A Dependability Case Language for a Radiation Therapy System

Michael Ernst, Dan Grossman, Jon Jacky,
Calvin Loncaric, Stuart Pernsteiner,
Zachary Tatlock, Emina Torlak, Xi Wang

University of Washington

end-to-end verification for safety critical systems

Memory Model

COMPCERT

IronClad

Quark

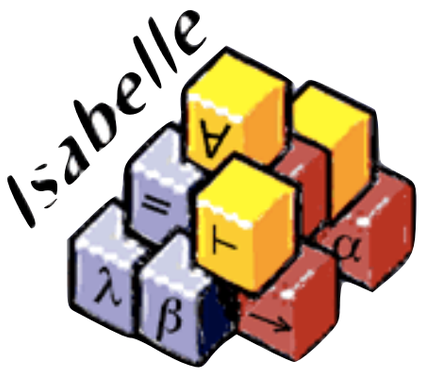
frenetic >>

seL4

SUPPORTED BY

ROSETTE

alloy



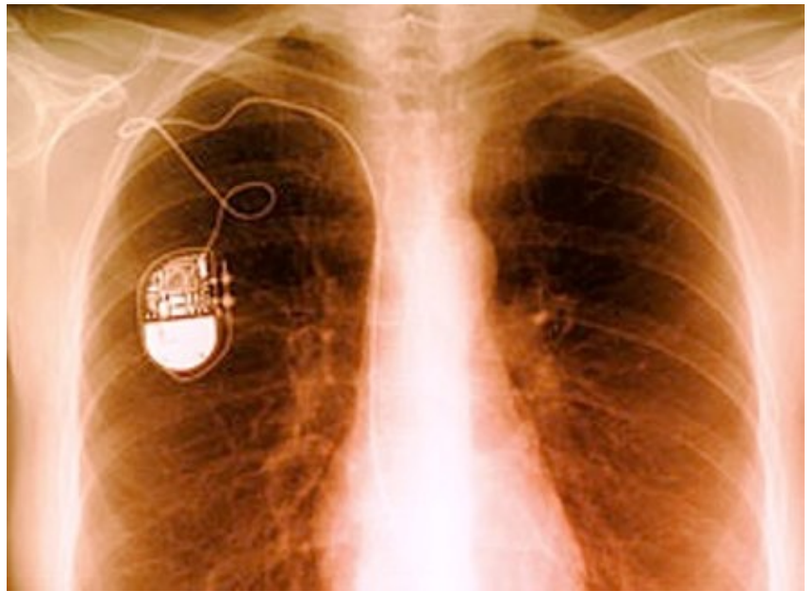
Formal

COMPCERT

IronClad

Quark

frenetic >> seL4




NYSE
CYPRESS


SPACEX

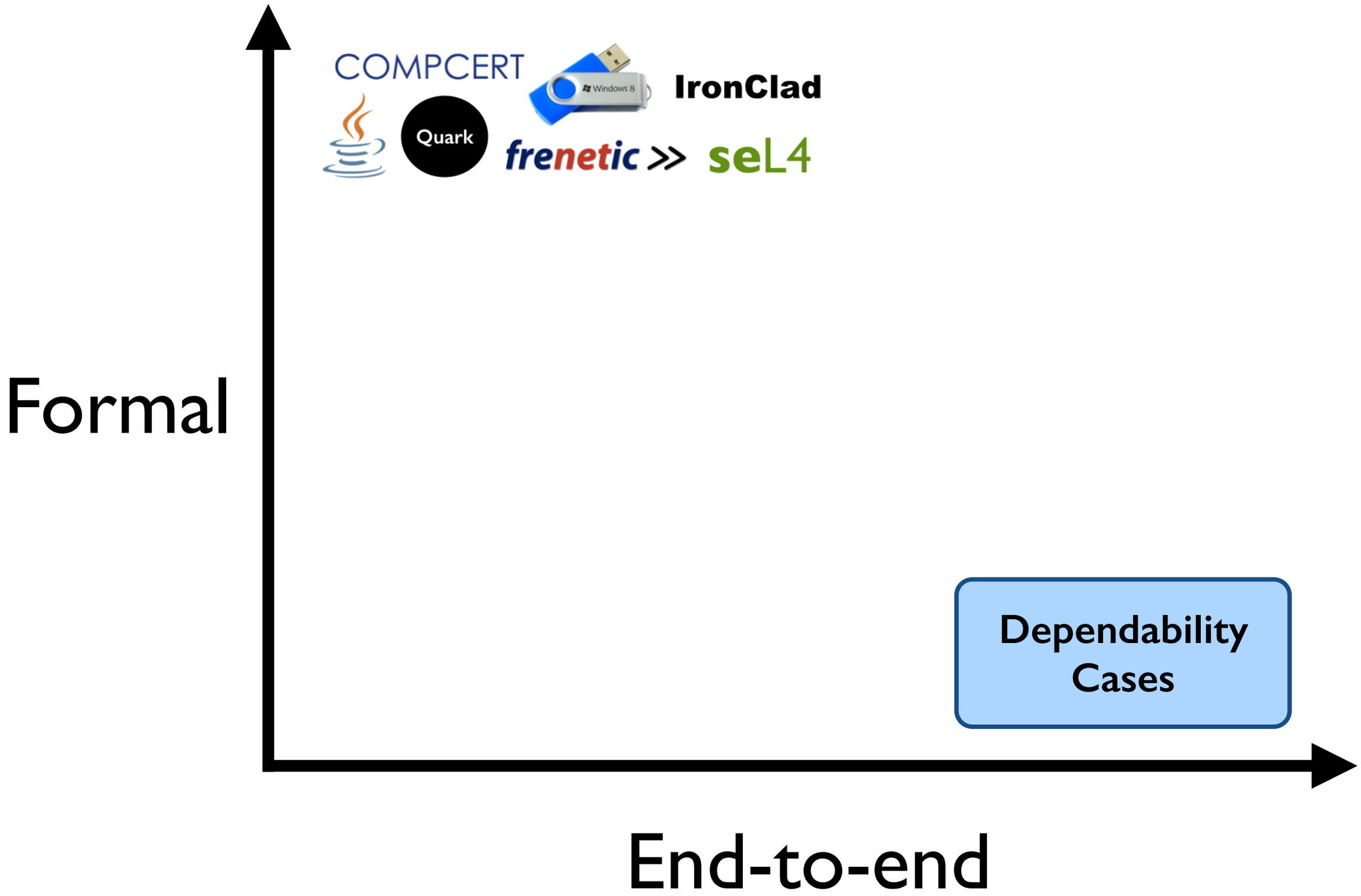
Formal

COMPCERT

Quark

IronClad

frenetic >> seL4


COMPCERT
