition system models.
- Continuing to push on our case studies as they represent significant modeling and verification challenges.
- Converging on a suitable modeling framework (calendar automata, clock, and fault model)

# Case Studies

During year 2 we focused mostly on two case studies:

- **OM(1)** - the classic "oral messages with one round" algorithm for byzantine fault tolerant validity and agreement,
- **WBS** - a real-time model of a supposedly fault tolerant wheel break system that exhibits problematic sampling.

The two case studies entail very different models. The OM(1) model explores message passing and data flow, while the WBS model explores the phase offset and period timing in multiple nodes observing a common signal.

# A Calendar Based OM(1)

- Motivation
- Model highlights
- Deeper Dive
  - Fault model
  - Verification
  - Benchmarking

# Motivation for studying OM(1)

- It is an algorithm/system with a long history; many models and much verification work has been done on it

This means we can easily compare our models and results to a reference.

- Except for small instances, most of the existing verification work on OM(1) relies on interactive theorem proving.
- OM(1) is simple enough that if we can't scale verification here, it spells trouble for carrying out the larger project goals

# Results

- First k-inductive model-checker verified proof for fully parametrized OM(1)
- Model / lemma decomposition
  - Node behavioral vs. messaging, clock, and sync framework
  - State machine for node behavior
  - Decoupled state machine for the message passing and clock framework



# Highlights of our OM(1)

Much of our effort this year was targeted at finishing and refining all aspects of our OM(1) model in order to learn what is required in order to synthesize similar models.

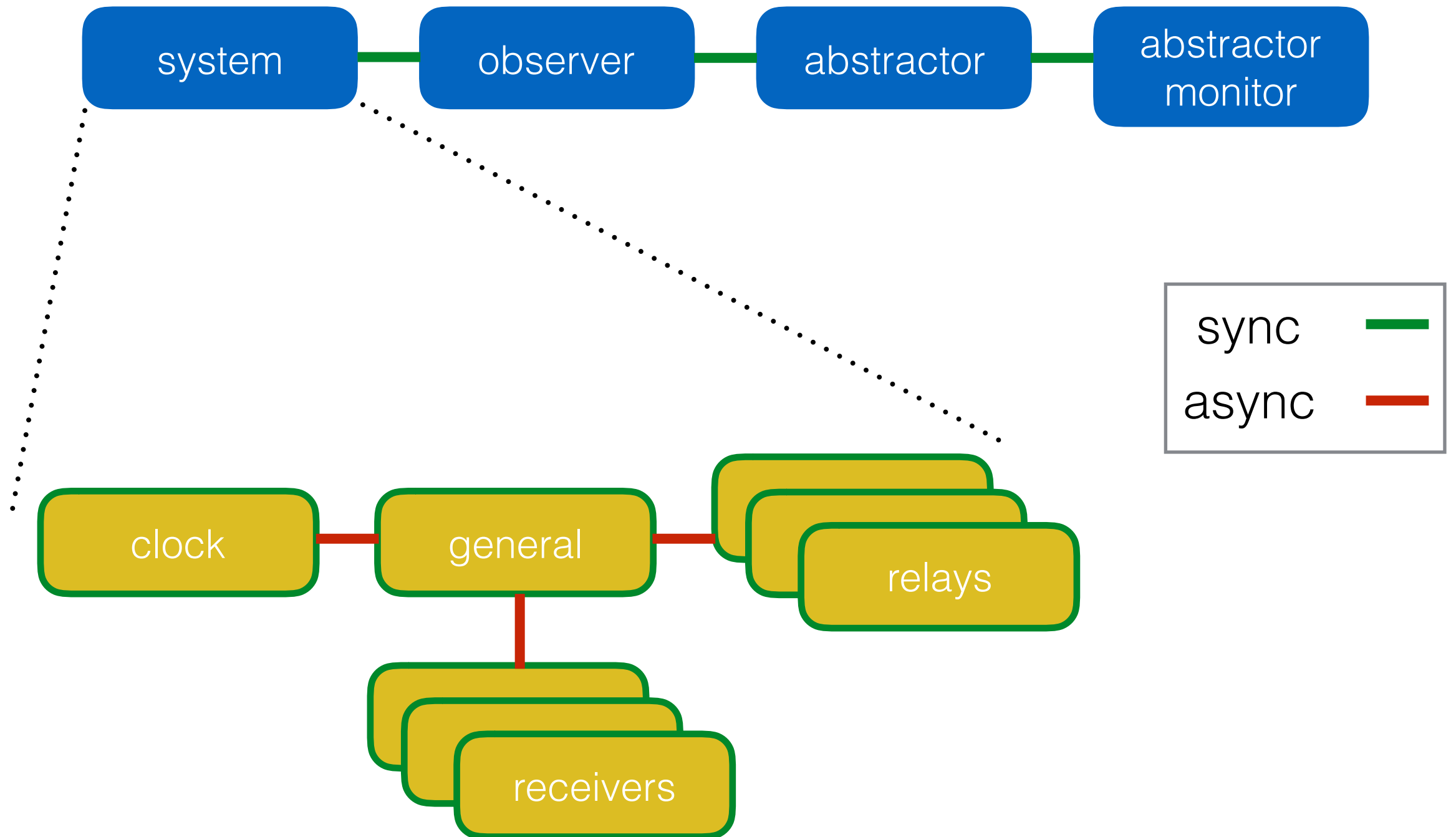
In its current form, the model has these features:

