SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Established in collaboration with MIT

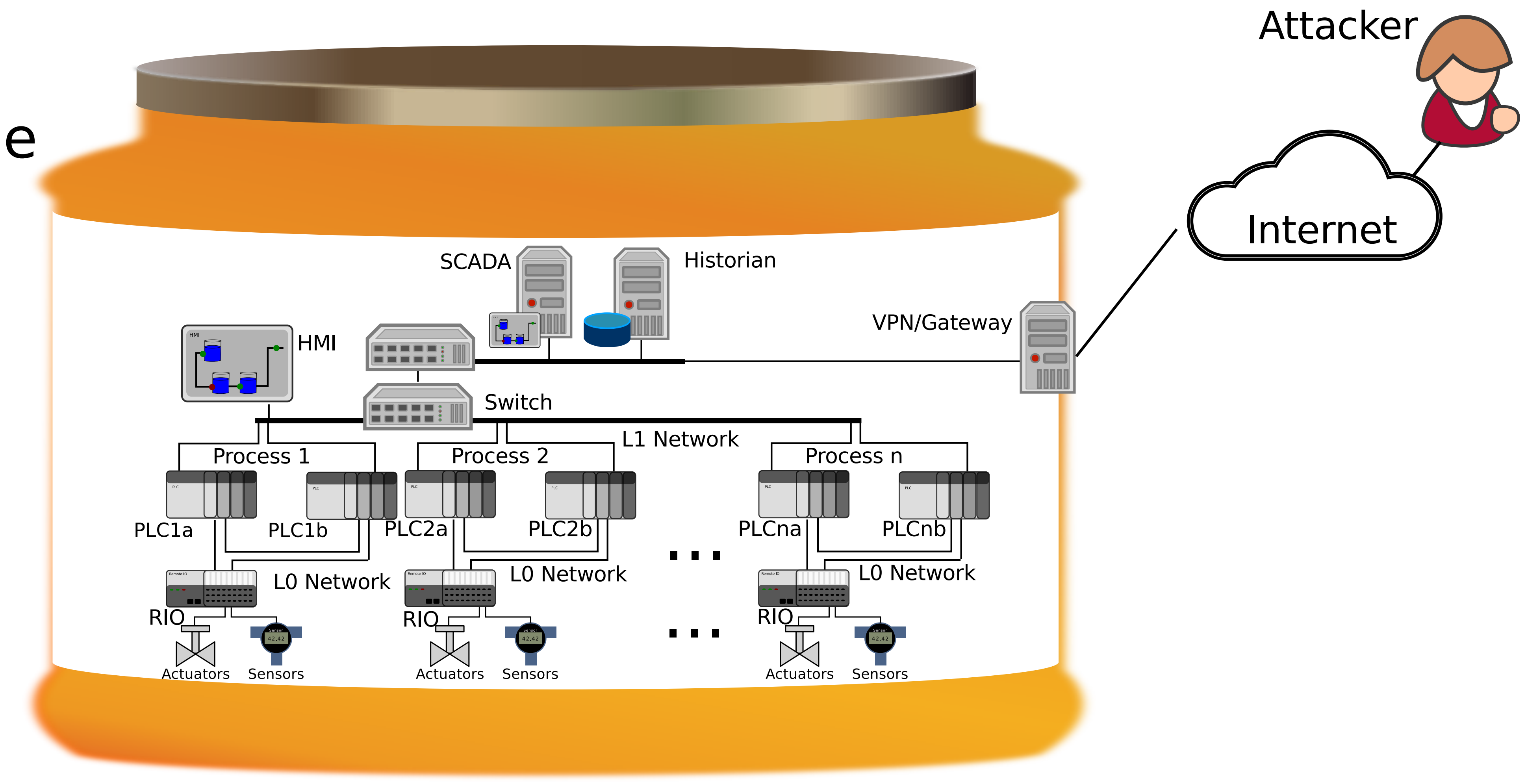
Towards High-Interaction Virtual ICS Honeypots-in-a-Box

Daniele Antonioli and Nils Ole Tippenhauer

iTrust Centre for Research in Cyber Security

Problem Statement: ICS Honeypots

- Honeypot as defense mechanims: intended to be probed and compromised by attackers.
- No available realistic (ICS) honeypots:
  - Requires physical process simulation
  - Requires industrial traffic emulation
  - Requires industrial devices simulation

