

Validation of Control Systems with Heterogeneous Digital Models and Virtualization Technologies

KIRILL SEMENKOV, VITALY PROMYSLOV, AND ALEXEY POLETYKIN

INSTITUTE OF CONTROL SCIENCES

RUSSIAN ACADEMY OF SCIENCES

Let me introduce ourselves (I)

The field of research:

- ❑ design and development of new methods of control for distributed I&C systems including NPP I&C systems
- ❑ methods of cybersecurity architecture design for I&C systems
- ❑ methods of cybersecurity risk analysis for I&C systems

Let me introduce ourselves (II)

Practical results and products:

- Software platform “Operator” for I&C systems that includes SCADA, CAD, development and maintenance tools
- Industrial quality Linux-based OS LICS
- Tools for cybersecurity simulation and risk assessment for complex systems (WWW-based demo – www.omole.ws)



Digital modelling for I&C

- ❑ Virtualization is an actively developing area of modern IT
- ❑ The technology is used in I&C world, too
- ❑ Modelling of complex systems is the emerging thread
- ❑ Digital twin is the most detailed model of a cyberphysical system

A few words about digital twin

Digital twin is a digital replica of a physical entity

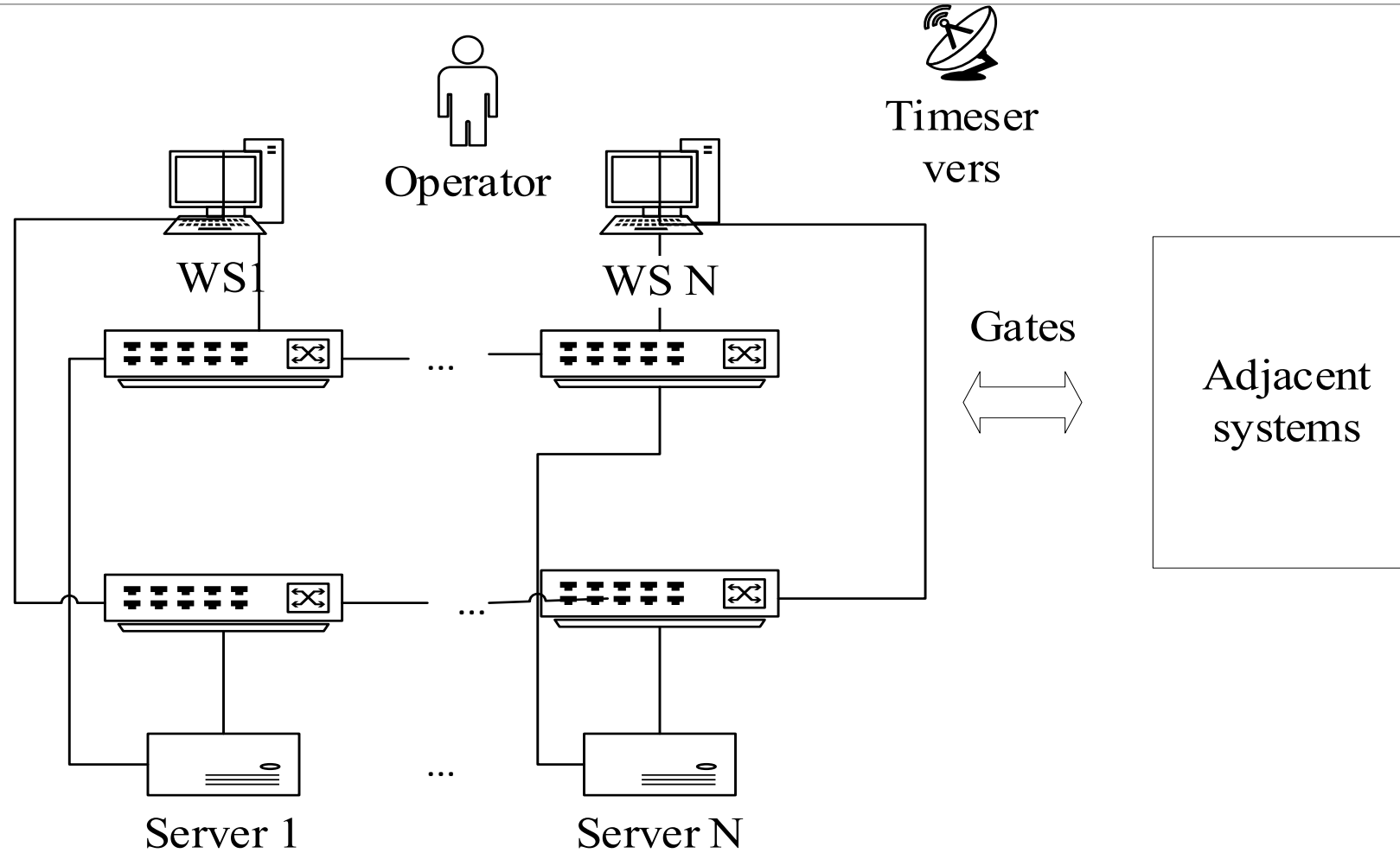
- ❑ A digital twin has a connection with the real counterpart
- ❑ The digital twin is fed with the data from the real twin
- ❑ The digital and physical object co-evolutionize together

