UNIVERSITÄT ZU LÜBECK
INSTITUTE FOR SOFTWARE ENGINEERING
AND PROGRAMMING LANGUAGES

isp

Runtime Verification for Interconnected Medical Devices

Martin Leucker Malte Schmitz Danilo à Tellinghusen
{leucker,schmitz,tellinghusen}@isp.uni-luebeck.de

Institute for Software Engineering and Programming Languages,
University of Lübeck, Germany

7th International Symposium on Leveraging Applications of
Formal Methods, Verification and Validation

Outline

1. Interconnection of Medical Devices

2. Runtime Verification for Medical Devices

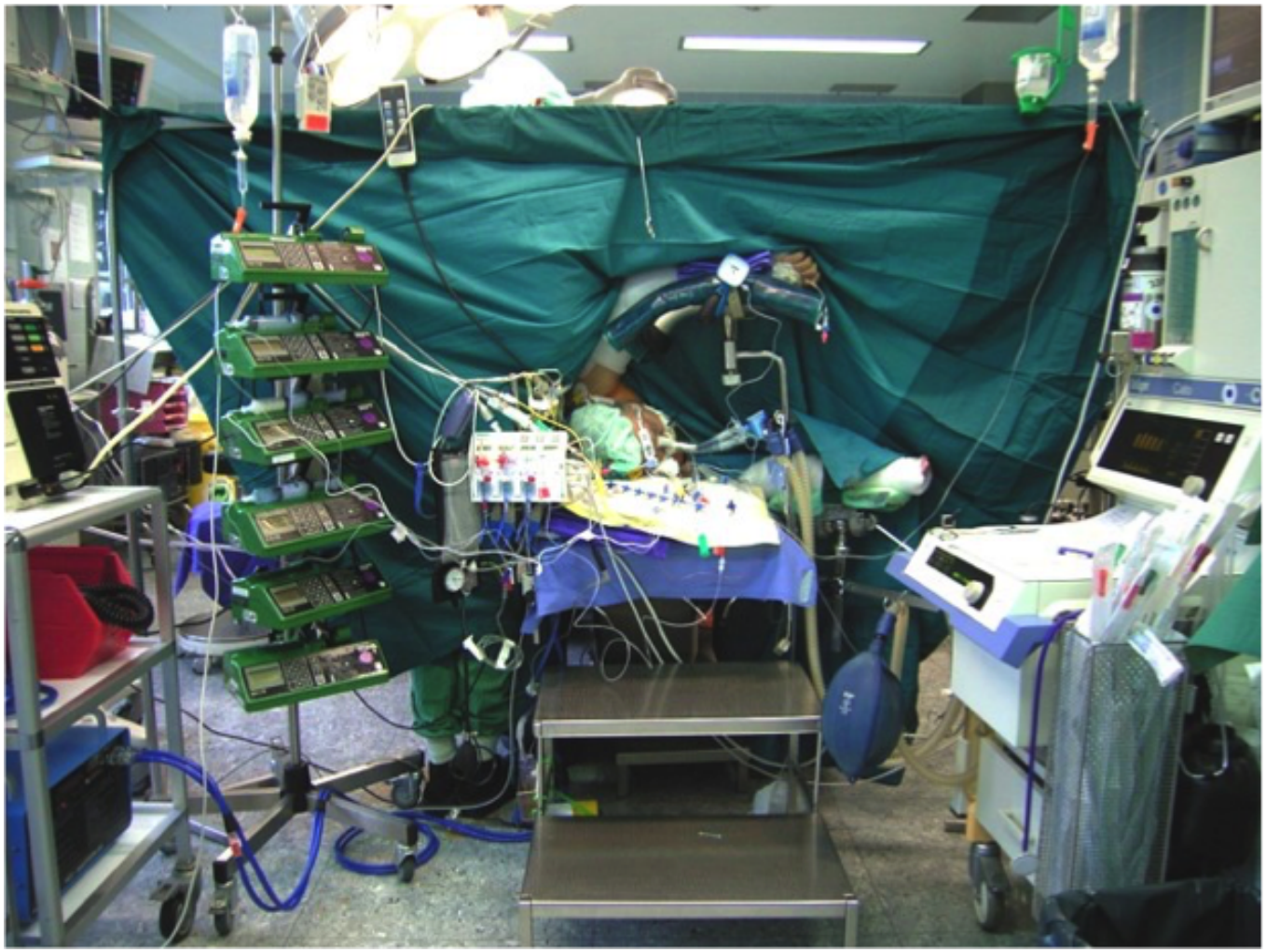
3. Device Modeler
   Risk Analysis through Contract Enforcement

4. Swiss Army Knife
   Interconnection Debugging Tool

Operation Room 1956

Bundesarchiv, Bild 183-35598-0002
Foto: Höhne, Erich; Pohl, Erich | 17. Januar 1956