- Fundamentally asynchronous but we don't model any real time constraints
- Message sends and receives are separate (async) transitions
- Modeling synchronous OM(1) on a message passing fabric that is asynchronous
- Number of relays and receivers is parametrized (for the model and the proof)

# Calendar Based OM(1)

- message passing and clock/time management is performed by a calendar automata
- a notion of "atomic" transition block that reduces exploration of interleaved transition steps
- a hybrid fault model is implemented along side the calendar, decoupled from node behavior
- a k-inductive proof of validity and agreement for each node configuration

# Model Architecture




# Focus on one aspect of the work this year

- Faults!
- Why are they interesting?
- why is how we modeled them interesting?

# Fault Model

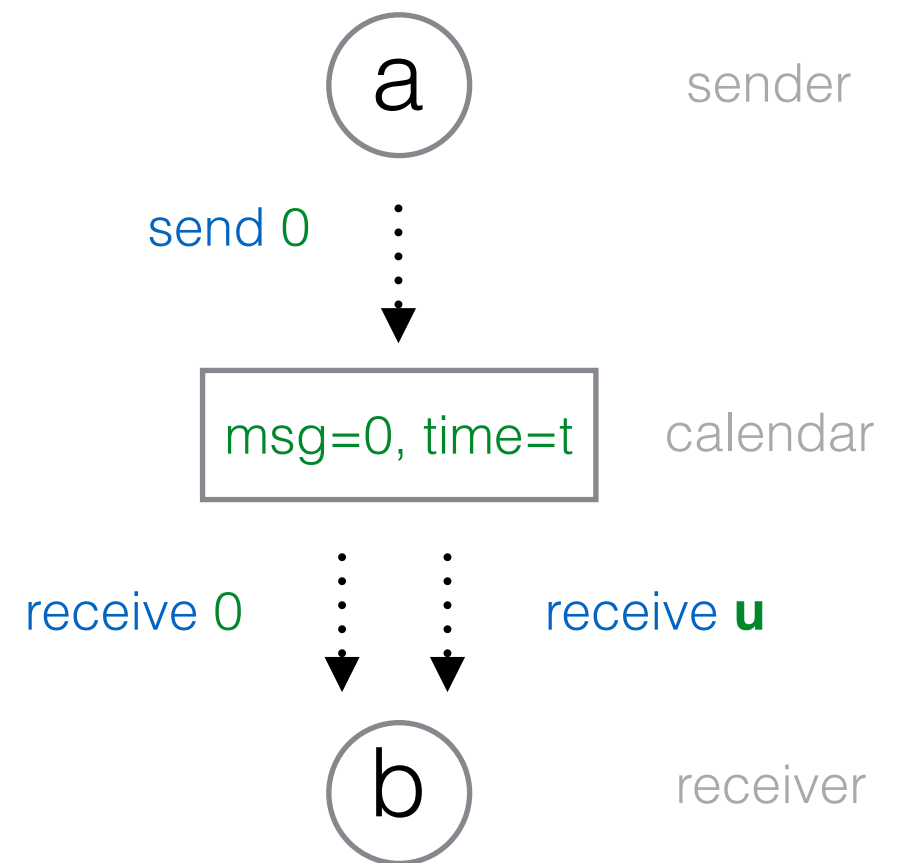
- We have implemented a full *hybrid fault model* on top of the calendar automata
- Fault types: byzantine, symmetric, manifest, none
- Messages are modeled by non-negative integers
- Each node is non-deterministically initialized faulty or not