The statement of the problem

Development of the top-level system for I&C system of a nuclear power plant

- ❑ Validation of system functionality
- ❑ Design and tests of cybersecurity controls
- ❑ System deployment
- ❑ Configuration management
- ❑ *Continuous development during the lockdown (new emergent problem)*

The system architecture



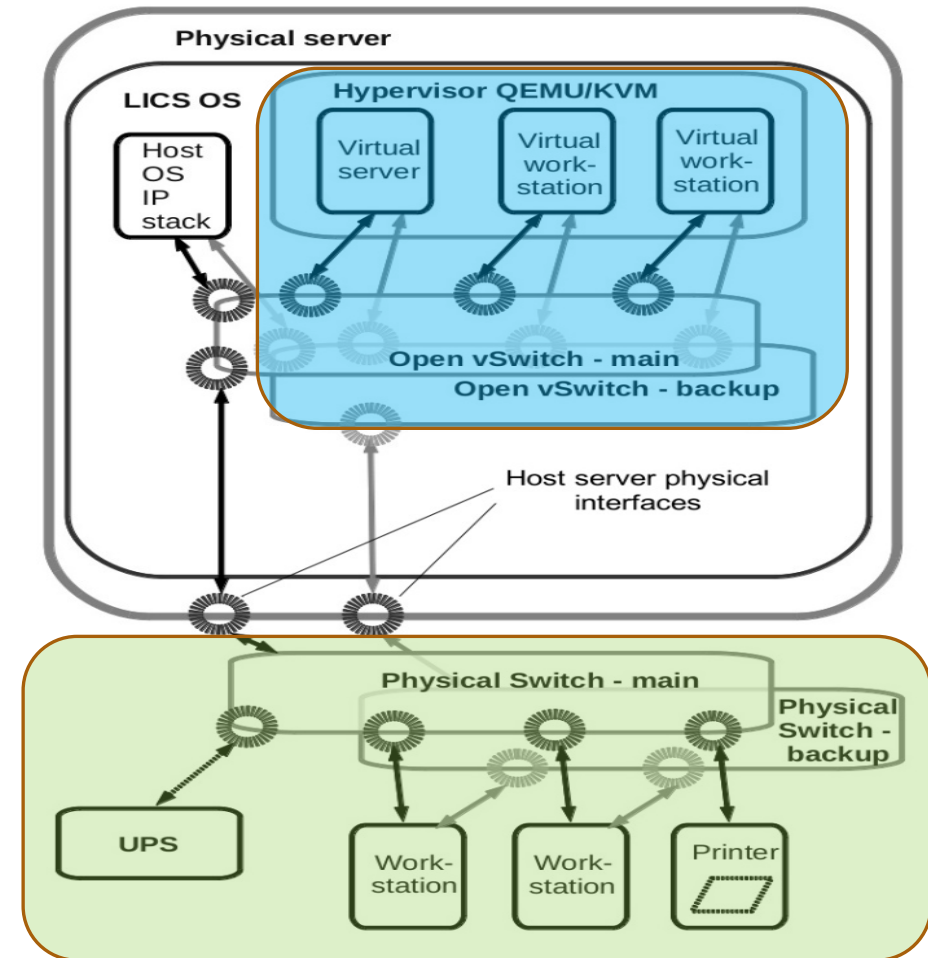
The system functions

- ❑ Operator control commands transmission
- ❑ Integration of the information from I&C subsystems within the power unit
- ❑ I&C system status monitoring
- ❑ Self-diagnostics