Operation Room 2016



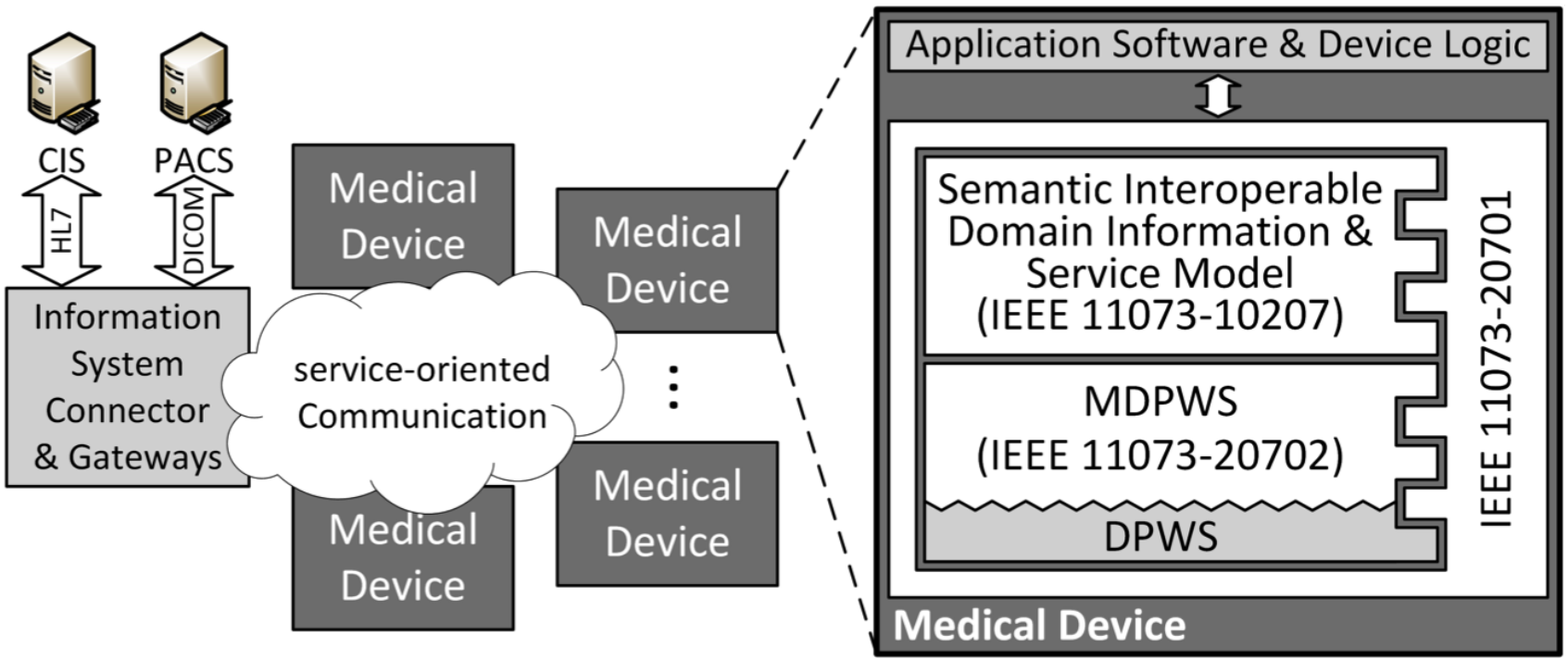
Safe Interconnection of Medical Devices

Upcoming IEEE 11073-SDC standard

- Interconnect medical devices in the operation room.
- Dynamic interconnection of devices from different manufacturers.
- Devices announce themselves in network with an interface description.

IEEE 11073-SDC

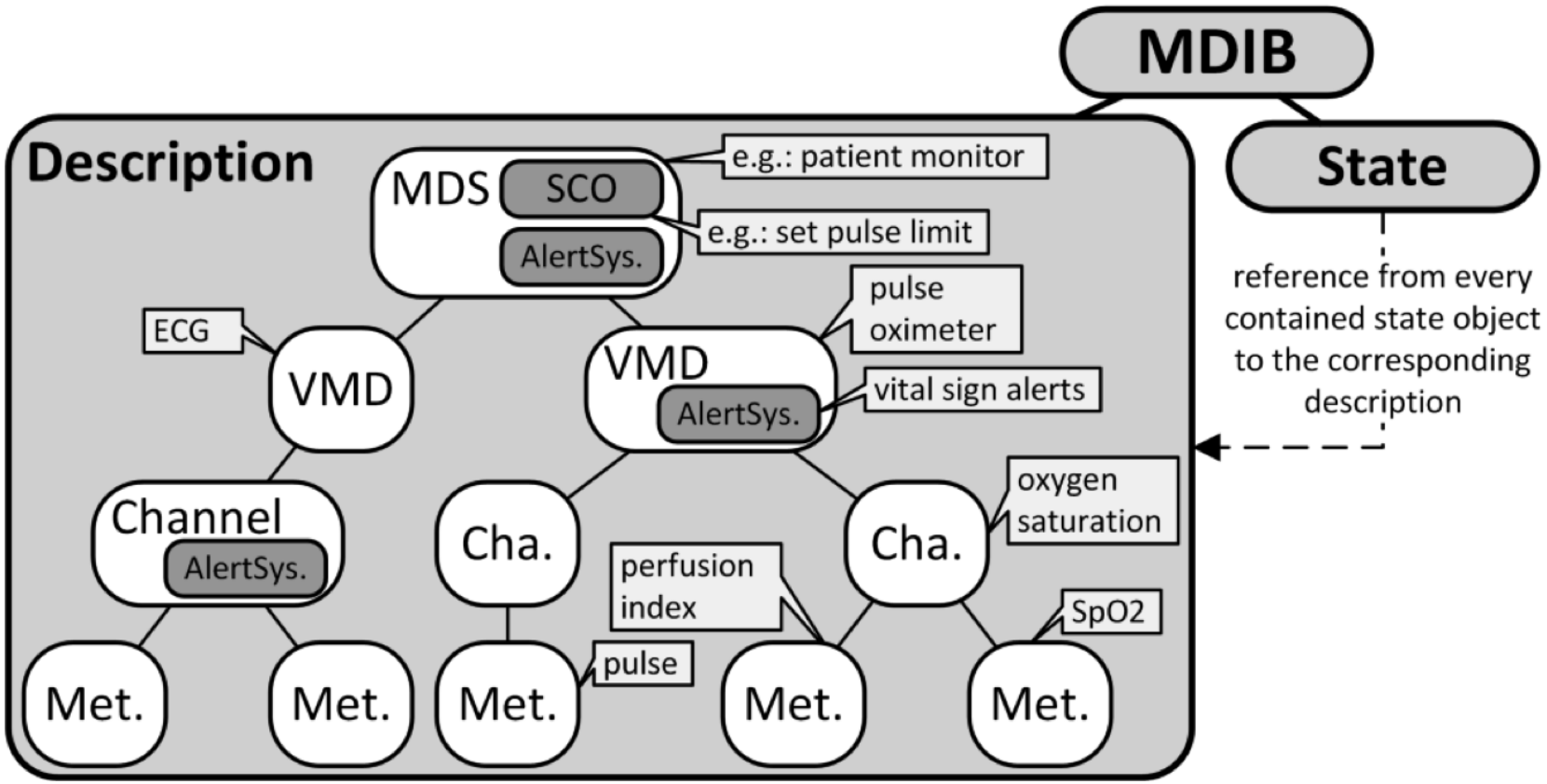
Open Surgical Communication Protocol (OSCP)



Source: Martin Kasparick, Stefan Schlichting, Frank Golatowski, Dirk Timmermann:
New IEEE 11073 standards for interoperable, networked point-of-care Medical Devices. EMBC 2015

IEEE 11073-10207

Semantic Interoperable Domain Information & Service Model



Source: Martin Kasparick, Stefan Schlichting, Frank Golatowski, Dirk Timmermann:
New IEEE 11073 standards for interoperable, networked point-of-care Medical Devices. EMBC 2015

Risk Analysis

- European Medical Device Directive demands execution of risk management.
- How to do risk management for dynamic interconnection?

