An Open Framework for Deploying Experimental SCADA Testbed Networks

Peter Maynard, Kieran McLaughlin, and Sakir Sezer

August, 2018

Queen's University Belfast « CSIT

Outline

- Background
- High-Level Overview of Framework
- Tooling
- Ongoing/Future Work

About Myself

- Research Assistant, at Queen's University Belfast, CSIT
  - PhD 4 years ICS Network-IDS
- Research Engineer, at Southampton University, UK
  - 5G Networks
- Computer Science BSc, at Aberystwyth University, UK

Introduction

- Framework for creating virtualised SCADA networks
- Developed for packet generation for NIDS
- Open Source (GPLv3)

Related Work

- IDS networking datasets (e.g. KDD'99)
- Lack of reproducible ICS/SCADA testbeds
- Lack of IEC 60870-5-104 protocol support

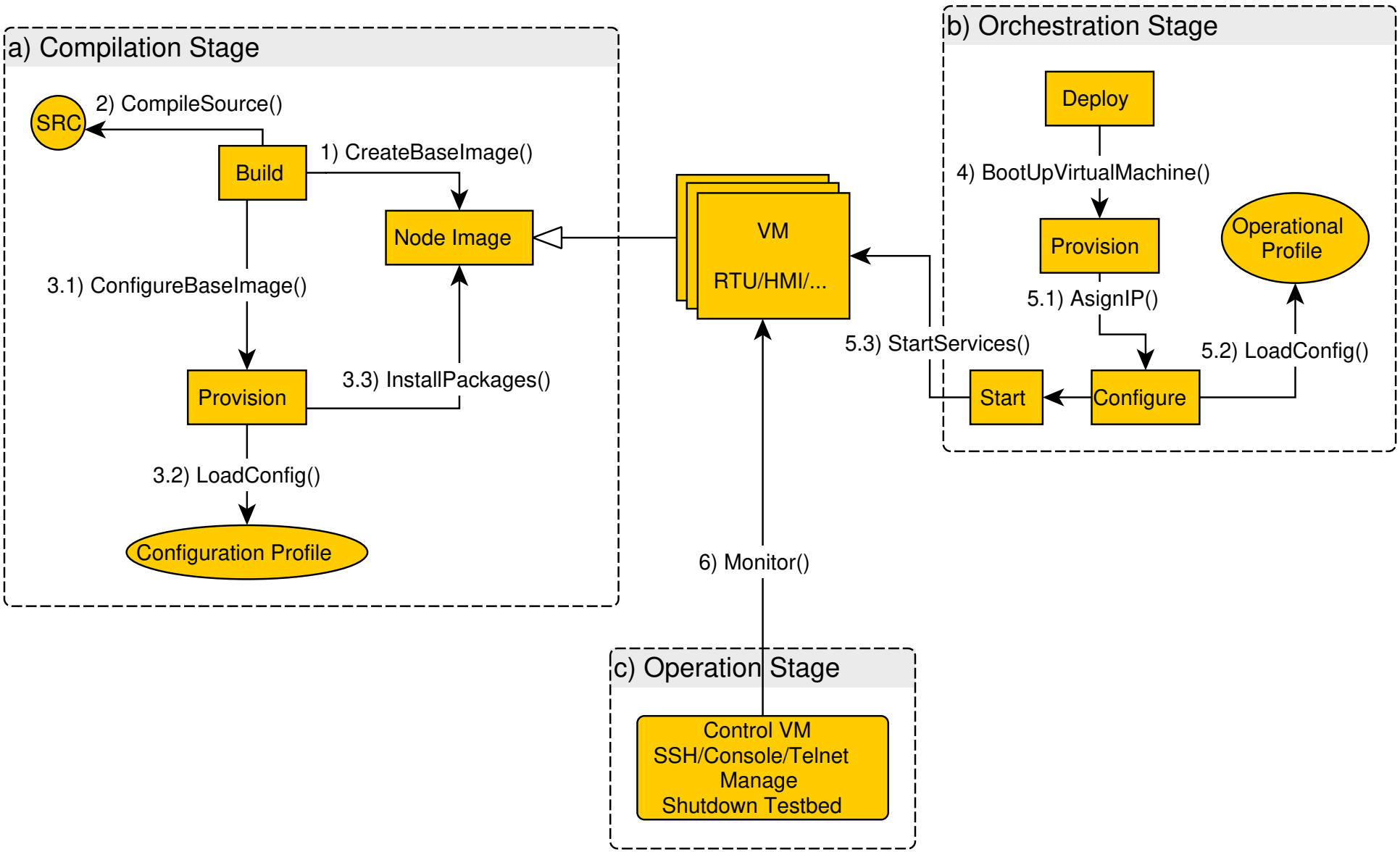
Use Cases TestBed

- Packet Generation
- Attack Simulations
- Agent Benchmarking
- Extending Limited Hardware

Requirements of a TestBed

- Reproducible
- Scalability
- Domain Fidelity
- Process Simulation
- Network Emulation
- Physical Network
- Physical Devices
- Multi-Protocol

