Verifying the Reliability of Robots and Assets using Rare Failure Data

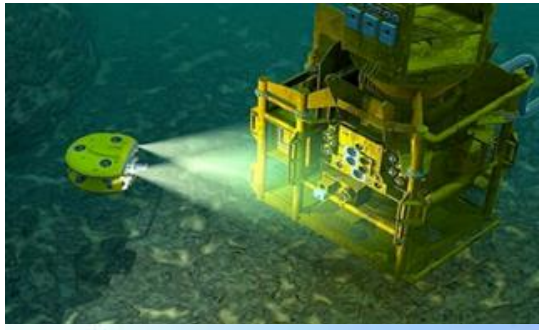
Valentin Robu

Heriot-Watt University, Edinburgh, UK

(Based on join work with Xingyu Zhao, David Flynn, Wenshuo Tang
presented at AAAI 2019, CIRED 2018, BINDT 2015)

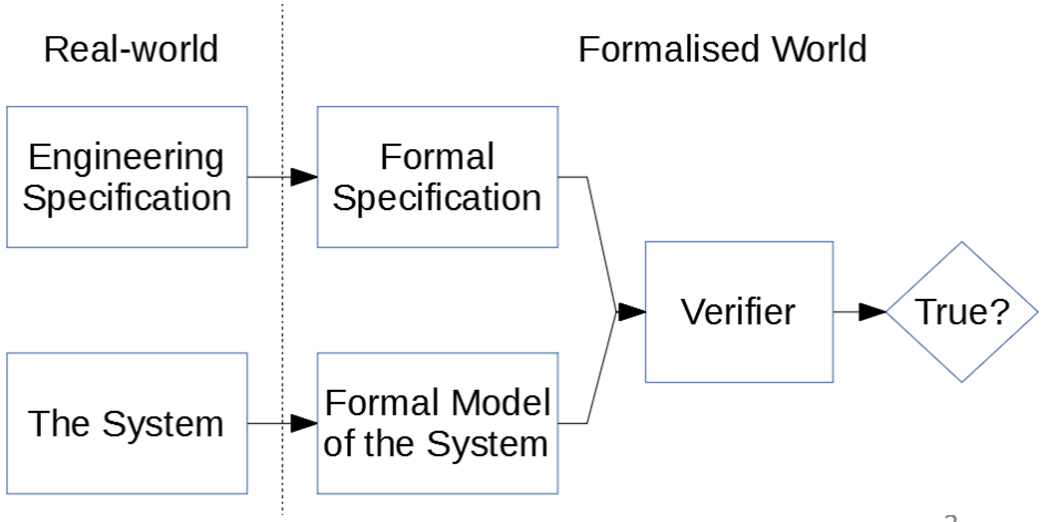
Background – Motivation

- The ORCA Hub
  - Offshore Robotics for the Certification of Assets
    - £36M, Founded by UK EPSRC, 5 Universities, https://orcahub.org/
- Extreme Environments
  - Remote and dangerous for humans
    - Communications are restricted
  - Robots need to operate autonomously under uncertainty
- Robot self-certification (WP4 – ORCA)
  - Identified as a key robotic capability [Lane et al. 2016]
    - Continuously monitor and assess the own performance during a mission



Proposed solutions

- Why runtime Probabilistic Model Checking (PMC)?
  - Probabilistic models capture inevitable domain uncertainties
    - Stochastic environments
    - Random sensors/component failures
    - Built-in algorithms making random choices
  - Quantitative properties of more interest
    - Chance of a successful mission
    - Chance of seeing a catastrophic failure
    - Expected time/energy costs