Risk Analysis: Contract Enforcement

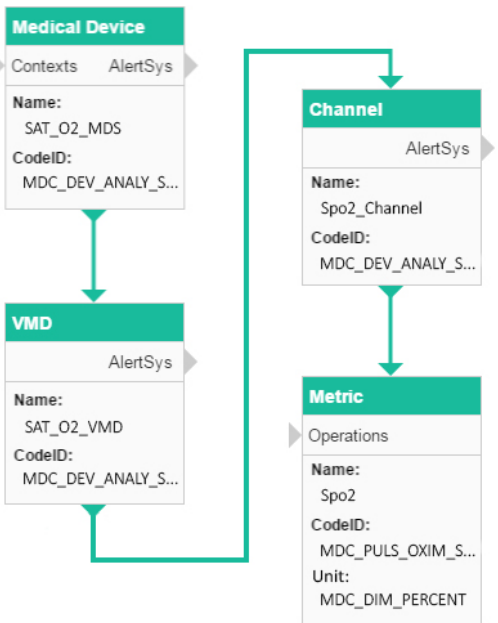
- European Medical Device Directive demands execution of risk management.
- How to do risk management for dynamic interconnection?

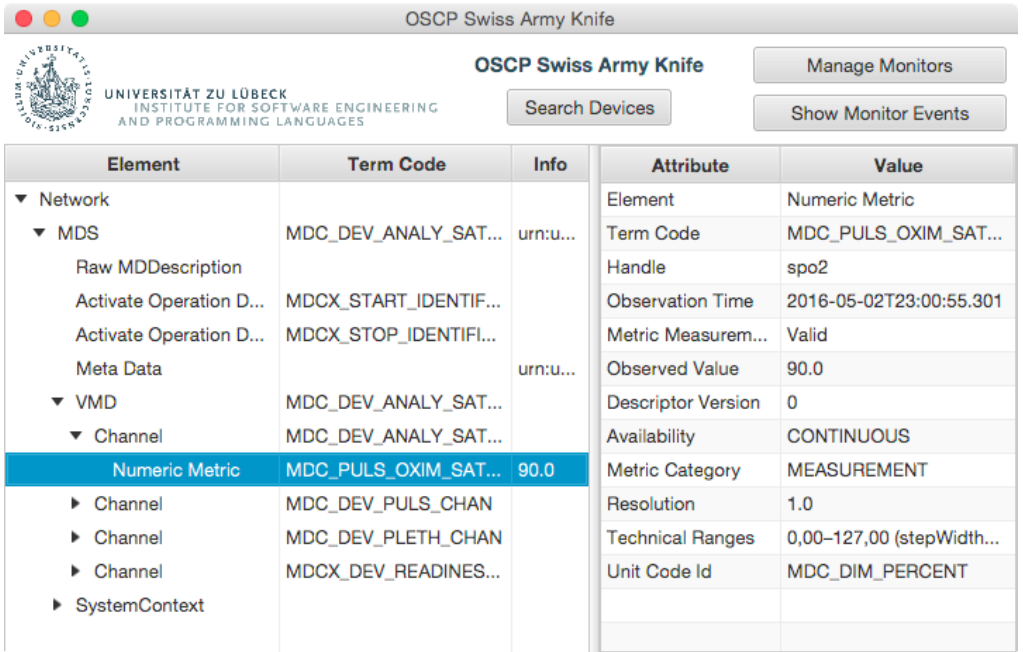
Embedded monitors check at runtime that

- the device itself and
- other devices controlling it

satisfy the interface description.

Our Tools

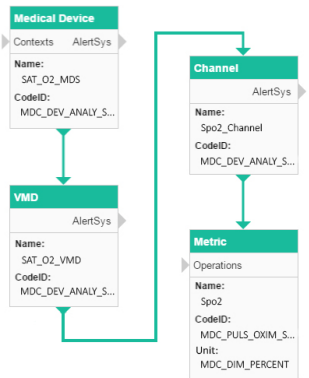

Medical Device
Contexts
AlertSys
Name:
SAT_O2_MDS
CodeID:
MDC_DEV_ANALY_S...
VMD
AlertSys
Name:
SAT_O2_VMD
CodeID:
MDC_DEV_ANALY_S...
Channel
AlertSys
Name:
Spo2_Channel
CodeID:
MDC_DEV_ANALY_S...
Metric
Operations
Name:
Spo2
CodeID:
MDC_PULS_OXIM_S...
Unit:
MDC_DIM_PERCENT


OSCP Swiss Army Knife
UNIVERSITÄT ZU LÜBECK
INSTITUTE FOR SOFTWARE ENGINEERING
AND PROGRAMMING LANGUAGES
OSCP Swiss Army Knife
Manage Monitors
Search Devices
Show Monitor Events
Element
Term Code
Info
Network
MDS
MDC_DEV_ANALY_SAT...
urn:u...
Raw MDDescription
Activate Operation D...
MDCX_START_IDENTIF...
Activate Operation D...
MDCX_STOP_IDENTIFI...
Meta Data
urn:u...
VMD
MDC_DEV_ANALY_SAT...
Channel
MDC_DEV_ANALY_SAT...
Numeric Metric
MDC_PULS_OXIM_SAT...
90.0
Channel
MDC_DEV_PULS_CHAN
Channel
MDC_DEV_PLETH_CHAN
Channel
MDCX_DEV_READINES...
SystemContext
Attribute
Value
Element
Numeric Metric
Term Code
MDC_PULS_OXIM_SAT...
Handle
spo2
Observation Time
2016-05-02T23:00:55.301
Metric Measurem...
Valid
Observed Value
90.0
Descriptor Version
0
Availability
CONTINUOUS
Metric Category
MEASUREMENT
Resolution
1.0
Technical Ranges
0,00–127,00 (stepWidth...
Unit Code Id
MDC_DIM_PERCENT

Our Tools

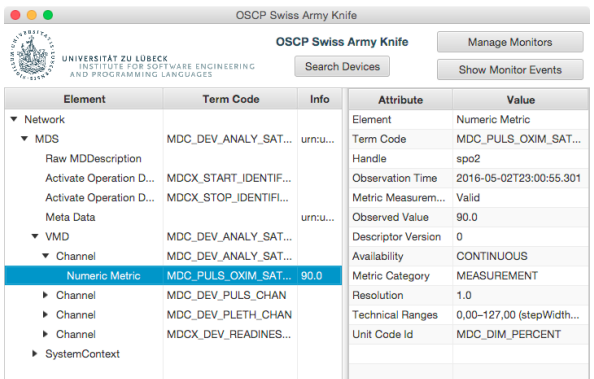
Device Modeler

- Model the device containment tree including constraints for metrics
- Generate network interface code including runtime monitors



