# From Proof to Product

*Why Formal Methods is ~~finally ready~~ really, really needed*

**Martin Dehnel-Wild**

Chief Scientist, Kry10

seL4 Summit, September 2026, Vancouver

KRY10


trade.gov.pl

# 01
# The Stakes

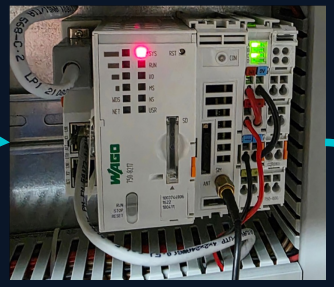
KRYIO

**29th December 2025**

The Intertubes


**18th Dec**


Teltonika




WAGO PFC 200

STOP

**25th December:**
Siemens S7-300, S7-1200, S7-1500

KRYIO

- No zero-days, no exotic malware: too much trust between vulnerable boxes.
- Poland was done over by hand.
- Two weeks ago, five US agencies warned these same approaches are now being AI-generated and driven.

***"This is not a theoretical risk; it is an active threat."***

***NSA, CISA, FBI, DOE, EPA***
***August 2026***

KRYIO

# The cost of attack is falling, *fast*

# The attacker's ROI just went up.

# Ours has to go up faster.

KRYIO

02

# Security is economics

KRYIO

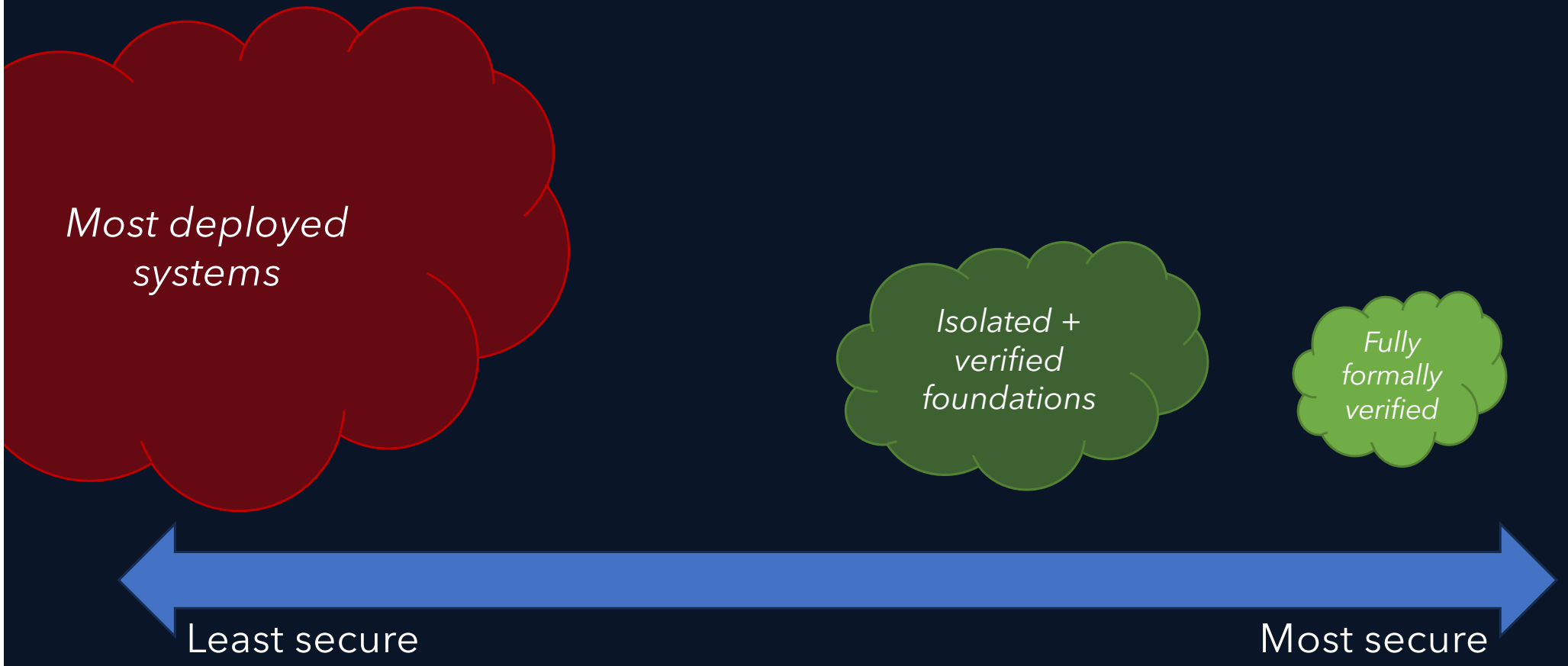
***There's no such thing as a perfectly secure system.***

*— Bruce Schneier (probably, idk)*

KRYIO

*“I don’t have to outrun the bear,*
*I just have to outrun you”*

# Perfect is the enemy of good




KRYO

***"The economic bound on attack has broken."***

– ***Gopal Sarma**, RAND, (former White House Cyber Security)*

KRYIO

# 03

# This is FM's moment

*…if we choose to take it.*

KRYIO

# What went wrong?

- We over-promised.
- Tools barely talk to each other.
- And we've stayed stuck in the lab.