The choice of the model

Type of model	Motivation	Phys.	Dig.
Analytical	Description of a physical object behavior	+	-
	Verification and validation of algorithms	-	+
	Verification of timing characteristics	+	±
	Staff training	+	±
	Design of the control (system black box design)	+	+
Statistical	Reliability and stability estimation	+	+
Functional	System design	+	+
Data and data flow	Data representation and system logics	-	+
Full-scale	Full system validation	+	+
	Staff training	+	+
Digital twin	Validation of system logical structure and interfaces	+	
	Validation of discrete (state-by-state) time behavior	+	+
	Validation of system security	-	±
	Staff training	+	+
Heterogenous	Combines all advantages of the digital and physical models	+	+

The model architecture



The art of model design:

Full software emulation is impractical

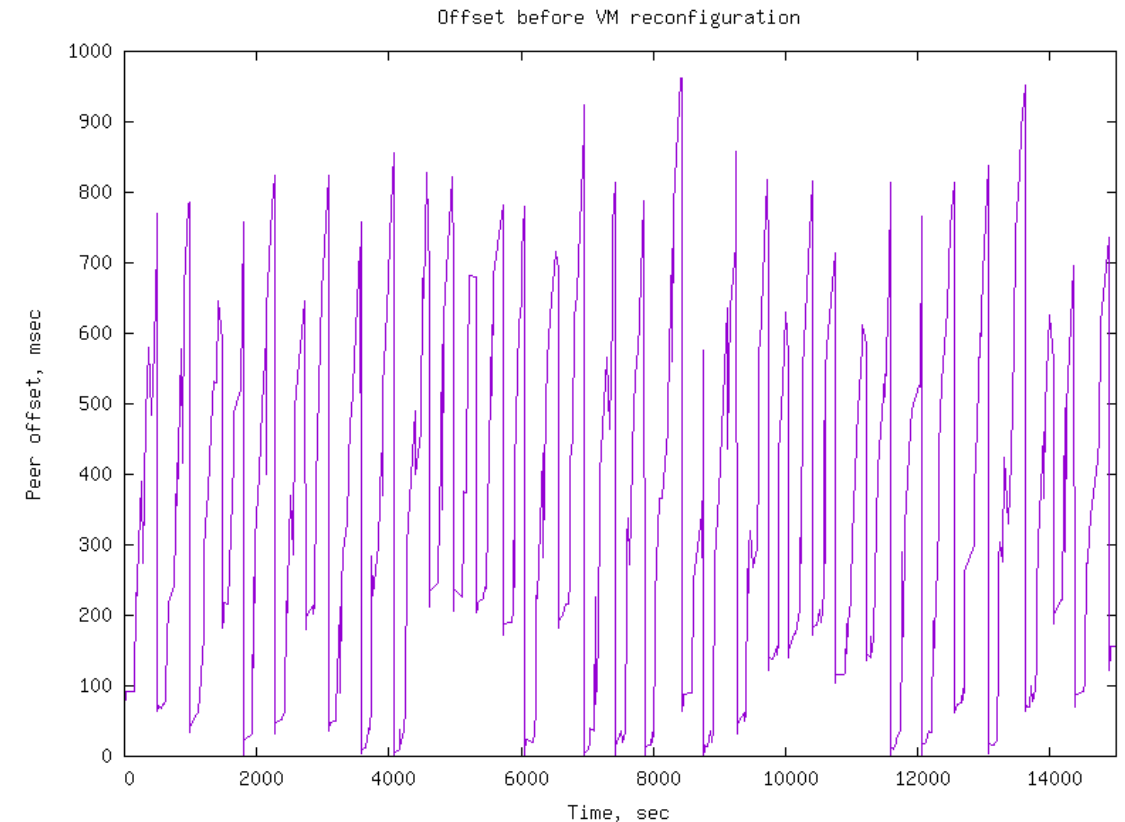
Example. Network card simulation

