A model of Asymmetric Replicated State Machines

Roland Kuhn @ Actyx
Daniela Marottoli @ UBA
Hernán Melgratti @ UBA
Emilio Tuosto @ GSSI

School of Informatics, Leicester

October 22, 2021

Research partly supported by the EU H2020 RISE programme under the Marie Skłodowska-Curie grant agreement No 778233

BEHAPI
Behavioural Application Program Interfaces

Take-away message

Behavioural specs for the (existing) Actyx industrial platform to develop applications for factory automation

Take-away message

Behavioural specs for the (existing) Actyx industrial platform to develop applications for factory automation

With respect to the state-of-the-art, our models

- feature
  - pub-subscribe (instead of point-to-point)
  - (generalised) choices
  - arbitrary (and variable) number of instances

Take-away message

Behavioural specs for the (existing) Actyx industrial platform to develop applications for factory automation

With respect to the state-of-the-art, our models

- feature
  - pub-subscribe (instead of point-to-point)
  - (generalised) choices
  - arbitrary (and variable) number of instances
- trade consensus for availability

Take-away message

Behavioural specs for the (existing) Actyx industrial platform to develop applications for factory automation

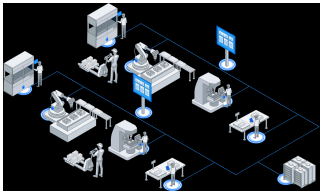
With respect to the state-of-the-art, our models

- feature
  - pub-subscribe (instead of point-to-point)
  - (generalised) choices
  - arbitrary (and variable) number of instances
- trade consensus for availability
- focus on new properties (eventual-consistency) instead of "old" ones (eg. session fidelity)

– Prelude –

[Factory automation]

Industrial scenarios



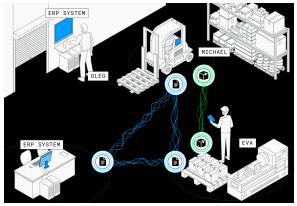
(courtesy of Actyx)

A highly collaborative environment

People + Real-time controllers + IT systems and networks:

- work divided among many autonomous production cells
- efficiency is determined by designing and controlling the flow of resource and information
- local failures must be tolerated for brief time periods

Industrial scenarios



(courtesy of Actyx)

Execution model

machine/operator/forklift/... $\mapsto$ Local Twin (state machine)

- twins are replicated where needed
- events have unique IDs and record facts (e.g. from sensors) or decisions
- state is computed from locally known log of events
- logs are replicated and merged

Challenges

Specify application-level protocols where decisions

- don't require consensus

Challenges

Specify application-level protocols where decisions

- don't require consensus
- are based on stale local states

Challenges

Specify application-level protocols where decisions

- don't require consensus
- are based on stale local states
- yet, collaboration is successful