Swiss Army Knife

- Debug devices in network and manipulate them through SCO
- Specify constraints for metrics and execute monitors checking those



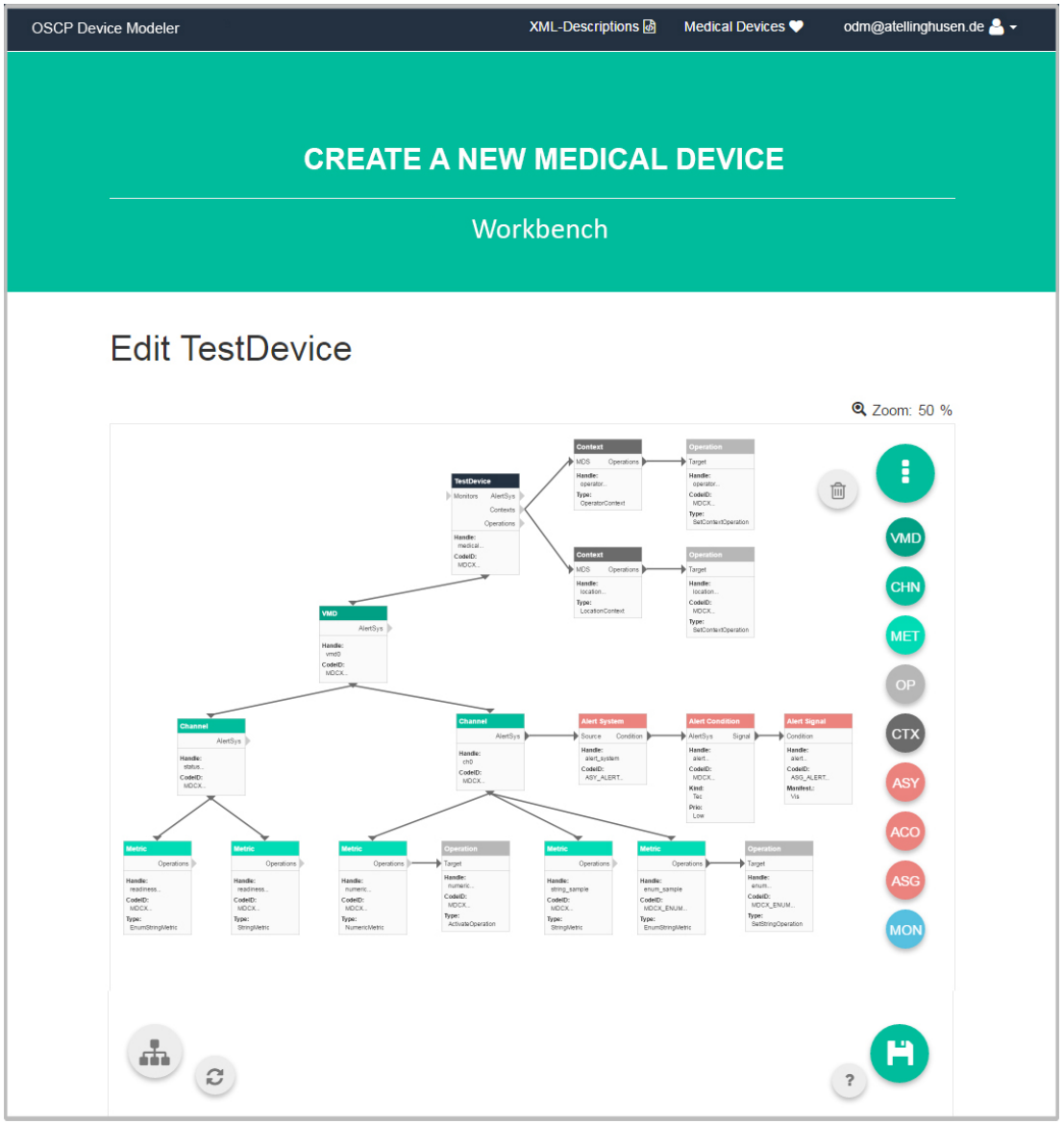
Specifying Temporal Properties

- Specify temporal behavior of metric's observed value, invocation state, ...
- Smart Assertion Logic for Temporal Logic (SALT, Bauer, Leucker, Streit 2006) ...
- Impartial Anticipation using LTL_3 Semantics (Bauer, Leucker, Schallhart 2011)