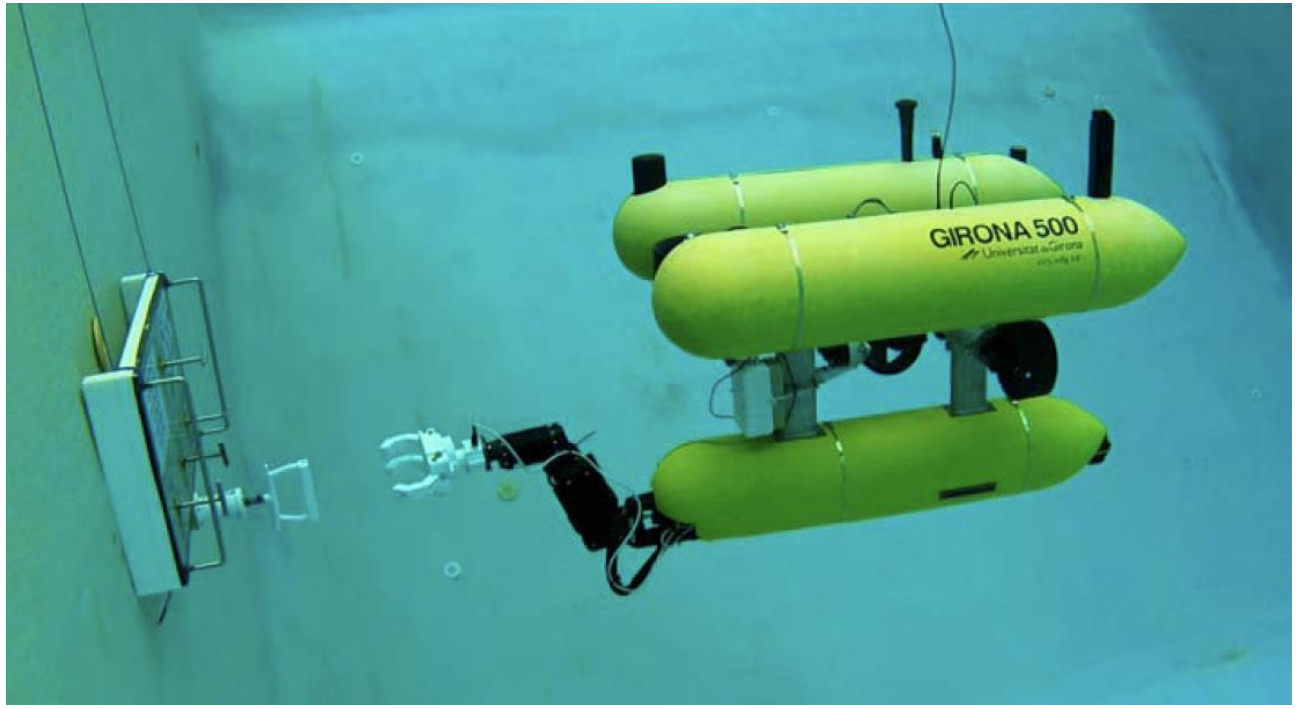
Challenges in doing probabilistic PMC

- Assuming the formal model accurately represents the real-world.
- Failure data is often too sparse to do accurate estimations, especially for catastrophic failure parameters.
  - In reality, catastrophic failure -> redesign-> renders failure data obsolete
  - **Effectively, only catastrophic failure-free data observed in practice**
  - **How to estimate a failure-rate with only failure-free data, and without being optimistic?**

- **Conservative Bayesian Inference (CBI)**
  - New Bayesian technique
  - Explored in complex software reliability, application to robotics is challenging