Windows 8
IronClad
Quark
frenetic >> seL4
Formal
Dependability Cases
End-to-end

Dependability cases

Integrate diverse sources of evidence

check interfaces of design, testing, proof, review

Argue end-to-end claim based on evidence

show claim holds across all layers of a system

Focus on physical system properties

eases validation and focuses verification effort

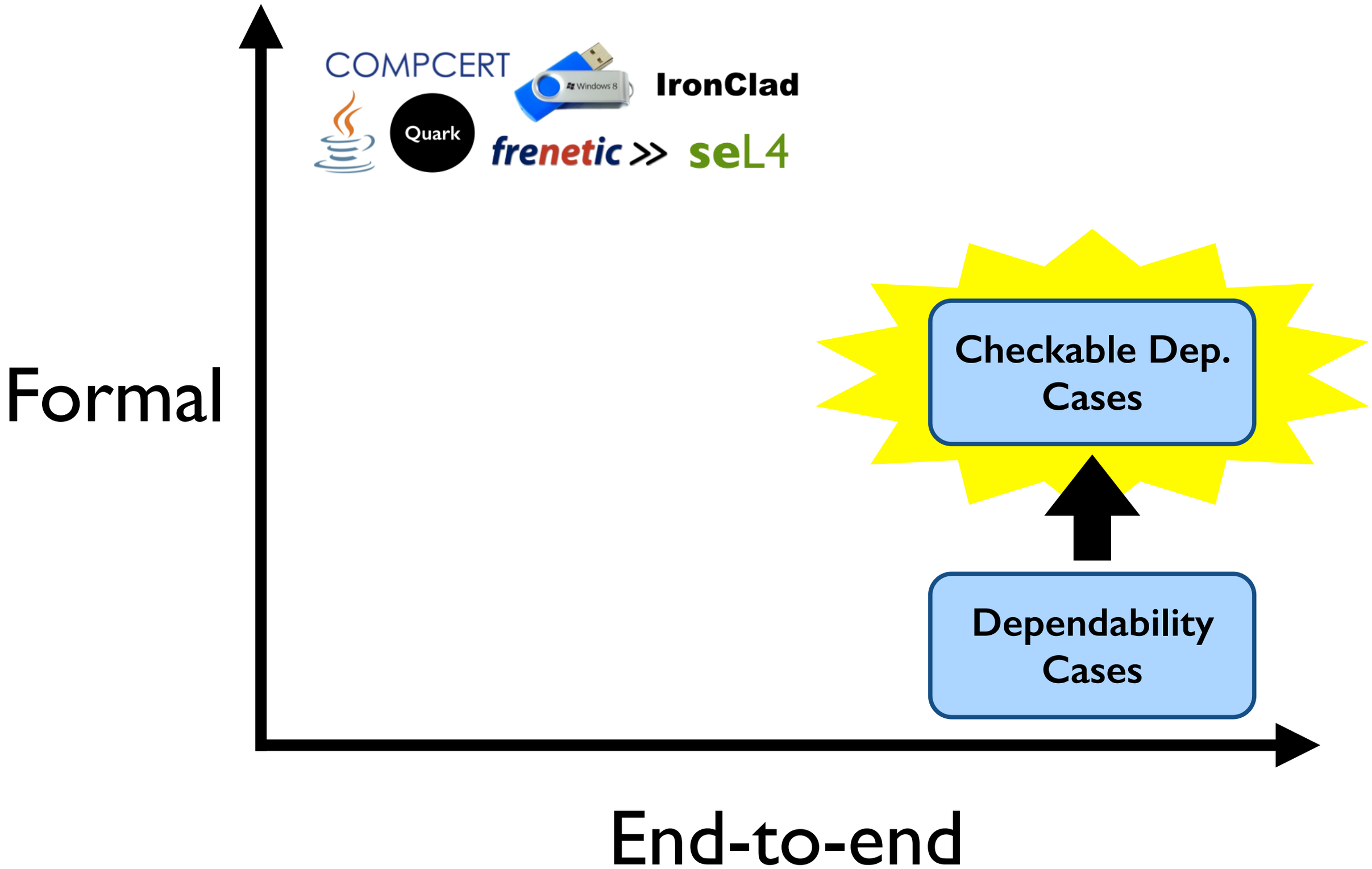
Dependability case engineering

Difficult to develop

Difficult to check

Difficult to maintain

SUPPORTED BY


COMPCERT
IronClad
Quark
frenetic >> seL4
Checkable Dep. Cases
Dependability Cases
Formal
End-to-end