-1	missing
0	good
>0	faulty

# Fault Model

- When a node sends a message, it appear on the calendar as normal
- When a message is read, the result is either:
  - (sender is not faulty) the intended message
  - (sender is faulty) **uninterpreted constant** of type Message
- A-priori, the number of distinct messages generated in a trace is **unbounded**



**u** is a non-negative integer that we know nothing about  
**u** is a (potentially) different constant on each receive

Rushby quote from  
conference paper

# Fault Model

- Faults are manifested through reading from the global calendar
- Nodes in the model can be specified without any awareness of the fault model and don't need to be changed if the fault model changes
- The extent and type of faults is easily controlled from a single place in the model
- ... but use of uninterpreted constants limits our choice of model checking tools



# Hybrid Fault Model

- The hybrid fault model accounts for four different fault behaviors: byzantine, symmetric, manifest, non-faulty
- The maximum fault assumption is an inequality between the weighted sum of faulty nodes and the total number of nodes

n=3	n=4
1 byzantine fault 1 symmetric fault up to 2 manifest faults	1 byzantine & 1 manifest fault or 1 symmetric & 1 manifest fault or up to 3 manifest faults

Now let's talk about  
verification!

# Verification

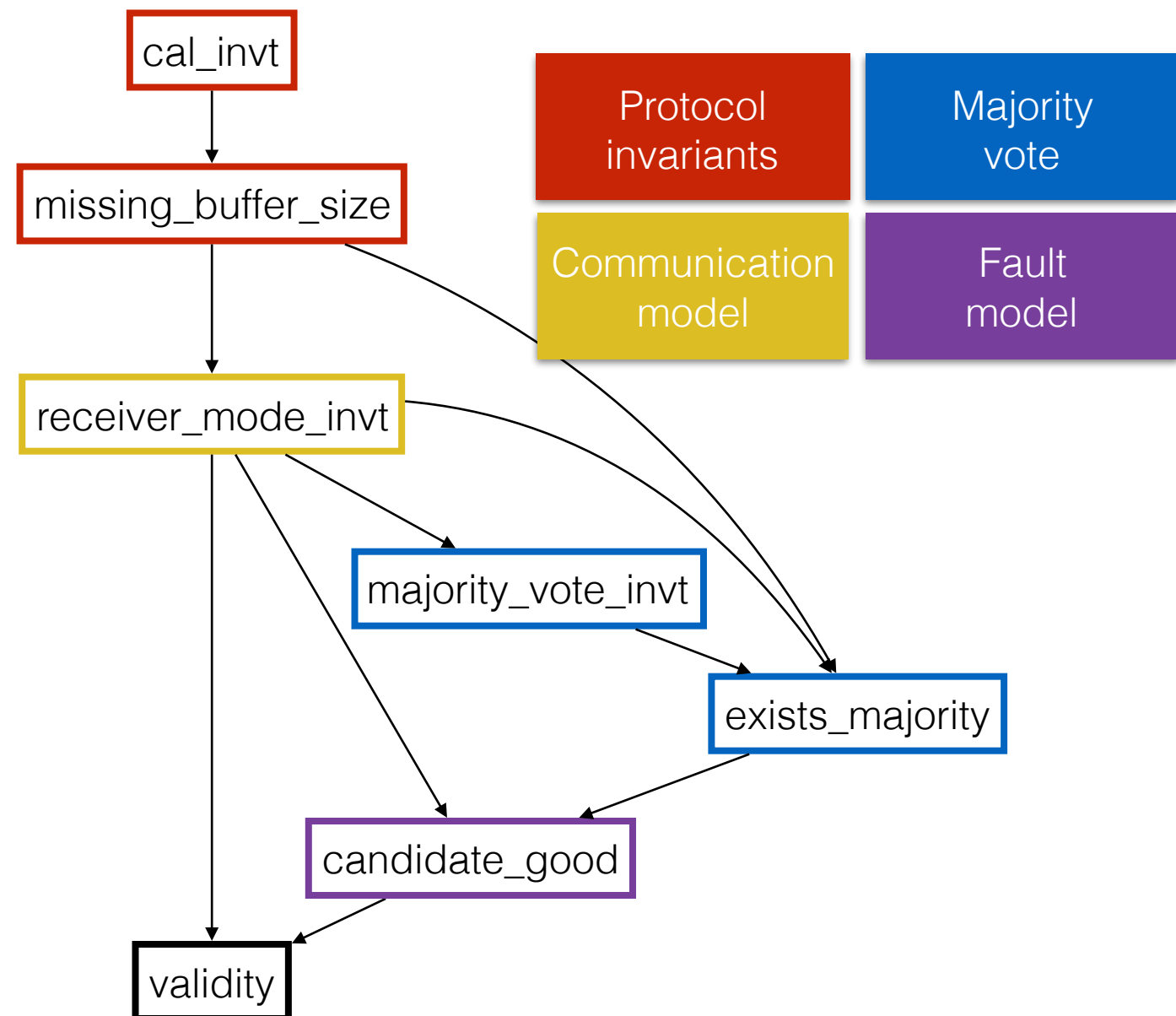
- For infinite models, we cannot use symbolic (BDD) model checking, nor ordinary bounded model checking
- *Infinite bounded model checking* is an SMT-based approach to model checking infinite systems
  - It is supported by SAL (`sal-inf-bmc`)
  - The main technique used is **induction**:
    - user provides inductive invariants of the system
    - model checker tries to prove a given property by induction using the invariants
    - ... or else provides a counter-example trace.
  - Proof by induction generally requires more work on the user's side (providing invariants)
  - Proof by induction is generally much faster and scalable

