Hacking the Vertical

Cybersecurity Risks in Connected Elevators in the Age of AI

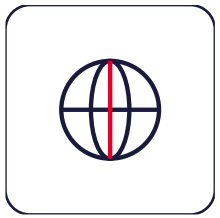
Alwin Warringa & Tom Dantuma
Sopra Steria Red Team
in partnership with Liftinstituut

ELA Conference 2026 · Rotterdam

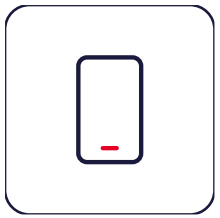
Who we are

We find weaknesses before someone else does

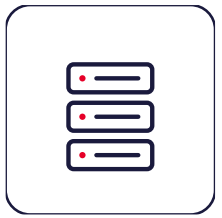
WHAT WE TEST



Websites



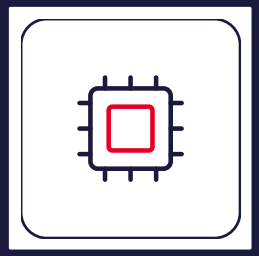
Mobile apps



IT infrastructure

Phishing & people

TODAY'S FOCUS



Connected products — like lifts

Two perspectives, one fleet you can trust

Why we work together with Liftinstituut

LIFTINSTITUUT

Audits the lift

Does it work as designed?

SOPRA STERIA RED TEAM

Tests the lift

Can someone make it misbehave?

Together they give customers a complete answer.

The machine room is no longer the perimeter

Lifts used to be mechanical. Today they are connected.

YESTERDAY

A locked door was enough

Risk was local

TODAY

The lift talks to the internet

Risk is global

Physical safety stays mechanical. Trust depends on software.

What this looks like in practice

Four real ways attackers approach connected products

01	Hardware bought online
02	Mobile apps
03	Cloud connections (APIs)
04	Chip extraction

Old hardware is someone else's research lab

Example: the secondary market

A few hundred euros on eBay

=

A weakness you don't know about

New No Box KONE Elevator KM802890G11 802893H03 LCECCBN2 Lift Car TOP Board

New – Open box

$349.00

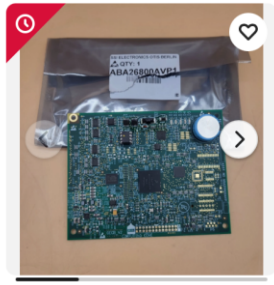
or Best Offer

+$30.00 delivery

Located in India

virammariness 99.5% positive (408)

Sponsored



Elevator Controller CPU Board. GCS/ Gen2 Traction Platform. OTIS PCB- GECB 2

Brand New

$485.00

Only 1 left!

SLIDE 7

The mobile app is the front door

Example: apps and cloud connections

The app talks to the cloud.

The cloud talks to every lift.

One weakness scales to thousands of units.

Test it like an attacker would — before your customer does.

When attackers turn to the chip itself

Example: hardware extraction

€2,000

of hobbyist equipment

is enough to read most chips

Weeks → Days

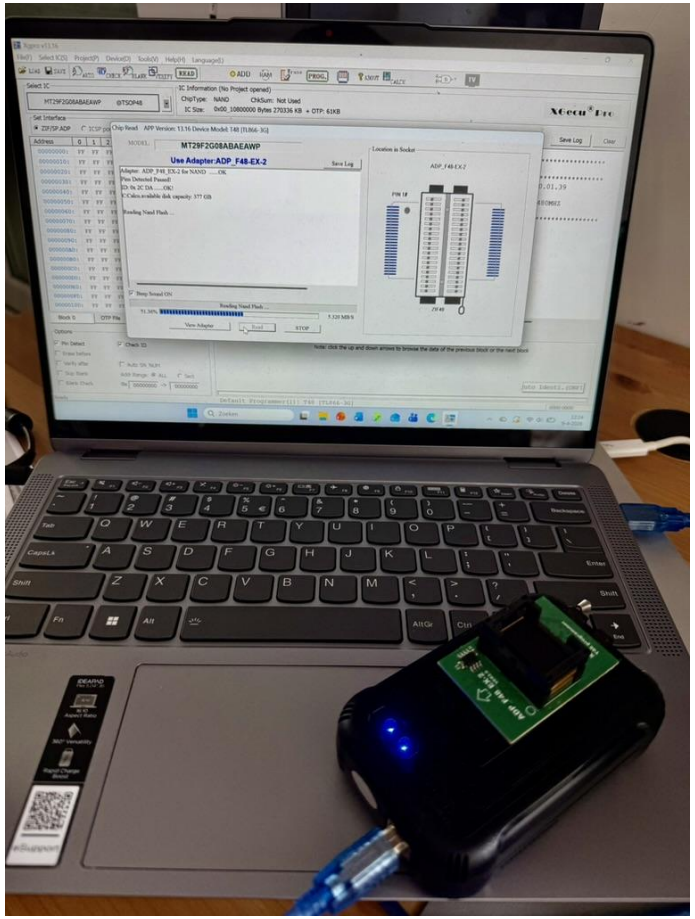
Specialist lab work

is now a hobbyist project

One controller in attacker's hands shouldn't compromise your fleet.

When attackers turn to the chip itself

Example: hardware extraction



What AI changes

It doesn't invent new attacks — it makes them much faster

TASK	BEFORE AI	WITH AI
Studying how a device works	Weeks	**Hours**
Finding software weaknesses	Manual review	**Automated**
Building a working attack	Days	**Minutes**
Targeting technicians	Generic	**Personalized**

Testing components before release is no longer optional.

What to take back to the office

01	Connectivity changed the threat model
02	Trust depends on software, not hardware
03	Assume your products will be studied
04	AI shortens the attacker's timeline
05	Audit + pentest = complete picture

Thank you

Questions?

Alwin Warringa & Tom Dantuma
Sopra Steria Red Team
alwin.warringa@soprasteria.com / tom.dantuma@soprasteria.com

In partnership with Liftinstituut · ELA Conference 2026 · Rotterdam