Developing a Dependability Case Language

1. Target specific system

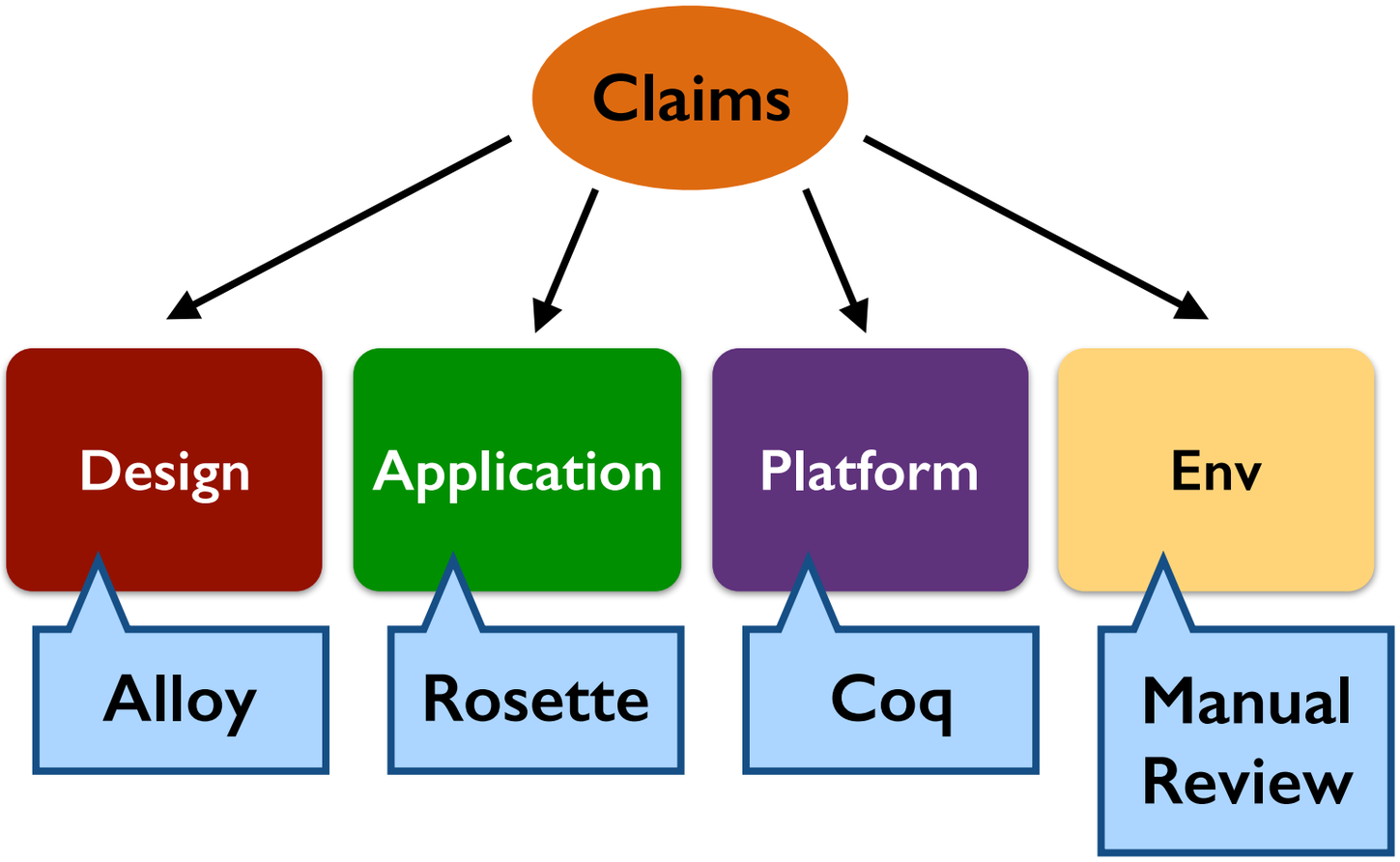
Move from specific to general

avoid attempt to design "silver bullet"