- ❑ The hypervisor emulates the same network interface card as presents in real server or workstation
- ❑ Result – network disruption on medium and heavy loads because of low performance of emulation mode
- ❑ Solution – switch to the paravirtualization.
- ❑ Drawbacks:
 - ❑ we cannot validate some hardware-dependent modes
 - ❑ *software configurations of the model and the real system differ*
- ❑ In general, we assume that the full emulation cannot be achieved

The art of model design:

Unified timescale provision

- ❑ The single timescale and time synchronization of units are crucial for the I&C systems
- ❑ The community recommends using paravirtual system clock drivers for the virtual machines
- ❑ Result: no synchronization
- ❑ Possible reason: simultaneous use of paravirtual clock driver on a number of competing VMs causes delays in hypervisor response



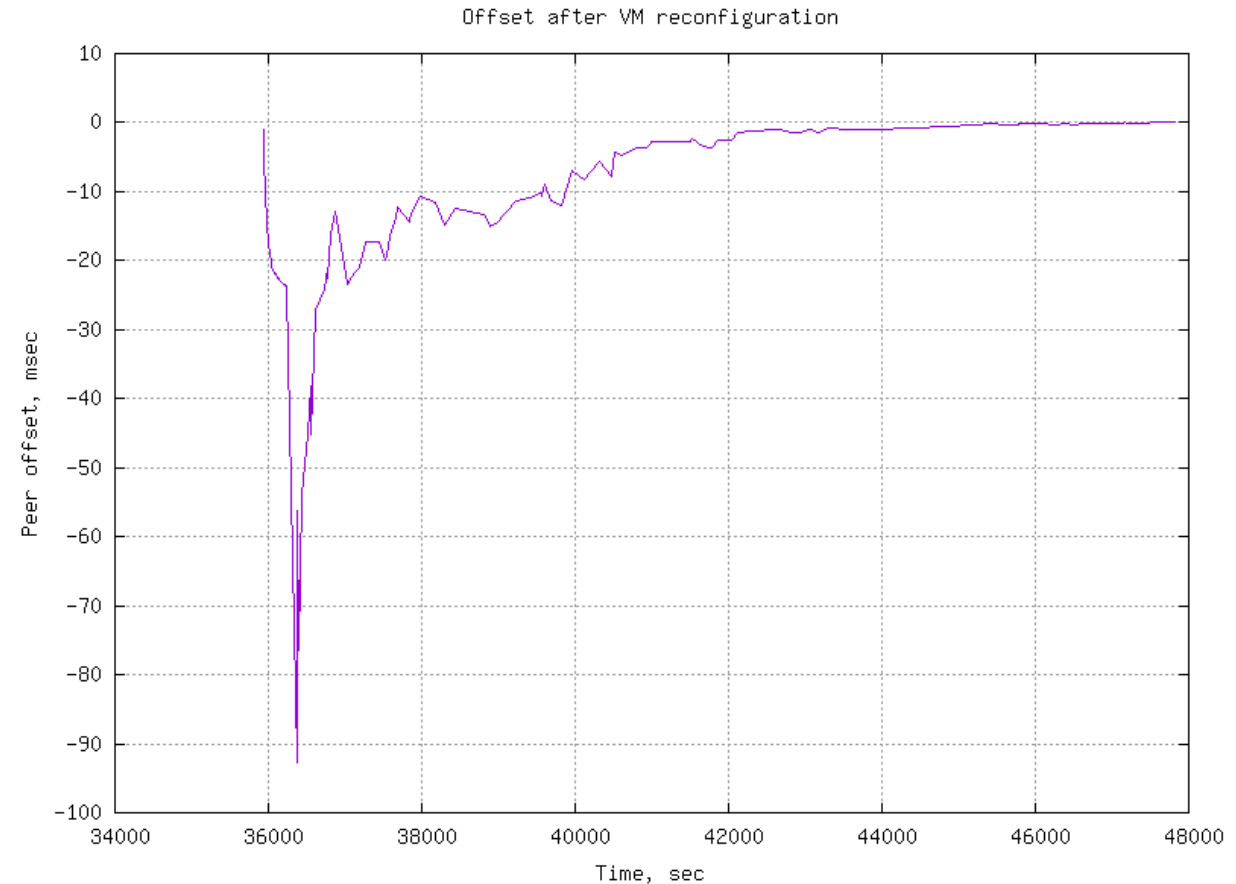
The art of model design:

Unified timescale provision

- ❑ TSC, Tick Step Counter, a counter of CPU cycles is the main timer in the modern computers
- ❑ The TSC increases evenly and does not depend on the dynamically changing CPU frequency
- ❑ The usage of TSC emulation for the guest machine allows NTP algorithms to converge

Name	Description
μ	Update interval
Δ	Root delay
E	Root dispersion
Θ	Clock offset
ϑ	System jitter
φ_S	Selection jitter
ρ	Max. reading error
φ	Frequency tolerance

Mills, David L. Computer Network Time Synchronization: the Network Time Protocol on Earth and in Space, Second Edition, 2011



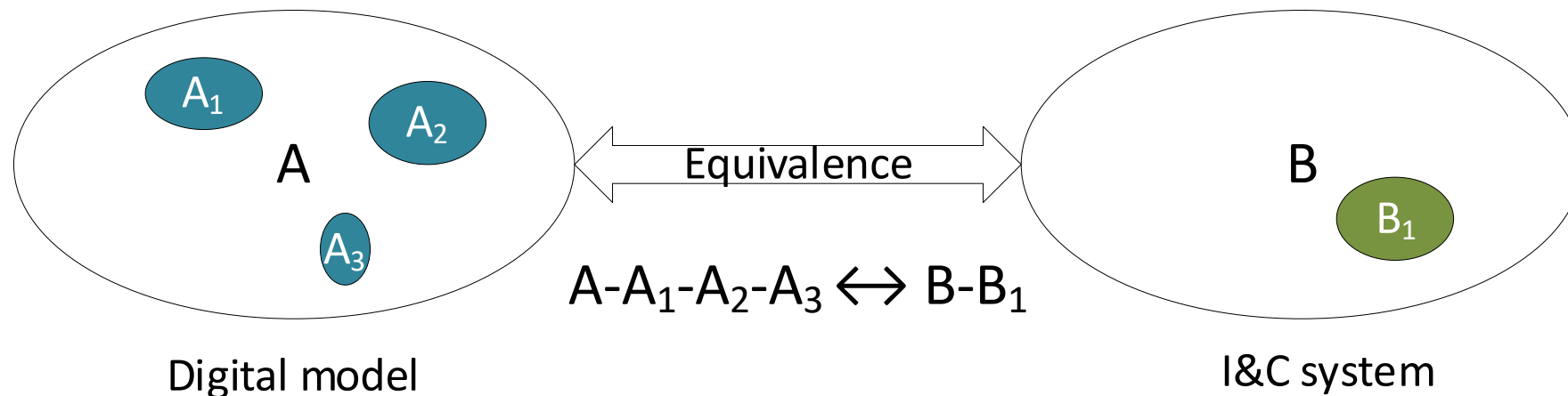
The limitation of the digital twin

- ❑ The exact estimation of the time characteristics and time-dependent procedures or algorithms of the I&C system requires to use identical hardware component
 - ❑ The achieved performance of an I&C system depends on the exact configuration of the real hardware
 - ❑ Virtual models allow to make only rough estimation of system performance
- ❑ The model always has components that differ from the its real counterpart
- ❑ The limitations may be smoothed by using the presented heterogeneous models

The configuration management

With the deployment, the virtual model and the real system must live “in parallel” and have identical configurations

We assume that configuration (software configuration) is a set of backbone components **currently installed** in the system.



Conclusions

1. Digital modelling is a powerful tool for the validation and deployment of I&C systems.
2. The full equivalence between the real object and the virtual model is hardly achievable
3. The models require close attention to the configuration management at all stages of modelling
4. A side-effect of the digital models: they are very usual in times of lockdown.