Robot case study

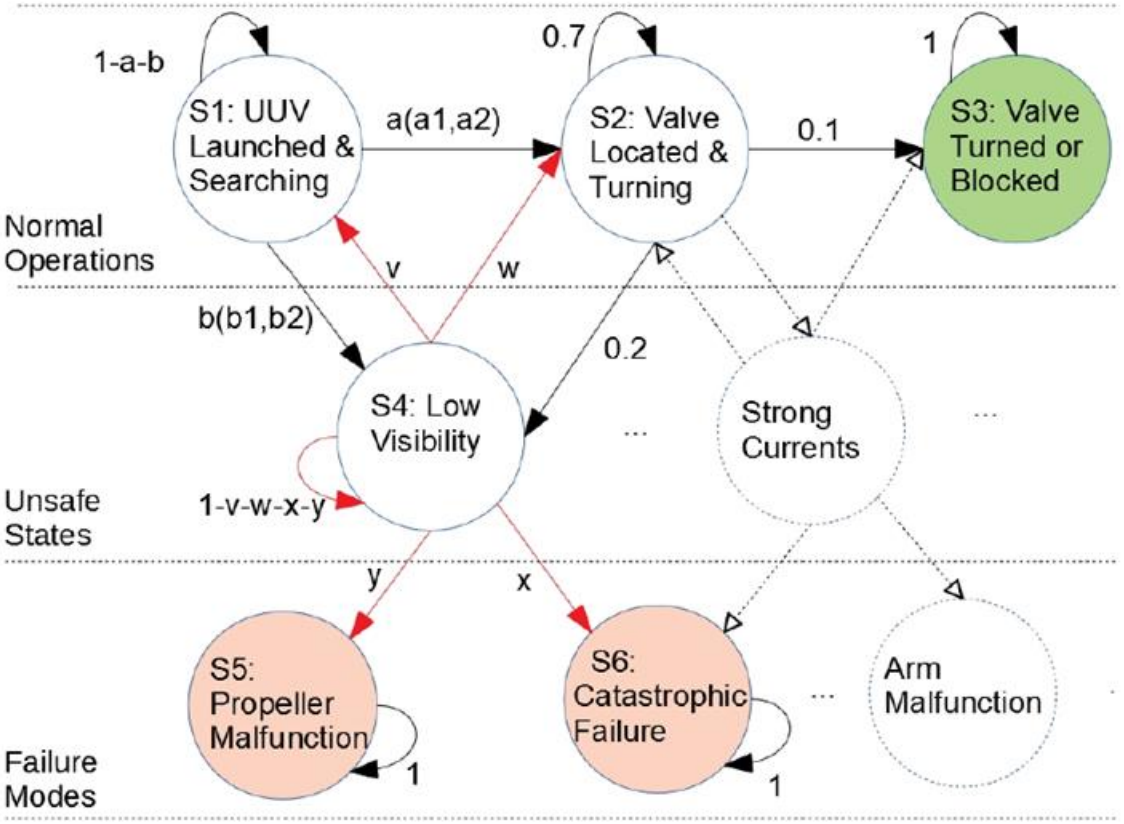
- An UUV valve turning mission
  - The UUV was built by PANDORA project (http://persistentautonomy.com/)
  - Locate a valve panel among different locations
  - Modify the valve handles to achieve different panel configurations



A generic way of structuring DTMCs

- Layered Markov model:
  - 3 layers: Normal operations, unsafe states, failure states
  - Top Layer: Probabilities from induced DTMC
  - Bottom Layer: can be informed from safety analysis methods (FMMEA, fault tree analysis)

- Development of new Bayesian estimators
  - **Conservative Bayesian Inference** for catastrophic failure related parameters:
  - Issue of of “known unknowns” vs. “unknown unknowns”



Battery Lifetime prediction

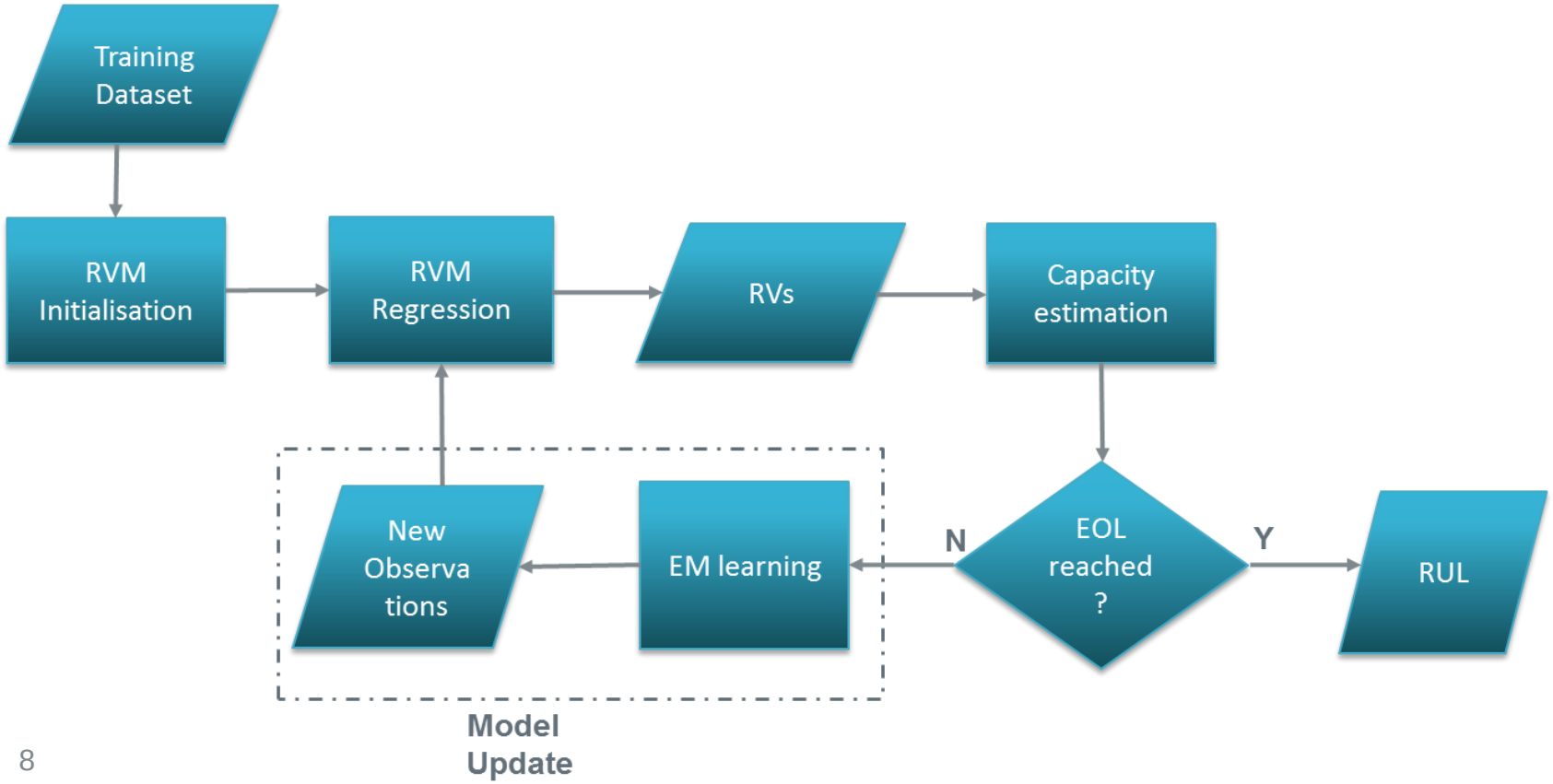
- Batteries are a critical component both for robotic autonomy, transport and grid applications (e.g. frequency response)