Developing a Dependability Case Language

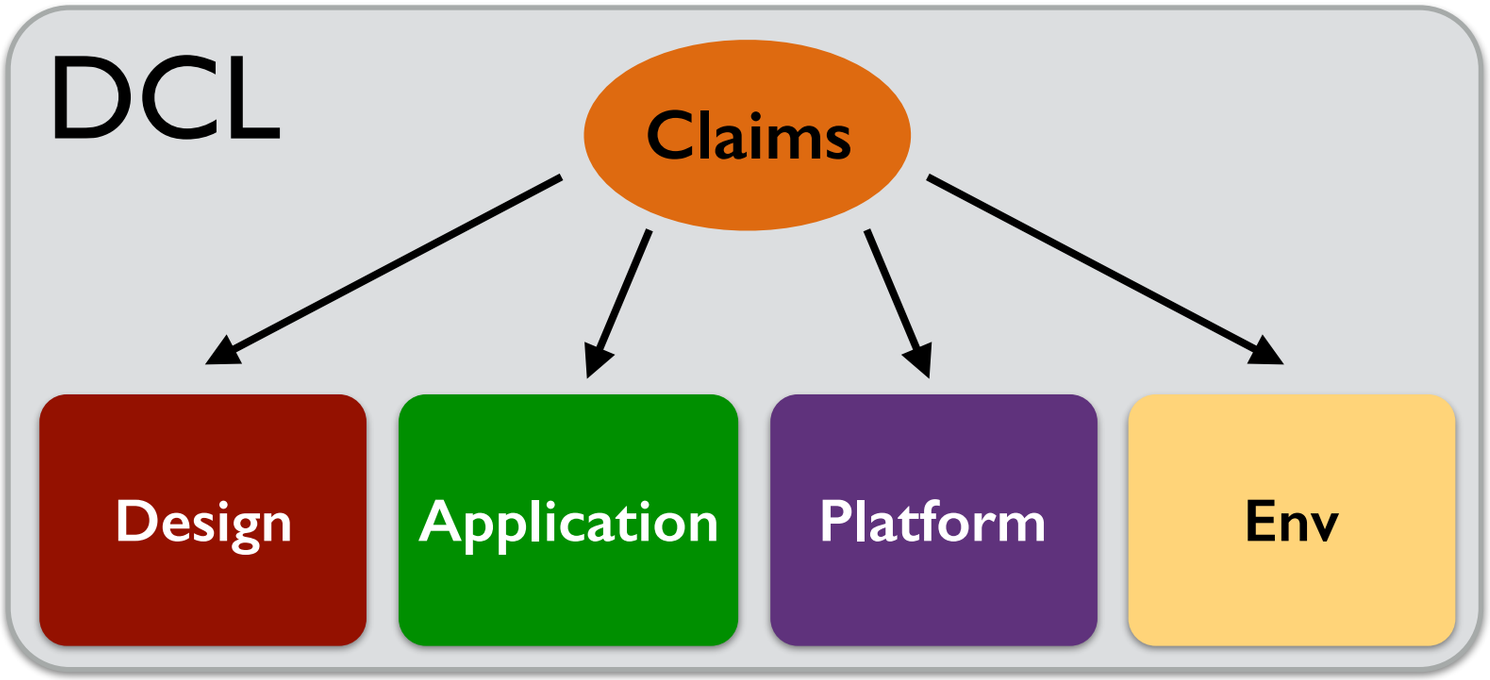
1. Target specific system
2. Develop dep. claims

Developing a Dependability Case Language



1. Target specific system
2. Develop dep. claims
3. Gather evidence

Developing a Dependability Case Language



1. Target specific system
2. Develop dep. claims
3. Gather evidence
4. Design + build DCL

Find general tradeoffs and patterns

make simple easy and hard possible

Impact real-world projects

bring current PL tech to the trenches

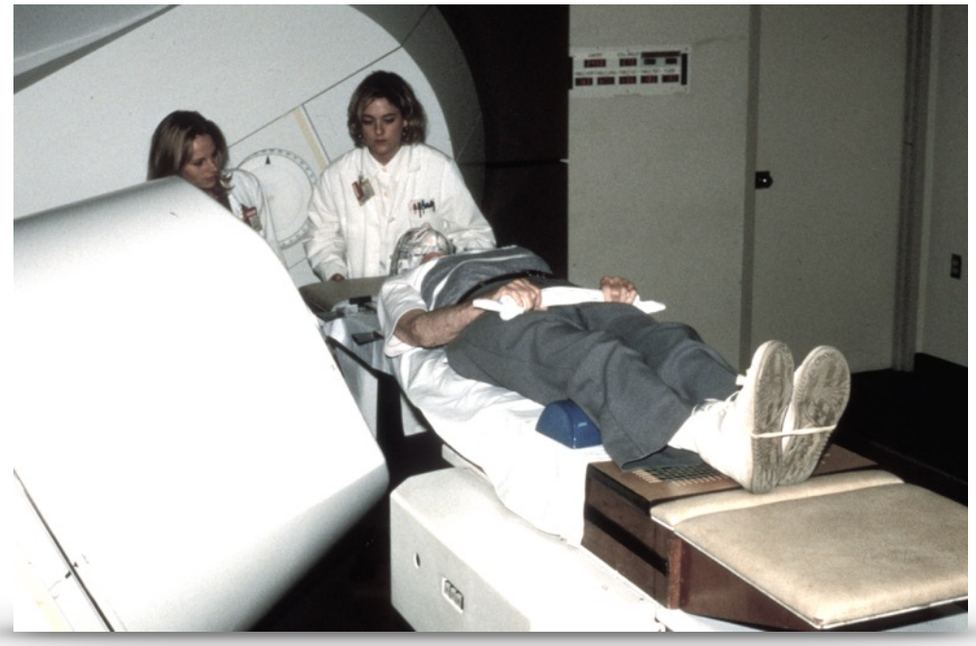
results

an end-to-end dependability case for CNTS

Checking safety of CNTS

Clinical Neutron Therapy System (CNTS) at UW

- 30 years of incident-free service.
- Controlled by custom software, built by CNTS engineering staff.
- Third generation of Therapy Control software now being built.



Therapy Control Software

Beam, motors, etc.