# Proof by Induction

- We first completed a proof by induction of the **validity** property for OM(1)
  - Many auxiliary lemmas were required to complete the proof – they were hand generated
  - A main goal of the proof's construction was to separate out those auxiliary lemmas that we believe can be generated automatically in our translation
- As a side benefit, we have a proof which is much faster to verify and which scales much better than symbolic or ordinary bounded model checking

# Lemma structure

- **cal\_invt** : basic framework lemmas, e.g. *"time is always non-negative and increases monotonically"*
- **missing\_buffer\_size** : filled cells + unfilled cells equals the buffer size
- **receiver\_mode\_invt** : abstract sub-state machine for the receiver nodes
- **majority\_vote\_invt** : main invariant of the MJRTY (fast majority vote) algorithm
- **exists\_majority** : invariant that holds when there is a majority in a receiver's buffer
- **candidate\_good** : validity means voting a good value



# Proof by Induction

We then completed a proof by induction of the **agreement** property for OM(1)

The proof involved two techniques not needed in the proof of validity:

- an abstract state machine (and associated invariant)
- history variables at points relevant to data flow

# Abstract State Machine

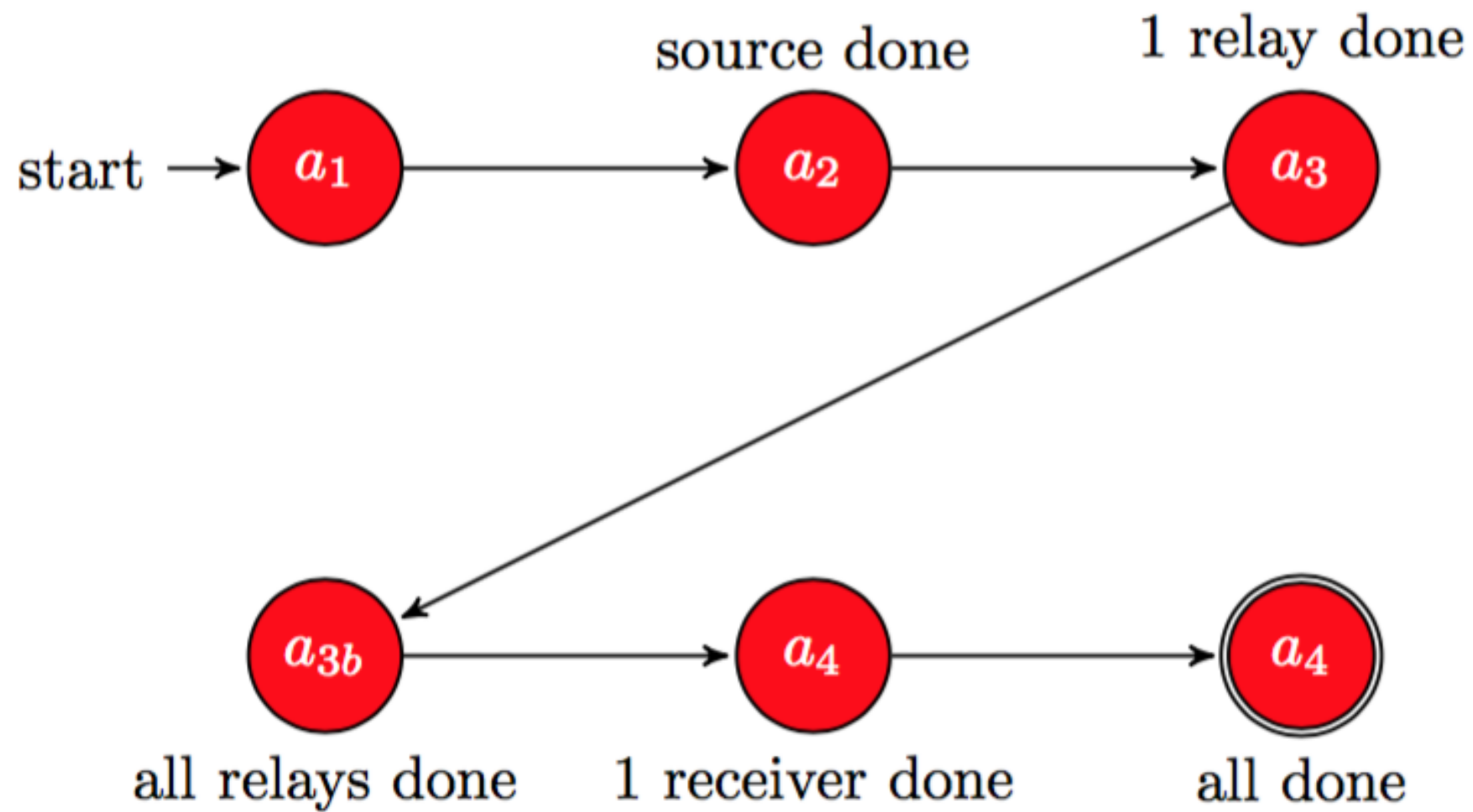
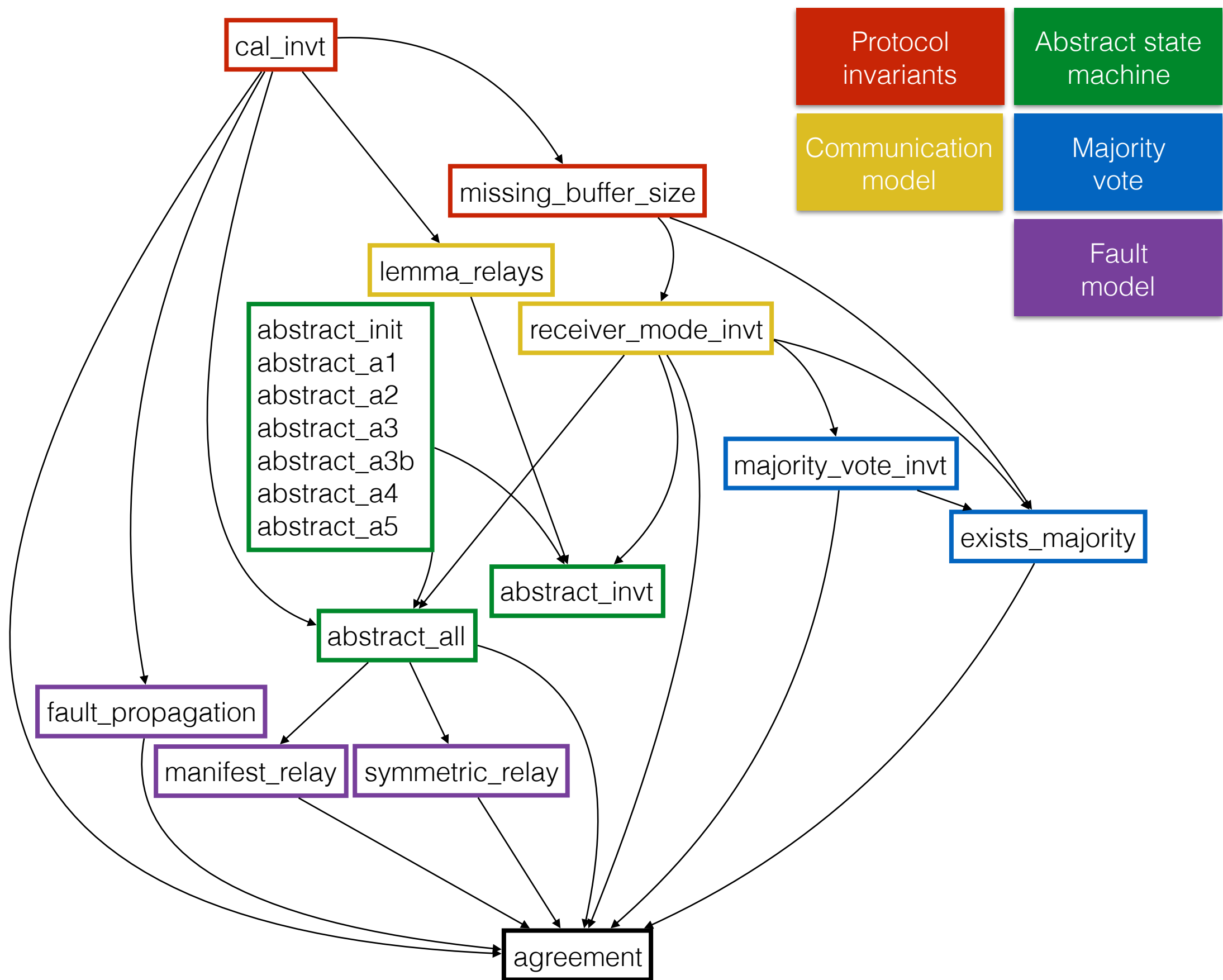