Hybrid Fusion Energy System (HyfeS)

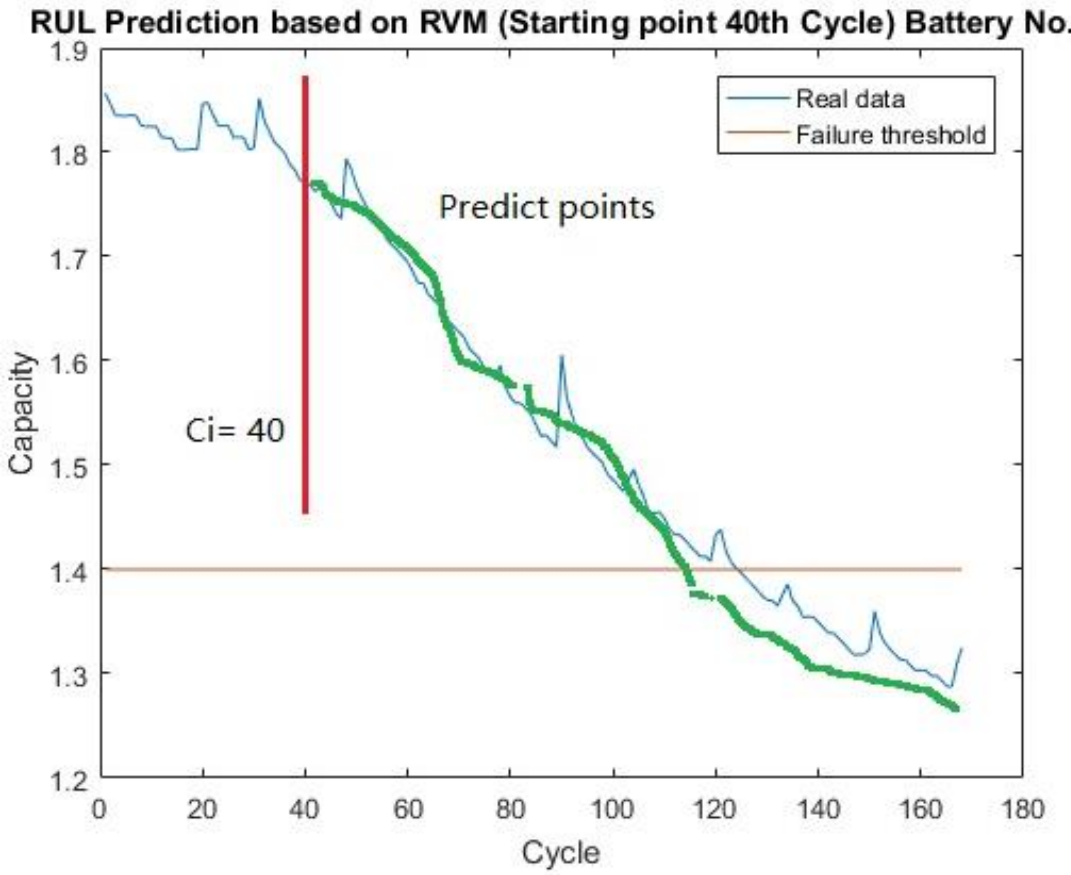
- Project looking at whole energy system optimisation of hybrid-propulsion vessels operating on the Thames in London
- Different assets:
  - Diesel engines
  - **Li-ion batteries (propulsion)**
  - Lead acid batteries