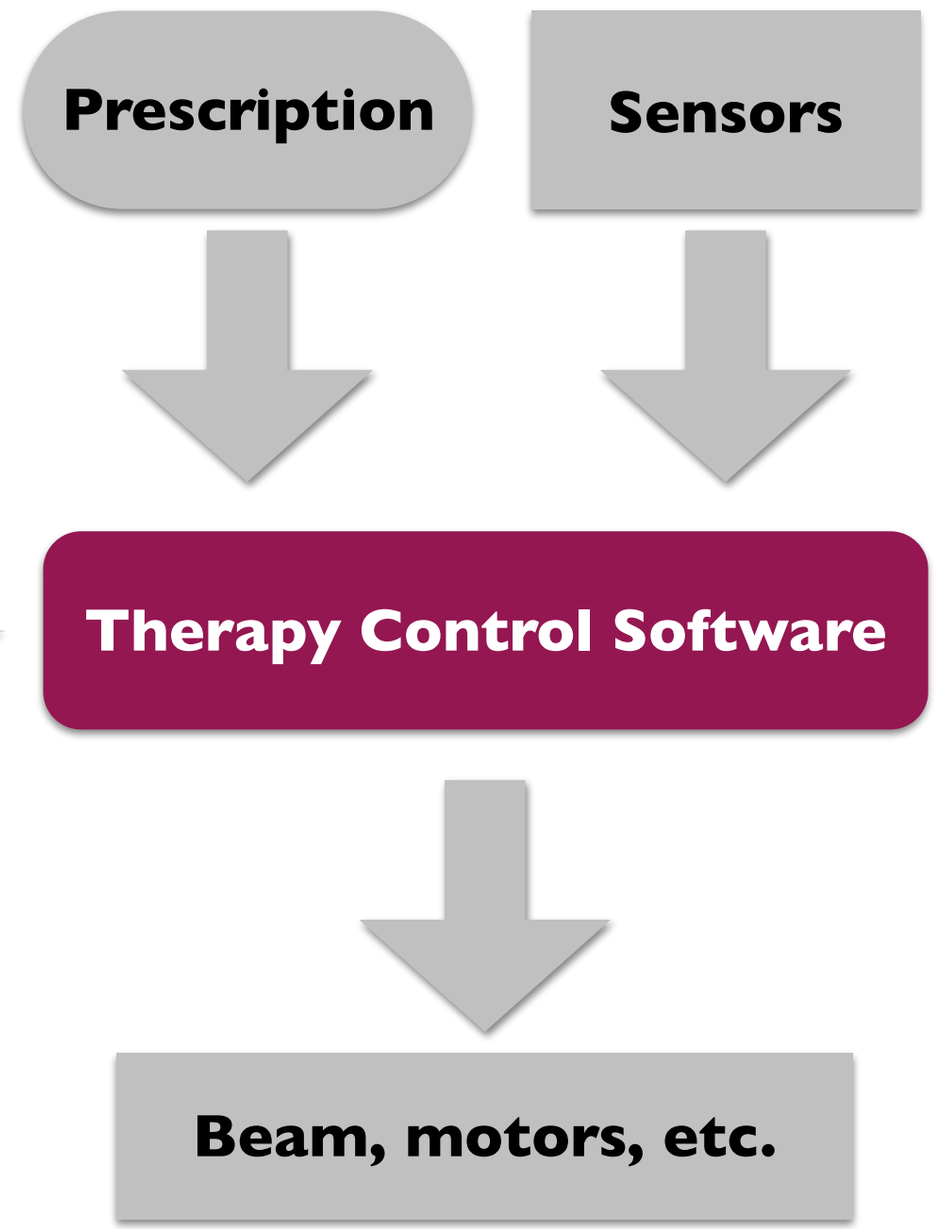
Checking safety of CNTS

EPICS documentation / semantics

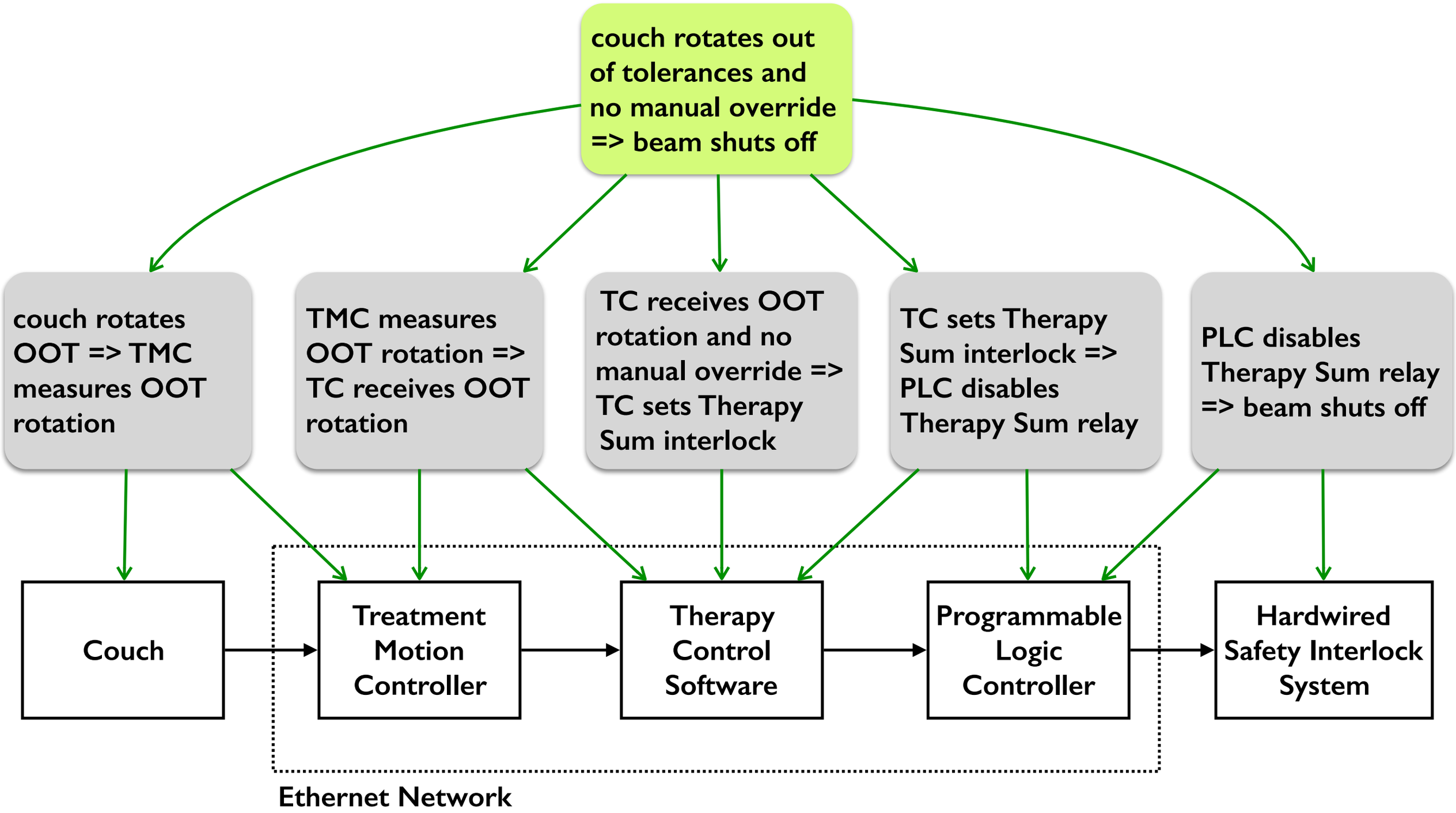
An *end-to-end property* that spans the entire system, not just software.