Figure 1





# Benchmarking

- In order to compare our "synthesizable" model to the reference (Rushby's model) we benchmarked the verification over many sets of node configurations
- The largest reference model we were able to verify had 8 nodes
- The largest of our models we were able to verify had 10 nodes
- We see clear indications of single exponential time complexity verifying our model vs. double exponential for the reference

# Benchmark

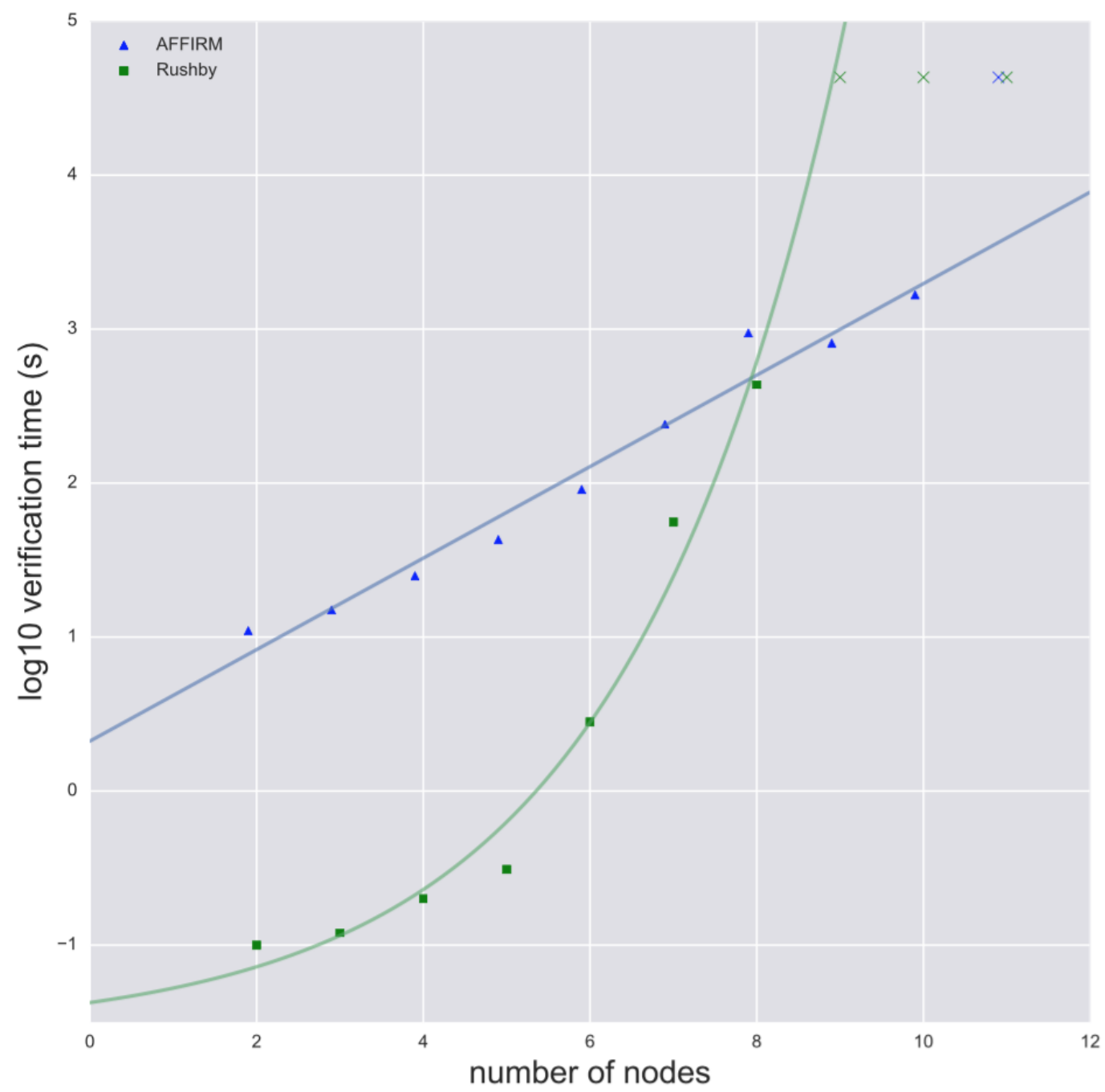


Figure 2

# Beyond OM(1)

- Automatic lemma generation
- ADSL workbench prototype
- Year 3 plans

# Automatic Lemma Generation

We have experimented with tools that provide lemma learning along with model checking

- Experiments with Rockwell Collins using JKind
- Reimplemented physical-layer protocol proofs (8N1, Biphase Mark) in Lustre
- JKind Implements *IC3 Modulo Theories via Implicit Predicate Abstraction* (<http://arxiv.org/pdf/1310.6847.pdf>), and k-induction
- Upshot: lemma generation only works for fixed constants, not uninterpreted constants

# Evidence of PDR Effectiveness

- snippet of constraints on uninterpreted constants
- snippet of learned lemmas to compare

# ADSL Workbench Prototype

We've been working towards a prototype with the following features:

- DSL with simple, intuitive syntax and a well-defined semantics
- C code generation backend
- SAL/Sally model generation backend
- Fault model configurable from the DSL
- Synchronous observers and abstract state machines that can be specified at a high level in the DSL

# ADSL Workbench So Far

- As a starting point, we've chosen the Haskell DSL **Atom** <sup>[1]</sup>
- We added a typed, uni-directional communication channel as a primitive to Atom and augmented the C code backend accordingly