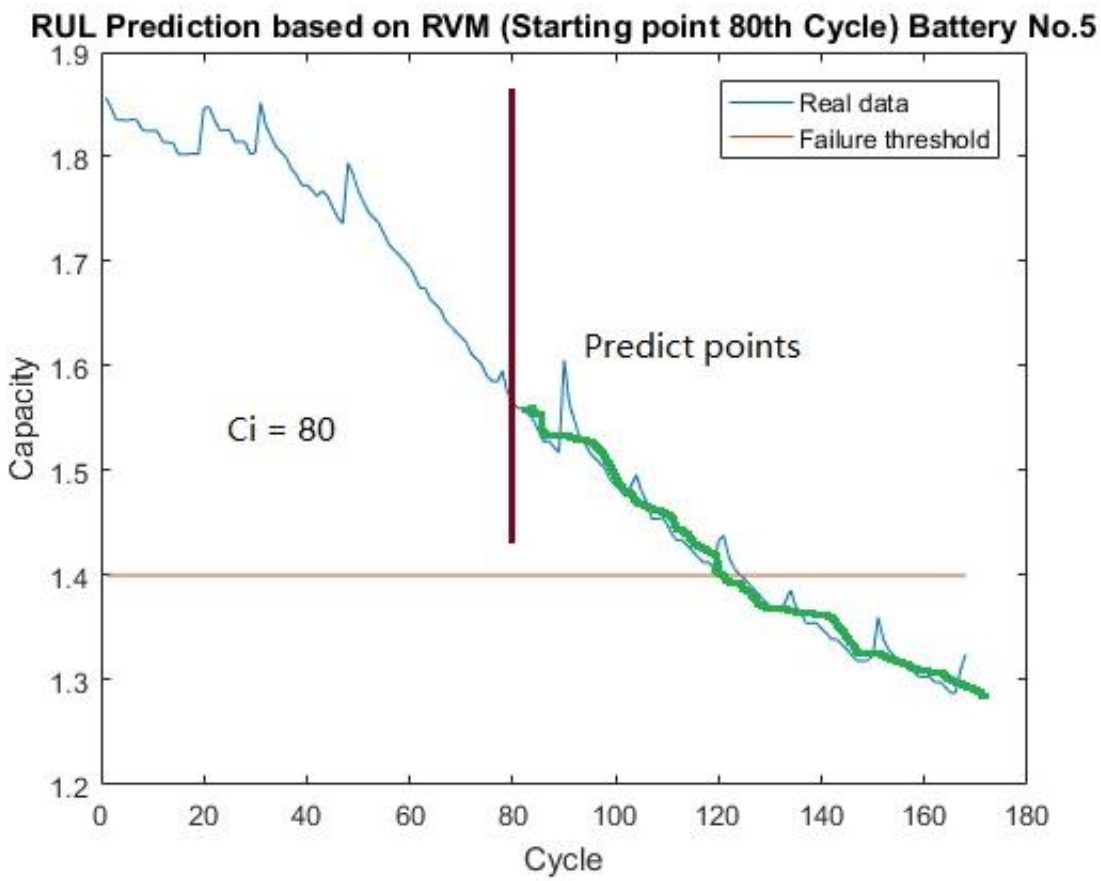
Battery Remaining Useful Lifetime Prediction

- Open-source dataset of 34 Li-ion batteries (4 cells/battery) by ***NASA Ames Prognostics Data Repository***
- Life cycle tests for several experimental conditions
- Application of **Relevance Vector Machines (RVM)** algorithm



RVM prediction curve at different starting points





C.f: Merlinda Andoni, Wenshuo Tang, Valentin Robu David Flynn (CIRED 2017)