CNTS Couch Safety Property:

The beam will turn off if the couch rotation angle moves out of tolerances during treatment and the operator has not issued the manual override command.



An informal dependability case for couch safety



A formal dependability case for couch safety

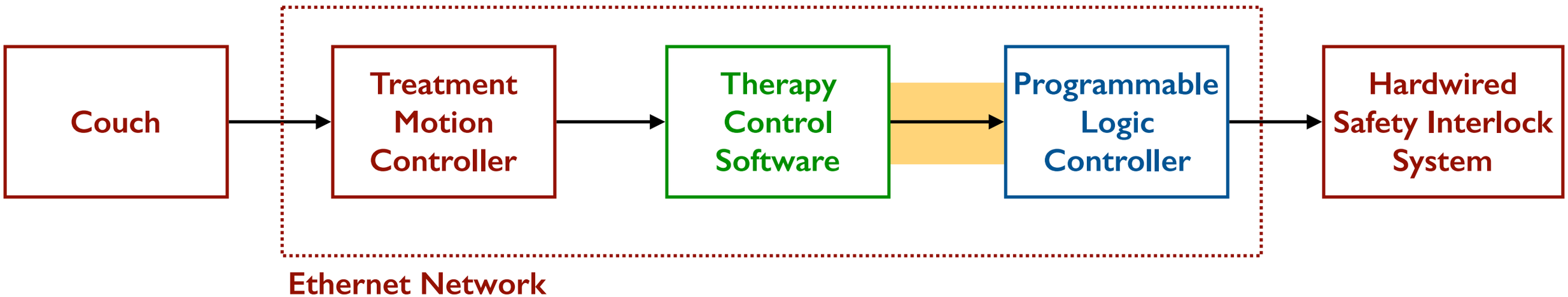
couch rotates out of tolerances and no manual override => beam shuts off

```
all r: Couch.rotation |
  (properties and
   r.angle not in Prescription.tolerance and
   no Event.GantryCouch_Turntable_Override) =>
 some Beam.state & BeamOff
```

PLC disables Therapy Sum relay => beam shuts off

```
evidence[“63c8d380", PLC_Analysis, …, Proof] =>
all relayState: plc.relay2754 & RelayOpen |
  one coilState: plc.sentMsgs & relayState.^next |
    coilState.coilNumber = Coil1623
    coilState.coilValue = False
```

