Improving Usability and Trust in Real-Time Verification of a Large-Scale Complex Safety-Critical System

Brian Kempa, Chris Johannsen, Kristin Y. Rozier
Iowa State University

26th Ada-Europe: Reliable Software Technologies
June 16, 2022
NASA Lunar Gateway: Assume-Guarantee Contracts

\[(CMD \equiv \text{START}) \rightarrow (\square[0,5](ActionHappens \& \square[0,2](CMD = \text{END})))\]

---

Real-time, Flight-certifiable, Embedded Runtime Verification

RESPONSIVE
REALIZABLE
UNOBTRUSIVE
Unit

R2U2
Requirements

**REALIZABILITY:**
- easy, *expressive* specification language
- *generic* interface to connect to a wide variety of systems
- *adaptable* to missions, mission stages, platforms

**RESPONSIVENESS:**
- *continuously monitor* the system
- *detect deviations* in *real time*
- *enable mitigation* or rescue measures

**UNOBTRUSIVENESS:**
- *functionality*: not change behavior
- *certifiability*: avoid re-certification of flight software/hardware
- *timing*: not interfere with timing guarantees
- *tolerances*: obey size, weight, power, telemetry bandwidth constraints
- *cost*: use commercial-off-the-shelf (COTS) components
Matching Input Specifications to Use-Cases

**Old Syntax**

```plaintext
a0 & (a1 & !a2 & !a3) || // AGC:
  (!a1 & a2 & !a3) || // TRUE
  (!a1 & !a2 & a3));

!a0; // AGC: INACTIVE
a0 & (!a1 & !a2 & !a3) || // AGC:
  (!a1 & a2 & !a3) || // FALSE
  (!a1 & !a2 & a3));

a0 = bool(s0) == 1;
a1 = bool(s1) == 1;
a2 = bool(s2) == 1;
a3 = bool(s3) == 1;
```

**New Syntax**

```plaintext
RVALID: resRactive => resRvalid;

taskAactive = bool(Aactive) == 1;
taskBactive = bool(Bactive) == 1;
taskCactive = bool(Cactive) == 1;
resRactive = bool(Ractive) == 1;
resRvalid =
  exactly-one-of(active_tasks) == 1;

active_tasks = {taskAactive,
               taskBactive,
               taskCactive};
```
Example: Assume-Guarantee Output

**Propositional Logic:**

\[
\begin{align*}
\text{False} & \rightarrow \text{True} \equiv \text{True} \\
\text{True} & \rightarrow \text{True} \equiv \text{True} \\
\text{True} & \rightarrow \text{False} \equiv \text{False}
\end{align*}
\]

**User-friendly:**

\[
\begin{align*}
& (\text{Assumption} = \text{False}) \rightarrow (\text{Guarantee} = \text{True}) \equiv \text{Inactive} \\
& (\text{Assumption} = \text{True}) \rightarrow (\text{Guarantee} = \text{True}) \equiv \text{True} \\
& (\text{Assumption} = \text{True}) \rightarrow (\text{Guarantee} = \text{False}) \equiv \text{False}
\end{align*}
\]
R2U2: Realizable Responsive Unobtrusive Unit

- **Data Integrity**: data is consistent, coherent, within expectations
- **Sanity Checking**: common-sense assumptions hold
- **Fault Mitigation**: real-time monitoring for fault signatures
- **Security Monitoring**: complex temporal patterns indicative of breaches
- **Mission Integration**: automatically catch misconfigured, or otherwise tenuous/faulty connections that elude system integration checks

http://r2u2.temporallogic.org/