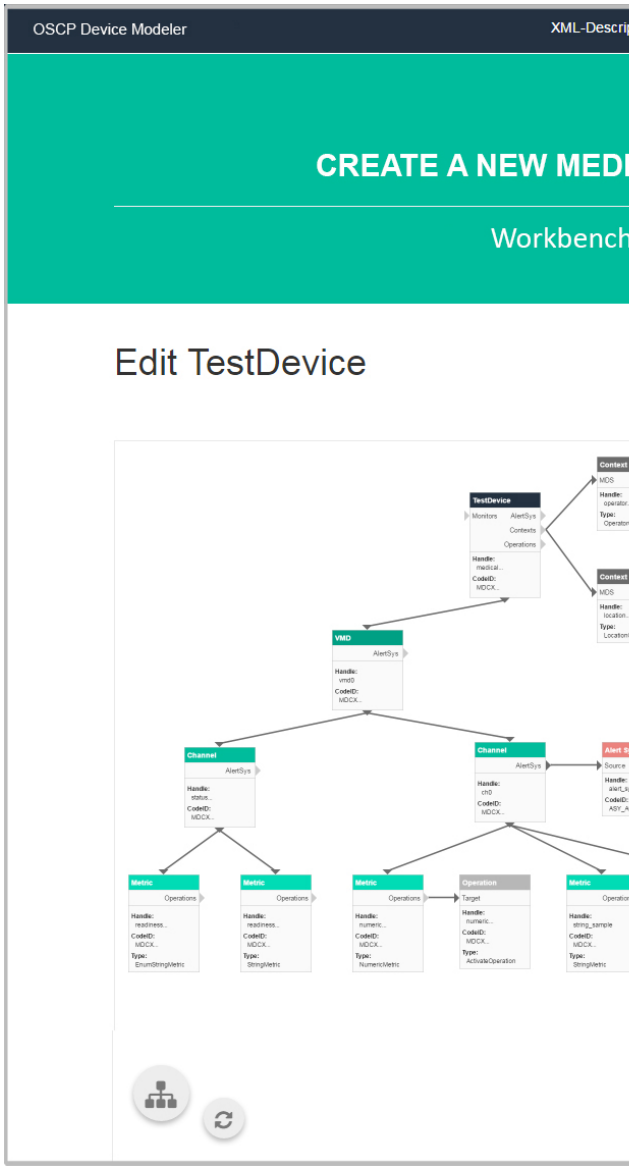
Example

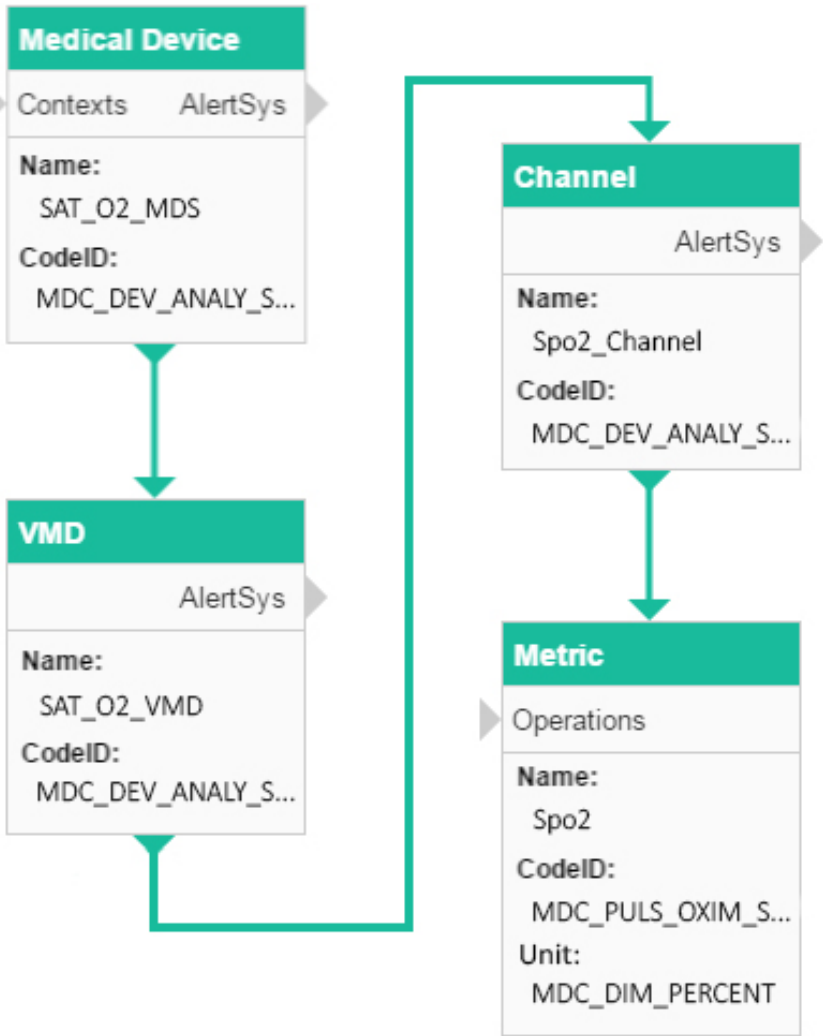
```
assert "brightness.value < 70"
  until "readiness_state.value = 'READY'"
```