Generating evidence for couch safety



Expert Review Validator

EPICS Linter

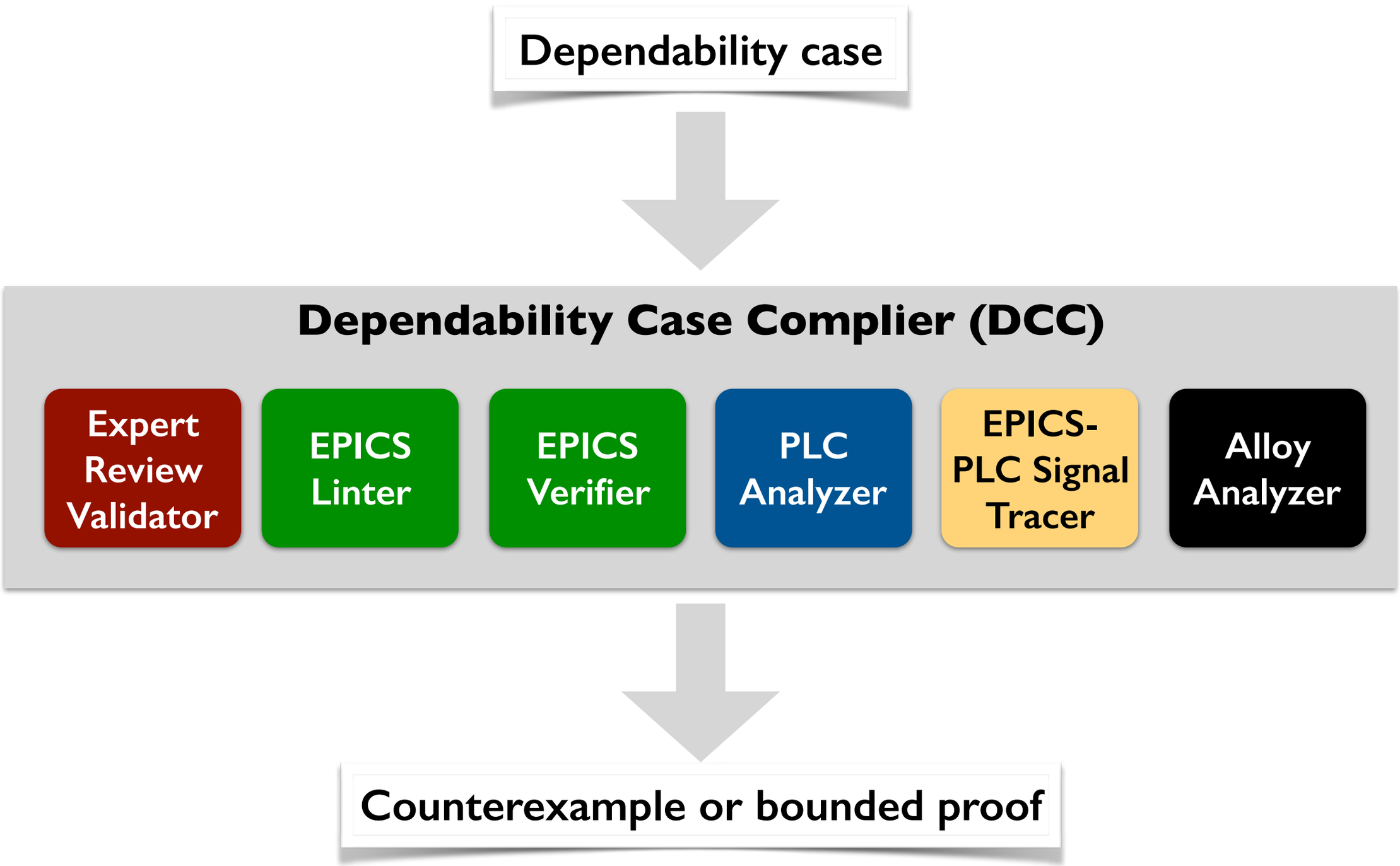
PLC Checker

A *solver-aided verifier* for the subset of EPICS used in CNTS.