High-Level Overview of Framework



Tooling


OPC
FOUNDATION


spring
by Pivotal


VAGRANT

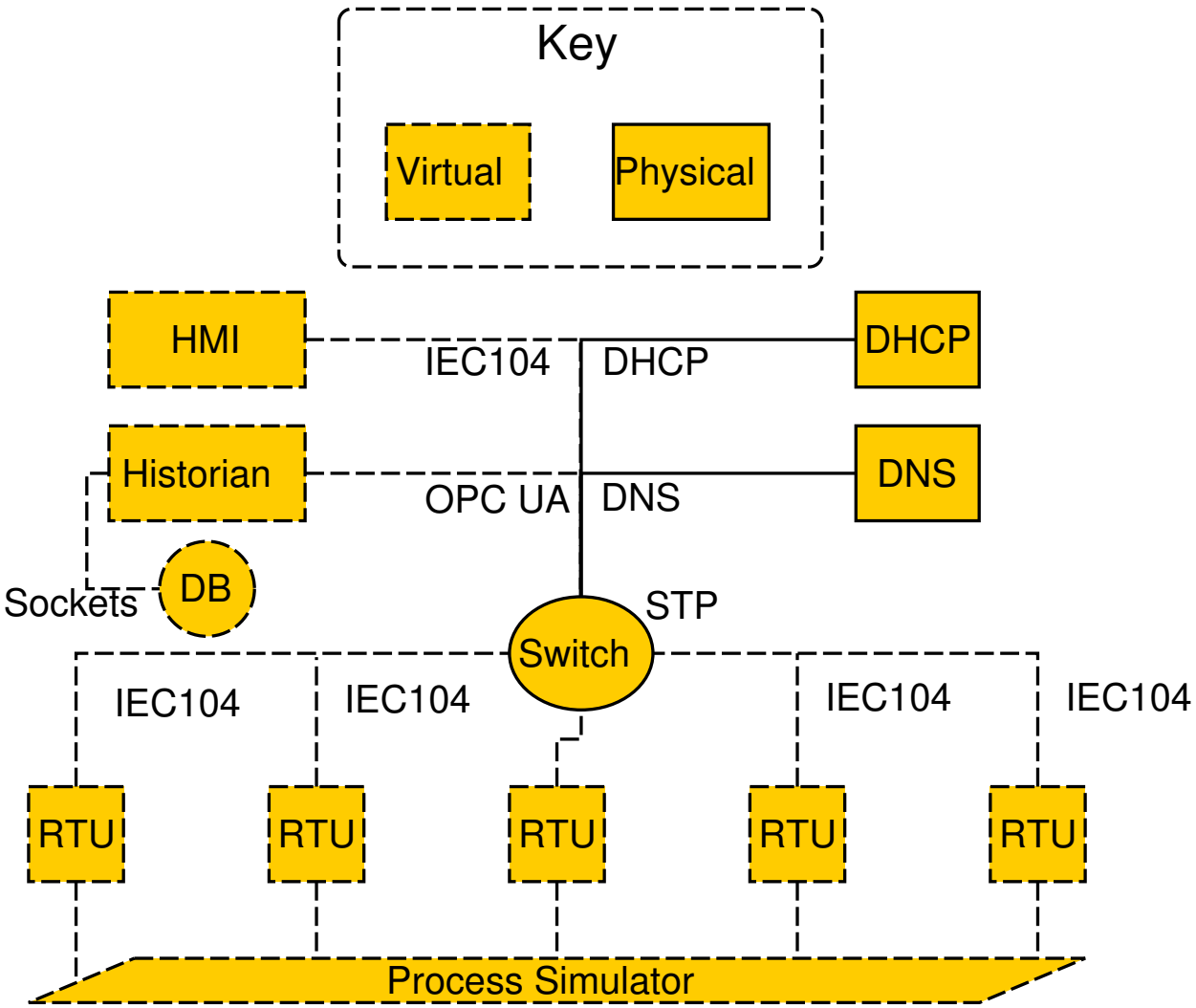

openMUC


ANSIBLE


JAVA™


Maven™

Example Network



Dataset

Host	IP	IEC104	OPC-UA	Other	**Total**
HMI	10.50.50.150	26,158	0	17,688	43,846
Historian	10.50.50.151	0	14,695	14,927	29,622
RTU-1	10.50.50.101	3,592	2,940	5,543	12,075
RTU-2	10.50.50.102	3,665	2,941	5,876	12,482
RTU-3	10.50.50.103	3,668	2,940	5,793	12,404
RTU-4	10.50.50.104	3,690	2,940	5,771	12,404
RTU-5	10.50.50.105	3,576	930	7,933	12,442
MITM	10.50.50.99	2,390	0	3,449	5,839
SCAN	10.50.50.3	15	0	28,351	28,366

- Network Reconnaissance
- IEC104 Command Injection
- 192K Packet Dataset

Ongoing Work

- Integration Process Simulators
- Implementing additional operation/configuration profiles
- Simplify deployment
- Expand documentation

Future Work

- Testbed Federation
- Auto configuration of networking equipment
- Amazon Web Services (AWS) and Google Compute Engine
- Experimentation with alternative network paradigms

End

- **www:**
  petermaynard.co.uk
- **twitter:**
  @pgmaynad
- **email:**
  p.maynard@qub.ac.uk
- **git:**
  https://github.com/PMaynard/ICS-TestBed-Framework
- **dataset:**
  https://dx.doi.org/10.6084/m9.figshare.6133457.v1