SWISS **OT-IT CYBER SECURITY** FORUM

AI, LLM & Digital Twins: **Which changes are necessary for being future-ready?**

All industries are confronted with a new revolution driven by AI, LLM and Digital Twins. Applications alike Agentic AI for OT Policies, Governance, Regulation and Compliance, Ai-Powered code Generation for OT Data Analysis

18th Forum, June 11, 2026 12:00-20:30 h
Hochschule Luzern, Suurstoffi 1a; Room Forum, 6343 Rotkreuz (parking available)

SWISS OT-IT CYBER SECURITY FORUM

Mission

Why should you attend?

The Swiss OT-IT Cyber Security Forum Series is a sequence of events which takes place three times per year, with the strategic goal to unify OT and IT decision makers. The main objective is achieving significant advances in security.

Background:

Historically, the two communitities had completely different set-ups:

- IT used to follow the speed of technology evolvement, with product cycles of about three years and extremely fast fixing of faults and errors: short reaction time of less than one hour is common practice by today.
- OT used to create solutions in the mechanical space with life cycles reaching from 25 to 70 years, with little maintenance on average every 3-5 years.
  In the past few years the use of IT in OT installation has been increasing dramatically and OT is now fully integrated in cyber-space. Therefore, the need to connect the two communitities is now more important than ever before in order to address the mutually dependent topics including security issues.

Design of the forum:

- 3 meetings per year
- 2-3 talks from industry leaders delivered in English
- Several roundtables lasting 1 hour
  in D, F and E at every meeting

Participation fee:

- CHF 360 per event, alternatively CHF 960 for three events (one year)
- Participation by invitation only. Proposal for inviting additional key persons mail to:
  bmhaemmerli@OT-IT-CyberSecurityForum.ch

Content:

The content will be coordinated by Prof. Dr. Bernhard M. Haemmerli, Hochschule Luzern, and will be created by the organizing committee.

Organizing Committee:

Drives the process for the meetings with delegates, sponsors and selected partners.

MAIN SPONSOR

KUDELSKI SECURITY

LOCATION SPONSOR

HSLU Hochschule Luzern

SPONSORS

ALSEC protect critical infrastructure

HSLU Hochschule Luzern

CKW.

PARTNER

satw it's all about technology

AI, LLM & Digital Twins: **Which changes are necessary for being future-ready?**

The key controls for AI integration for OT security are (i) agentic identity and access: Treat AI processes like human users. Each agentic workflow and model must have its own strictly limited identity, roles, and entitlements. (ii) Protocol-Level Enforcement: Do not rely only on prompt-level filtering but apply controls deeper at the system and network layers to block unauthorized changes. (iii) Tamper-Proof Auditing: Maintain high visibility into every action an AI agent takes on OT networks using deep behavioural analytics and continuous log tracing.

First Industry Standards as e.g. security agencies – including the Cybersecurity and Infra-structure Security Agency (CISA), the FBI, and international partners – have released official directives for the secure integration of AI in industrial environments. To implement these recommendations and learn how to secure autonomous AI logic pathways against prompt injections or data poisoning, review the Principles for the Secure Integration of Artifi-cial Intelligence in Operational Technology.

The **Defence Strategy of corporations using OT** must be supplemented with the use of LLMs to evolve from reactive chatbots to autonomous agents interacting directly with indus-trial data and physical systems. This means that security perimeter must also be adapted

Against this background Mark Campbell CISO, Lead Security Design and Governance at Axpo will give insights in one of the most innovative activities in this respect in Switzerland. He presents Agentic AI for OT Policies, Governance, Regulation & Compliance, and how AI-Powered Code Generation for OT Data Analysis & Interaction may be implemented for the benefit of a higher OT security level. But nothing good comes without any new potential risks. Therefore, he elaborates on the anatomy of an AI risk pattern in OT: The risk combination which AI agents inherently bring into the company. Finally, he touches how AI in OT can be deployed without creating new systemic Risk.

SWISS OT-IT CYBER SECURITY FORUM

AI, LLM & Digital Twins: **Which changes are necessary for being future-ready?**

The speeches prepare the two discussion rounds:

Discussion Round 1:
Practical AI application: Which applications are available, and which must be prioritized and implemented first to be future ready?

Discussion Round 2:
Risks coming with AI and Security opportunities given through Digital Twins: How to avoid Risks and how to position the use of digital twins?

We are looking forward to your participation, that we can elaborate forward think approaches, and get clarity and knowledge on AI in OT and IT security.

Bernhard Hämmerli on behalf of the organizing committee.