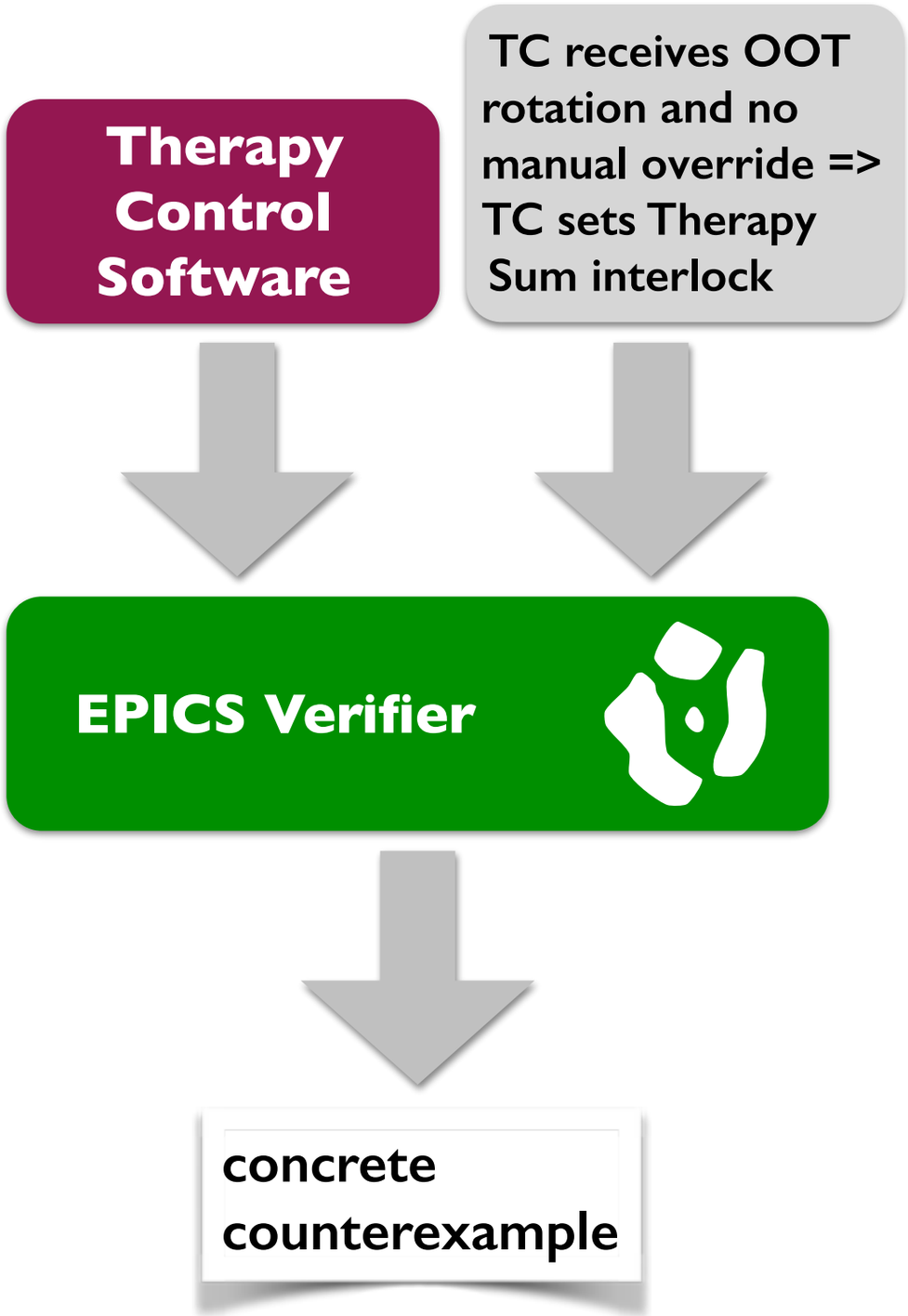
EPICS Verifier

EPICS-PLC Signal Tracer

Checking couch safety

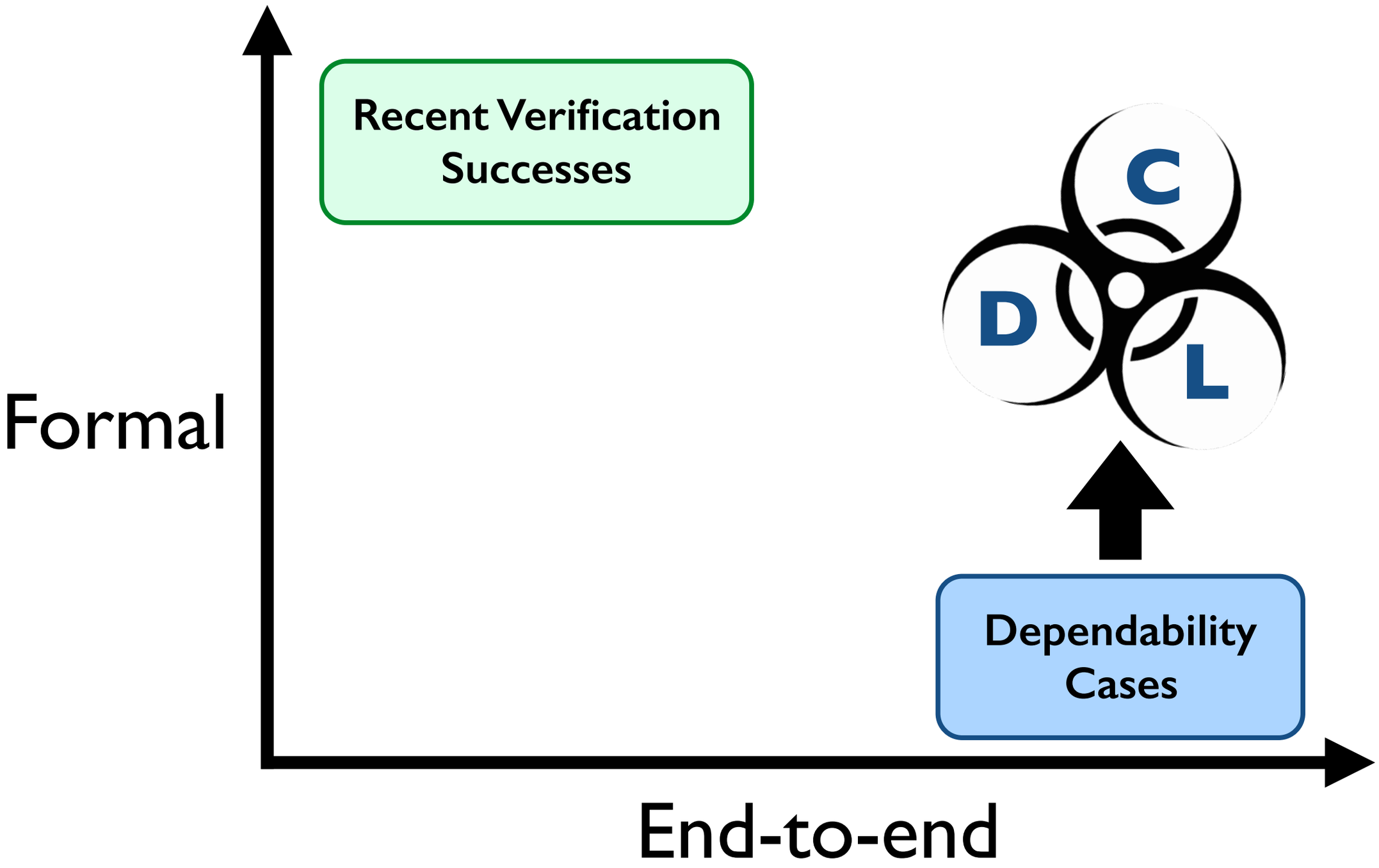


Deep analysis with <2000 LOC of tool code ...



Found a bug in the Therapy Control software (preventing beam shut off), masked by a bug in the EPICS runtime!

Thanks!


Recent Verification Successes
Formal
C
D
L
Dependability Cases
End-to-end