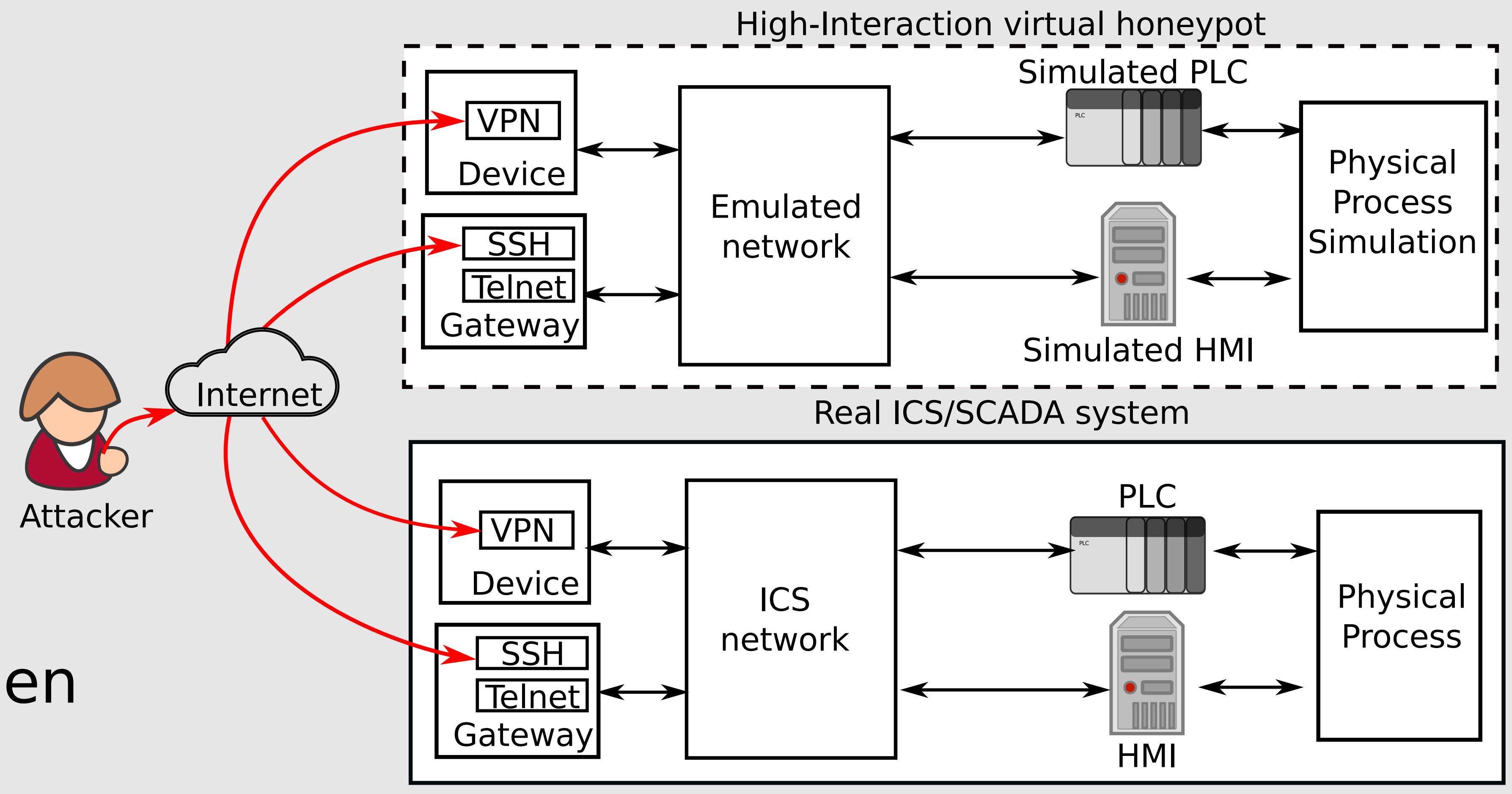


Our ICS Honeypot:

- Integrated simulation of process and control
- High-interaction, Virtual, Low cost
- Deterministic execution in real-time
- Runst in-a-Box, SDN compatible, Reconfigurable

Our ICS Honeypot Architecture:

- Vulnerable internet-facing interfaces: VPN, SSH, and Telnet.
- Network emulation: topology, protocol, link shaping.
- Simulated devices: PLC logic, web servers.
- Physical process simulation: water treatment, water distribution.
- Physical and network layer API: interfaces between devices, network and physical process.



Our ICS Honeypot SWaT Implementation:

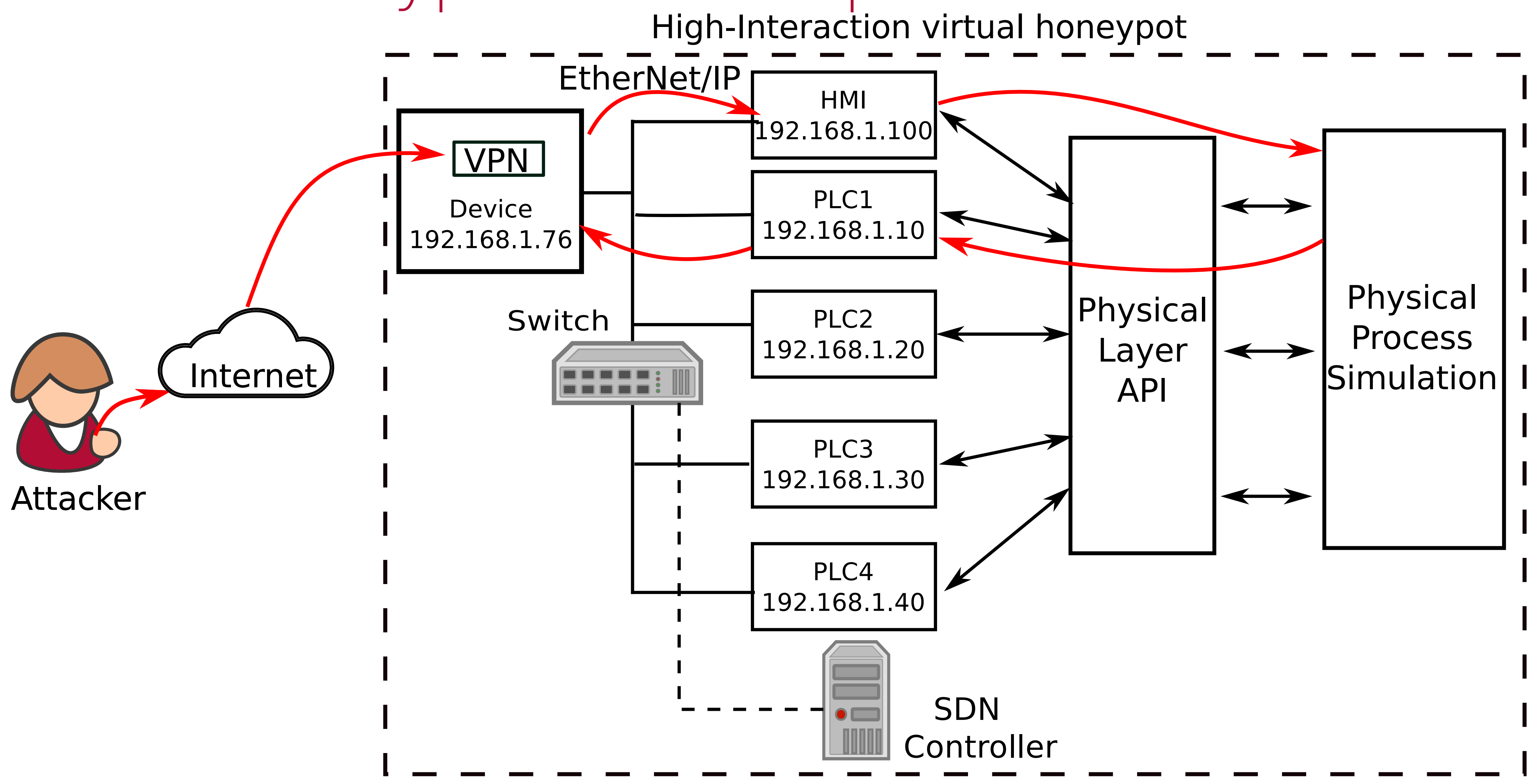


Table 2: Honeypot metrics evaluation summary.

Metric	By design	Implemented
Network		
IP, MAC and netmask	●	●
Packet loss	●	●
Packet delay	●	●
Bandwidth	●	●
Topology	●	●
Common protocols	●	●
Industrial protocol	●	◐
Advanced Traffic	●	◐
Physical		
Realistic math model	●	●
Sensor readings	●	●
Actuators driving	●	●
Control logic	●	●
Human operations	●	◐
Advanced Process	●	◐

Legend ●: full support, ◐: partial support.

Our ICS Honeypot S3 CTF Evaluationtation:

- S3 jeopardy-style Capture-the-Flag (CTF)
- Six m3-type AWS EC2, one OS per honeypot
- Idraulic simulation of water treatment (SWaT) process 1
- Simulated four PLCs, an HMI and two water tanks
- Star topology, EtherNet/IP, vulnerable SSH
- Scoring flask webapp using Let's Encrypt (HTTPS)

Table 1: CTF Results Summary.

Teams	# Captured Flags	# Distinct Cmds	# Executed LOC	# Recon Tools	# Attack Tools	Most Used Tools*
Team 1	2	20	1074	3	1	{1, 2, 6, 8}
Team 2	5	30	2488	6	2	{1, 2, 3, 4, 5, 6, 7, 8}
Team 3	3	23	2045	5	2	{1, 2, 3, 4, 6, 7, 8}
Team 4	4	27	963	5	2	{1, 2, 3, 4, 6, 7, 8}
Team 5	1	3	52	1	0	{1}

: Number Of, LOC : Lines Of Code

*{1: `ettercap`, 2: `nmap`, 3: `netstat`, 4: `tcpdump`, 5: `tshark` 6: `ifconfig`, 7: `cpppo`, 8: `ping`}

References:

[1] "Towards High-Interaction Virtual ICS Honeypots-in-a-Box" Proc. ACM @ CPS-SPC '16.

[2] "MiniCPS: A Toolkit for Security Research on CPS Networks" Proc. ACM @ CPS-SPC '15.