SWISS **OT-IT CYBER SECURITY** FORUM

18th Swiss OT-IT Cyber Security Forum
June 11., 2026, 12.00 – 17:30 h
Social activity and dinner end at 20:30 h

Agenda

In-Person Meeting: Hochschule Luzern, Suurstoffi 1a, Rotkreuz

Online Table will be offered, and online streaming of presentations
(high quality video and audio)

12:00	Lunch
12:45	Networking among participants
13:05	Welcome note by Prof. Dr. Bernhard Egger, Head of Study Program BSc ICS, and Prof. Bernhard M. Hämmerli
13:30	**Practical AI Applications for OT Cyber-Defence: Where we are today, and what improvements we can expect in the next few years?** *Mark Campbell, CISO – Lead Security Design and Governance, Axpo*
14:10	Roundtable 1: **Practical AI application: Which applications are available, and which must be prioritized and implemented first to be future ready?**
15:00	Exchange between groups
15:15	Break
15:45	**Anatomy of AI Risk pattern in OT and how to avoid new Systemic Risks?** *Mark Campbell, CISO – LeadSecurity Design and Governance, Axpo* **Digital Twins used for OT-Security: How to apply?** *Andrew Paice, iHome Lab HSLU*
16:25	Roundtable 2: **Risks coming with AI and Security opportunities given through Digital Twins: How to avoid Risks and how to position the use of digital twins?**
17:05	Exchange between groups
17:20	Wrap-up and information on next meeting
17:30	Social Activity at HSLU-Informatik: OT. Lab, Security Lab, in-depth & Background on study programs Bachelor and Master in Information & Cyber Security
18:45	Invited Dinner **Restaurant Siam Garden requested. Waiting on answer**
20:30	End of the forum

SWISS OT-IT CYBER SECURITY FORUM

Swiss OT-IT Cyber Security Forum 19

Auditing OT-systems: Which are the options for audit and its processes, and how to report for creating the best response? (reconfirmation by votes)

Audit and security testing offers many different options: but which option is the best for a specific situation? Therefore, it is important to get an overview from bug bounty, red teaming, penetration test to more compliance-oriented framework audits. Further, legal frame-works (NIS-2) demand real time / online compliance reports. The result must be communicated, but how? Is reporting the best option, or is risk communication better? We expect alively discussion and exchange of experience on these issues.

Date:	Tentative: Thursday, September 10, 2026, 12:00-20:30h
Place:	Emmi, Milchstrasse 9, 3072 Ostermundigen (Bern)
Speakers:	TBD
Roundtable 1:	Understanding security testing and audit: What are the options, and what are the criteria to select a specific approach?
Roundtable 2:	Reporting, risk communication and other influence on decision makers: What are the best options to invoke the desired actions?

Swiss OT-IT Cyber Security Forum 20

We vote. Top candidates are: SOC for OT / OT vs IT SOC and Supply Chain Risk and resilience

Date:	Tentative: Thursday, March 4, 2027, 12:00-20:30h
Place:	Zurich Area
Speakers:	TBD
Roundtable 1:	TBD
Roundtable 2:	TBD

SWISS **OT-IT CYBER SECURITY** FORUM

Registration

Register by replying to the invitation email with all your details – or by filling out this form, scanning it in or taking a smartphone picture.
Send the completed form to: info@OT-IT-CyberSecurityForum.ch

☐ Three consecutive forums for CHF 960.–
Forum 18 (11. 06, 2026), Forum 19 (10.09.2026) and Forum 20 (04.03.2027)

☐ 18th OT-IT Cyber Security Forum, June 11, 2026 only, at the price of CHF 360.– .

☐ Register for social activity 17:30-18:45

☐ Register for the sponsored Dinner 19:00-20:30 at
Restaurant SIAM Garden

☐ **Online Attendance: I will attend online in WebEx** (link is in the calendar entry)

First Name ..... Last Name .....

Organisation .....

Job Title .....

Street / No. ..... ZIP / City .....

Phone ..... Cellphone .....

Email .....

Please add instructions for invoice, needing an offer etc.:

.....

.....

.....

SWISS OT-IT CYBER SECURITY FORUM

Mission

The Swiss OT-IT Cyber Security Forum Series is a sequence of events which takes place three times per year, with the strategic goal to unify OT and IT decision makers and bring culture, language and security priorities on level of mutual understanding.

The main objective is achieving significant overall advances in security (OT & IT).

MAIN SPONSOR

KUDELSKI SECURITY

LOCATION SPONSOR

vetropack

SPONSORS

ALSEC protect critical infrastructure

HSLU Hochschule Luzern

CKW.

PARTNER

satw it's all about technology