OSCP Device Modeler Workbench

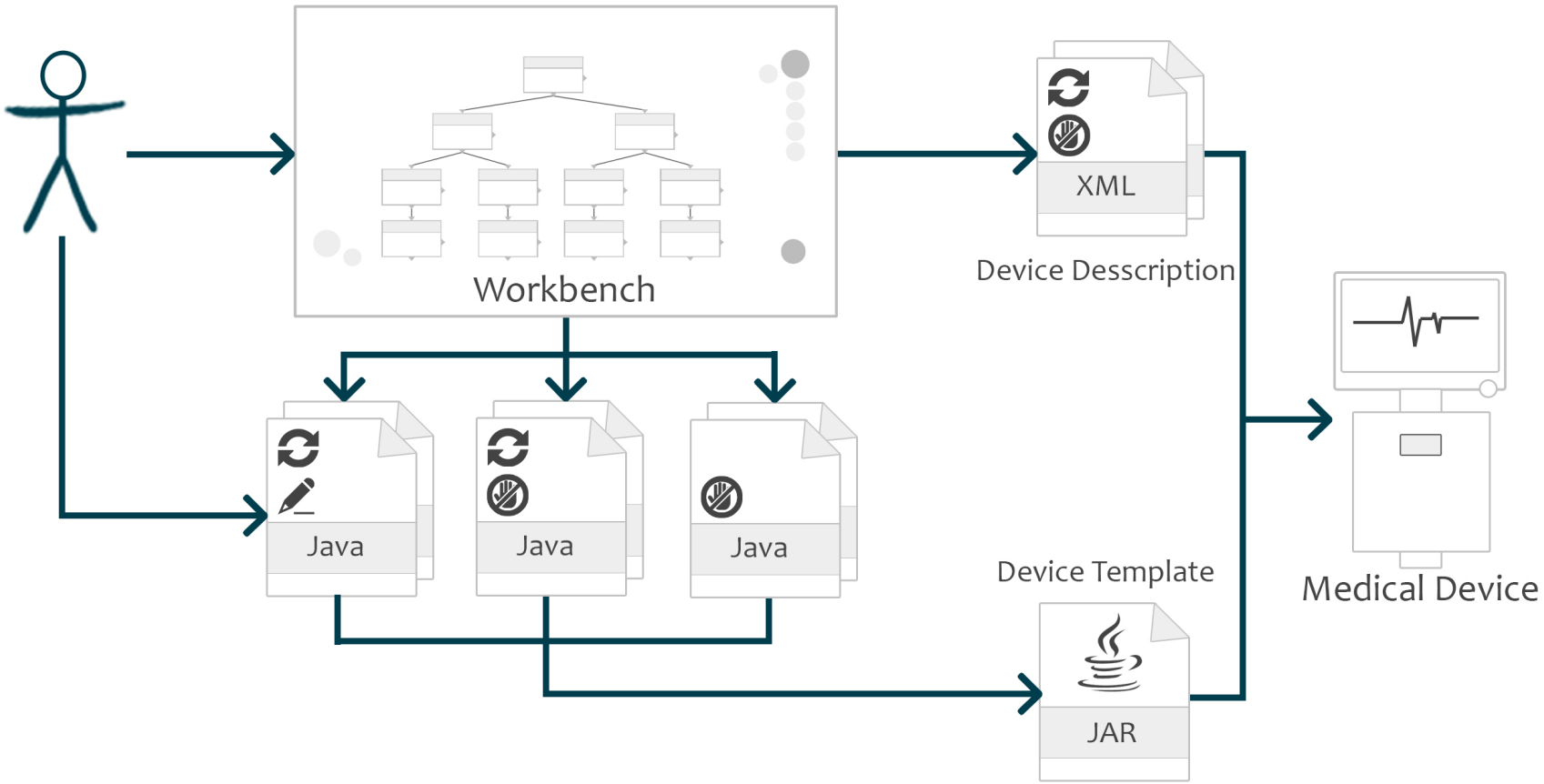


OSCP Device Modeler Workbench

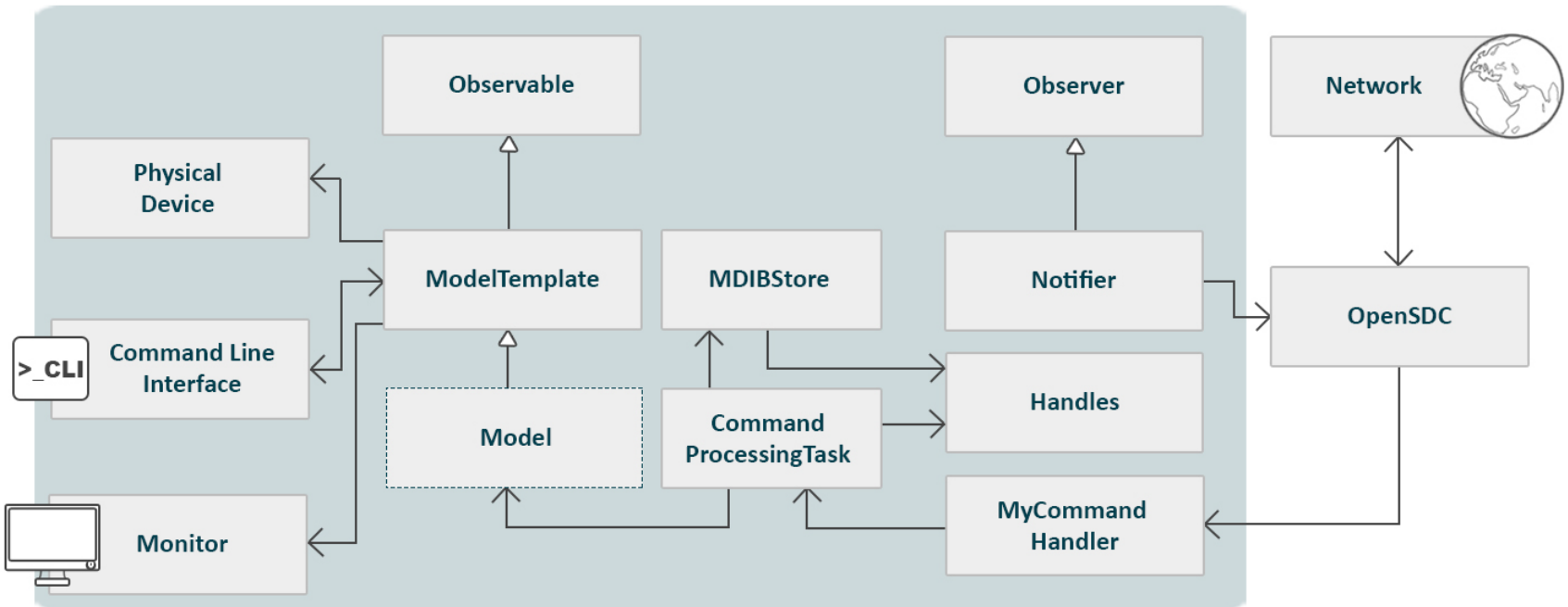




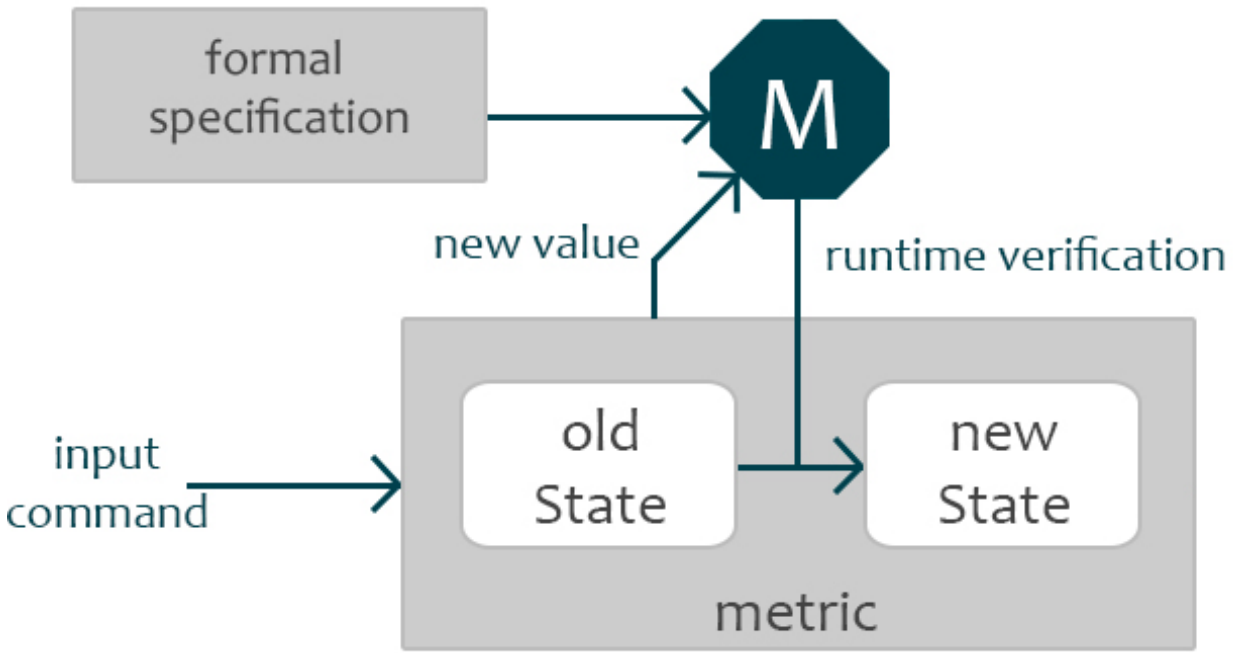
OSCP Device Modeler



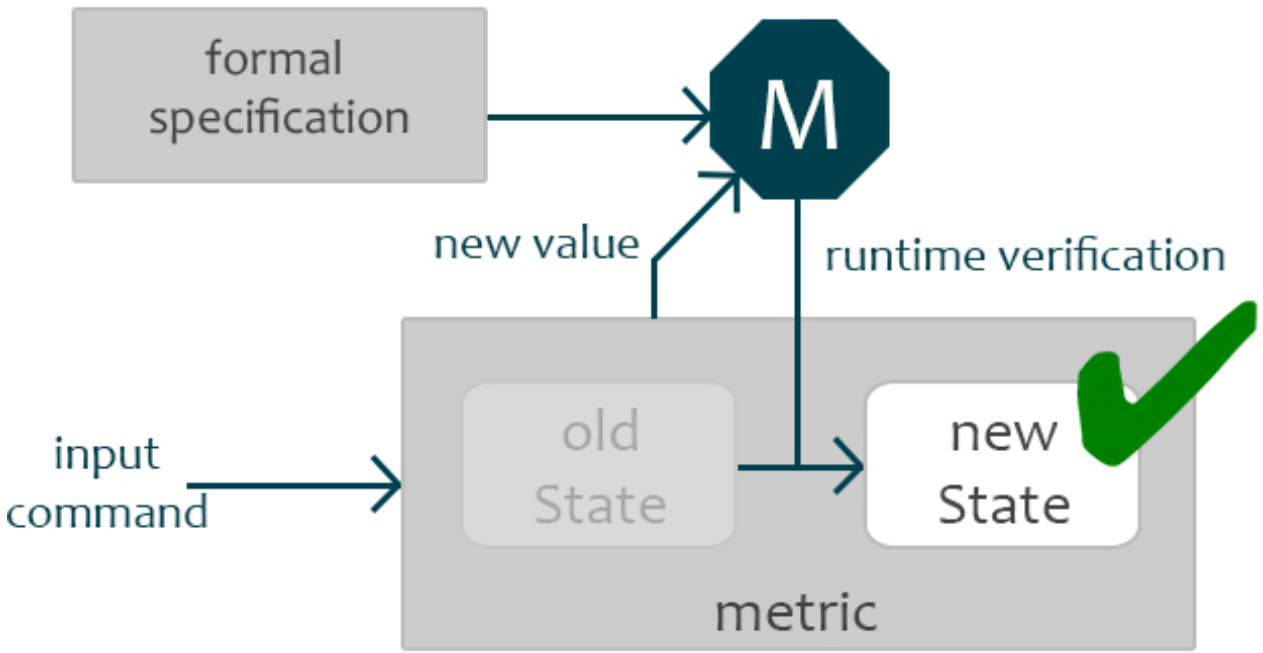
OSCP Device Architecture



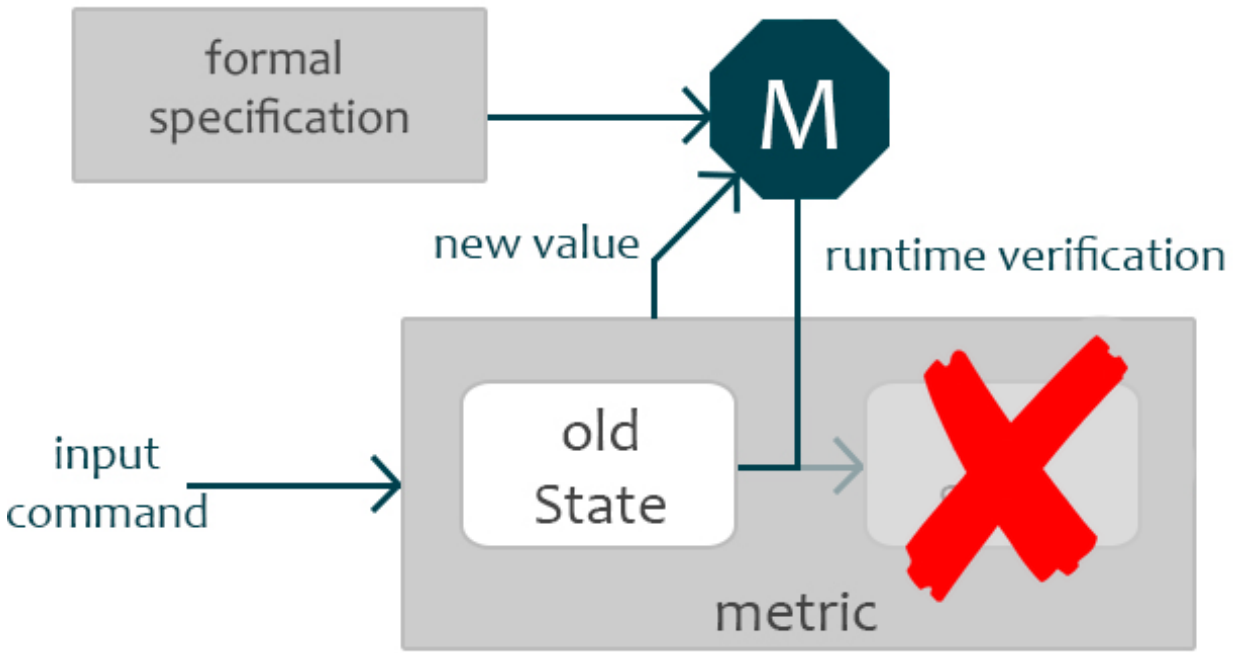
OSCP Device Monitoring



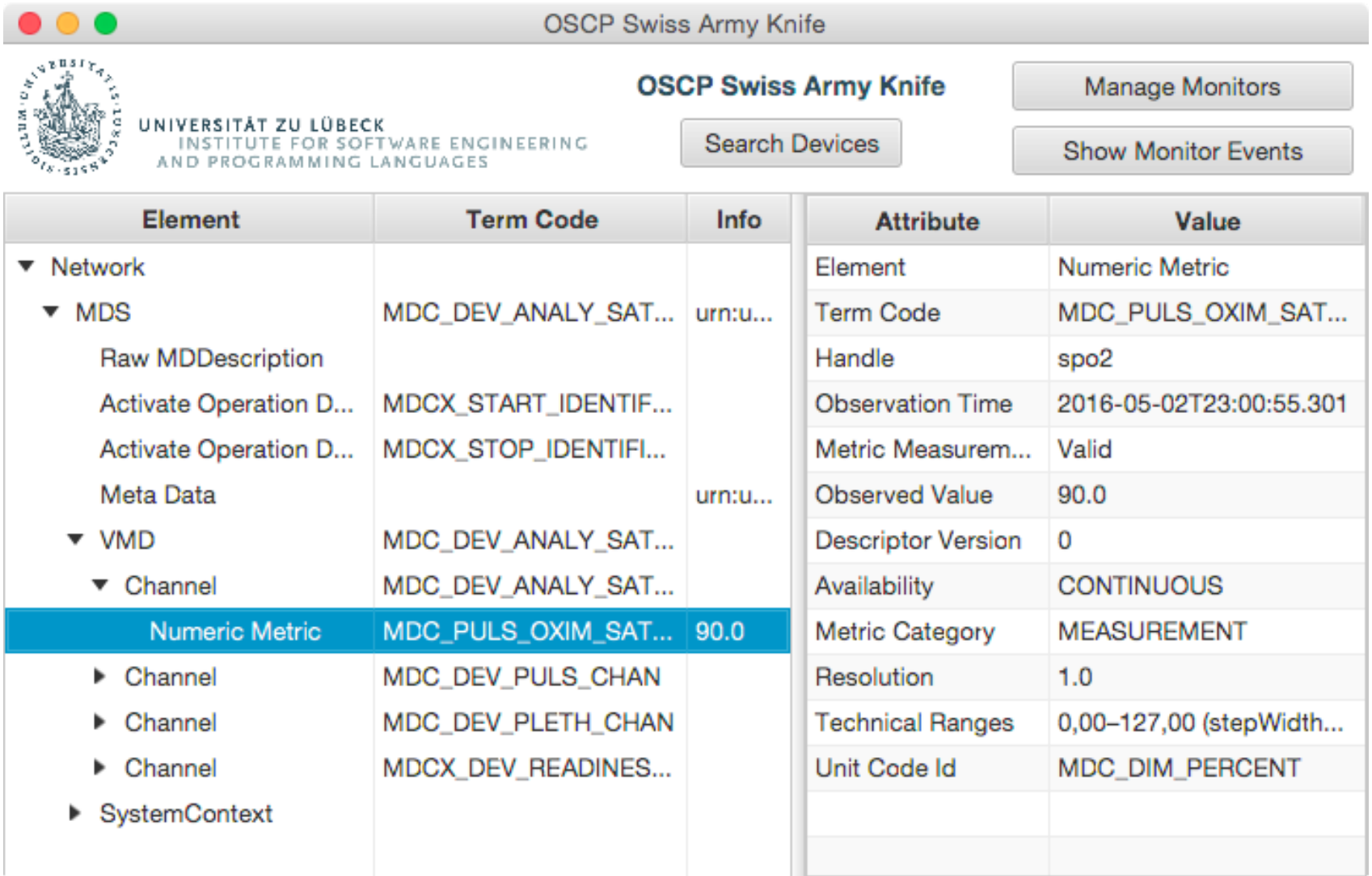