- We've produced an initial specification for OM(1) in Atom, patterned after our previous Ivory/Tower specifications

[1] Haskell EDSL for designing hard realtime embedded software  
<https://github.com/tomahawkins/atom>

## Source ("general") node in Atom

```
-- | Source node ("General")
source :: [V MsgType] -- ^ output channels
      -> Atom ()
source cs = period sourcePeriod
          . atom "source" $ do
    done <- bool "done" False
    let source_msg = goodMsg

    atom "source_poll" $ do
      cond $ not_ (value done)
      forM_ cs $ \c -> do
        c <== source_msg
      done <== Const True
```



## Relay node in Atom

```
-- | Relay node ("Lieutenant")
relay :: Int          -- ^ relay id
      -> V MsgType    -- ^ input channel
      -> [V MsgType]  -- ^ output channel(s)
      -> Atom ()
relay ident inC outCs = period relayPeriod
                        . atom (tg "relay" ident) $ do
  done <- bool "done" False
  msg   <- msgVar (tg "relay_msg" ident)

  atom (tg "relay_poll" ident) $ do
    cond $ isMissing msg          -- we haven't stored a value yet
    cond $ not_ (isMissing inC)  -- there is a value available
    msg <== value inC
    forM_ outCs $ \c -> do
      c <== value inC
    done <== Const True
```

# Year 3 Plans

- Finish work on an initial SAL/Sally backend for the DSL, including:
  - framework lemma generation
  - specification of properties
  - generation of observers and abstract state machines
- Specifying and modeling our other case studies in terms of the prototype workbench
- Investigate test generation for systems specified in the DSL
- Investigate modeling multi-level systems in the DSL
- Publishing the results of the project