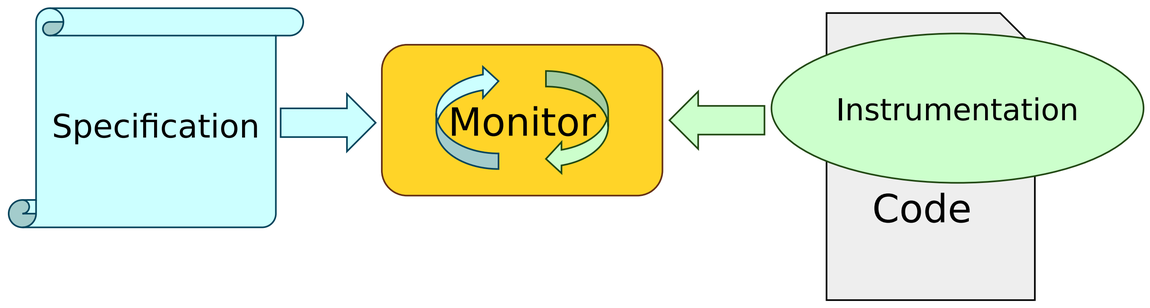
Integrating Testing with Runtime Verification for Mission-Critical Distributed Control Systems

D. Ancona*, S. Avola*, A. Ferrando†, P. Baglietto*, M. H. ter Beek‡
A. Parodi§, G. Camera¶ and M. Pinasco¶
∗University of Genova, Italy, †University of Modena and Reggio Emilia, Italy
‡ CNR–ISTI, Pisa, Italy, §M3S SrL, Italy, ¶Hitachi Rail STS SpA, Italy

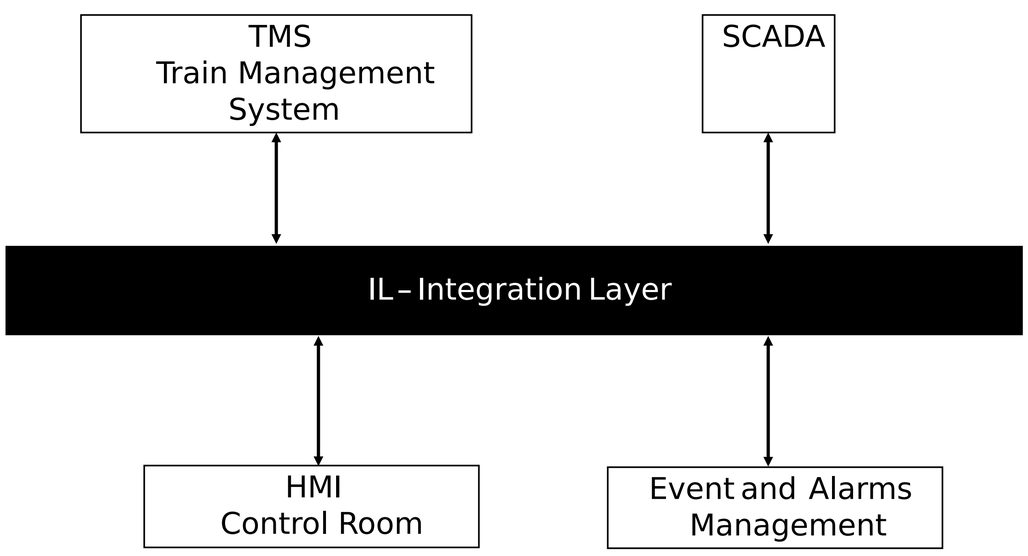
Motivation: Verification of the Integration Layer (IL) of a Distributed Control Systems is challenging.

Proposed solution: complement testing with Runtime Verification (RV) to detect non-systematic errors earlier and reduce time-to-production.

Contribution: test the IL of a real-world railway control system developed by Hitachi Railway STS), based on a Message-oriented Middleware (MoM) implementing a publish-subscribe communication protocol.



Runtime Verification




```
Main = relevant ⩥
(
CheckSubs ∧ CheckPub
NoMultipleSubs ∧ NoMultipleNewPub ∧
(subsOrRecv ⩥ SubsThenRecv) ∧
(newPubOrPub ⩥ NewPubThenPub) ∧
);
Queue<pubId, subId, topic> = let msgId; pub(pubId,
topic, msgId) ((recv | Queue<pubId, subId,
topic>) ∧ (recv >> recv(subId, topic, msgId,
pubId) all))?;
CheckSubs = notSubs* let subId, topic; subs(subId,
topic) (GenCheckSubs<subId, topic> ∧
CheckSubs)?;
GenCheckSubs<subId, topic> = notNewPub* let pubId;
newPub(pubId) ((involve(pubId, subId, topic) >>
Queue<pubId, subId, topic>) ∧
GenCheckSubs<subId, topic>)?;
NoMultipleSubs = notSubs* {let topic, subId;
subs(subId, topic)(notSubs(subId,topic)* ∧
NoMultipleSubs)}?;
SubsThenRecv = {let topic, subId; subs(subId,
topic) (recv(subId,topic)* | SubsThenRecv )}?;
```