OSCP Device Monitoring



OSCP Device Monitoring



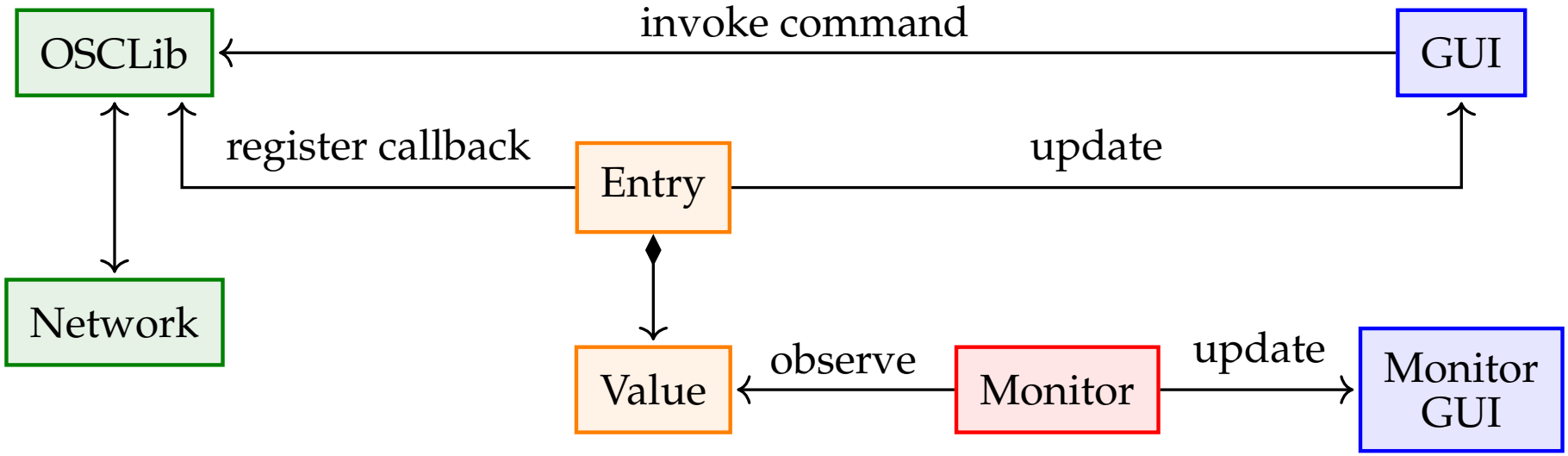
OSCP Swiss Army Knife



OSCP Swiss Army Knife

- Discover all active devices in network
- Show interface description
- Show current values
- Allow manipulation through service model
- Allow attachment of monitors

Monitor Injection in Swiss Army Knife



Demo

Demo

Conclusion

- IEEE 11073-SDC is upcoming standard for interconnection of medical point-of-care devices.
- Devices announce their interface to the local network.
- Monitors can be attached to devices' metrics.
- Monitors enforce own device and remote controlling device to satisfy the interface description.
- Swiss Army Knife discovers devices.
- Swiss Army Knife manipulates devices' states.