Runtime Monitoring for the Diagnosis and Recovery of Complex Physical Systems

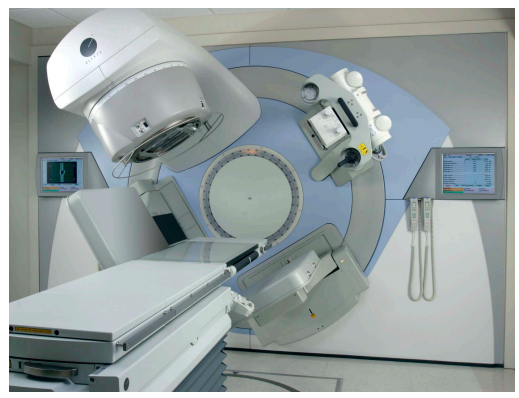
G. Pace[1], C. Colombo[1], K. Vella[1], G. Valentino[1,2], G. De Cataldo[2,3], A. Franco[4]

[1] University of Malta, Msida, Malta
[2] CERN, Geneva, Switzerland
[3] Istituto Nazionale di Fisica Nucleare (INFN), Bari, Italy
[4] Università degli Studi di Bari, Bari, Italy

Introduction

Reliability and fault tolerance in the operation of critical systems is imperative to avoid financial setbacks or even loss of lives. Despite the effectiveness of proper testing, it is extremely difficult to test huge software products in a sufficiently thorough manner to ensure their correctness. Such a system does not work in a vacuum, but in an environment for which is difficult to simulate all possible variations.

- Therac-25: a radiation therapy machine involved in 6 accidents in the 1980s.
- A 1-byte counter in a testing routine frequently overflowed..
- If the operator provided an input at that moment, a software interlock against high-power beams would fail!

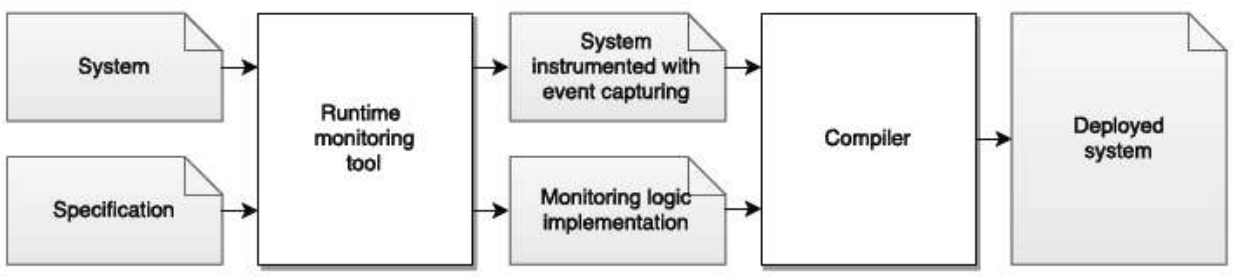


How do we ensure that our software operates correctly against a given specification?

E.g. Verify that the gas leak variable should not have been true for more than 1 minute in the last 30 min before the *induceSpark* function is called.

- **Testing,** checking the system on a number of possible inputs, does not guarantee full coverage of possible system behaviour.
- **Model checking,** the automated verification of a system against the specification does not scale up to large systems.
- **Runtime verification,** automatically weave together the specification to produce a monitored system which checks the system at runtime for correctness.

Runtime Verification



Benefits of Runtime Verification:

✓ The advantages of robust model checking techniques which scale well with large systems (checks are only done at run time).

✓ Different teams working on specification and system aspects.

✓ Can re-use the same specification across different versions, instances or systems.

✓ Avoids possibility to introduce new bugs as complexity of inline checks increases.

Potential Impact

Runtime Verification techniques have already been applied by researchers at the University of Malta to financial and telescope applications. At the moment, we are looking into the High Momentum Particle IDentification (HMPID) detector control system and ALICE-LHC interface control software, implemented in the WinCC OA environment, as use cases for Runtime Verification.

The concept could be easily extended to other large-scale High Energy Physics and medical control systems to ensure that these costly, high-profile devices operate even more safely and efficiently (e.g. reduced down time due to manual intervention needed after high-voltage trips, avoidance of catastrophic scenarios related to high-energy beams..).