But this is our moment.

# Either we lower the bar to entry, or we fail

**Most real attacks are *boring:***
stolen passwords, default creds,
well-known CVEs, flat networks,
mis-configured devices.

# 04
# Let’s do the fandango

KRYIO

# So, I rebuilt the box

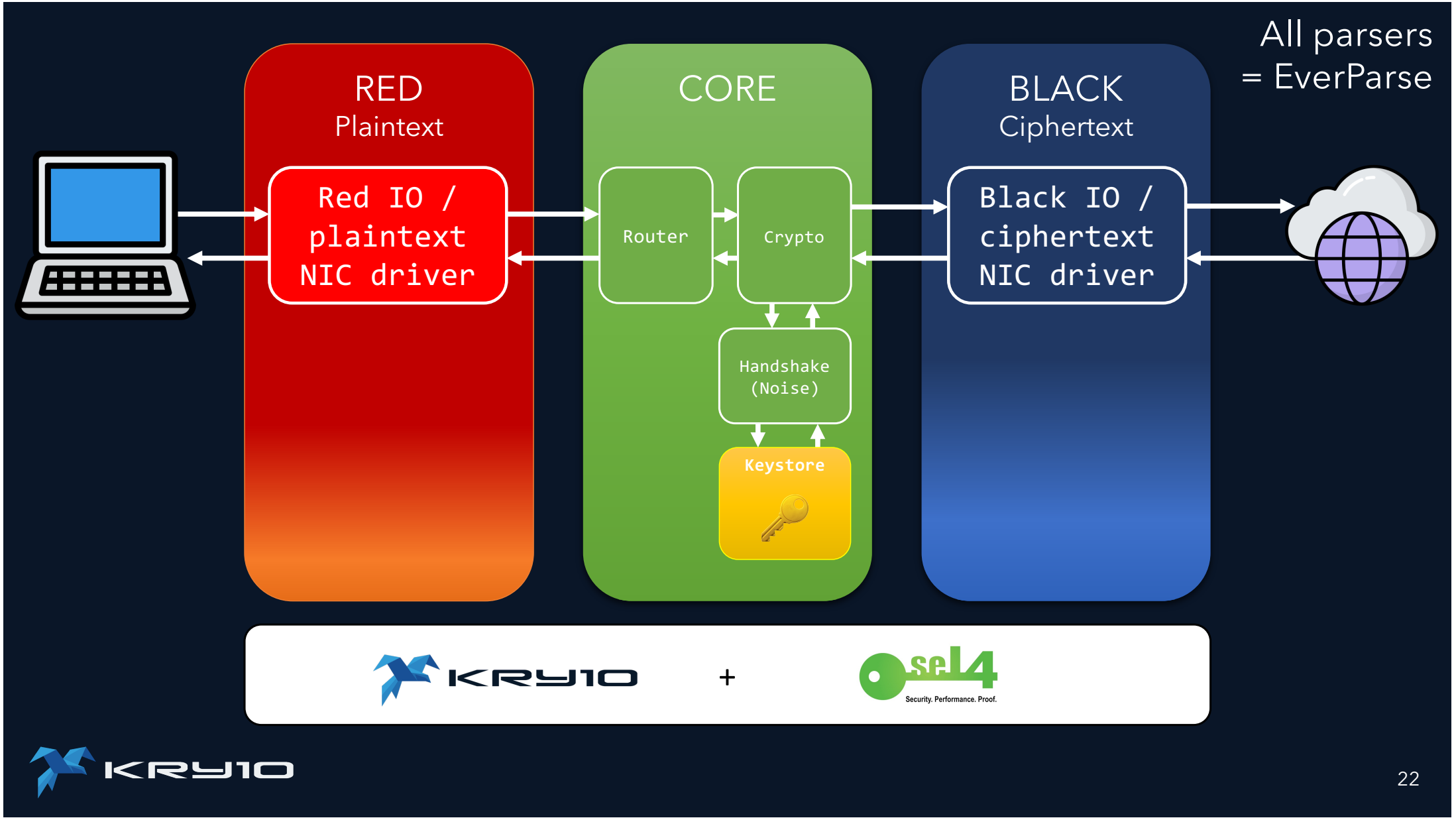

compulab.com

KRYIO

# Secure by construction

- HACL* for the crypto
- EverParse for the parsers
- seL4 + Kry10 OS for the isolation

- Bad packets are provably rejected


All parsers
= EverParse
RED
Plaintext
CORE
BLACK
Ciphertext
Red IO /
plaintext
NIC driver
Router
Crypto
Handshake
(Noise)
Keystore
Black IO /
ciphertext
NIC driver
KRYO
+
sel4
Security. Performance. Proof.

# We're Going on a Bear Hunt

Michael Rosen • Helen Oxenbury

Amazon.ca

Of course it’s not perfect

*…but where would you even start?*

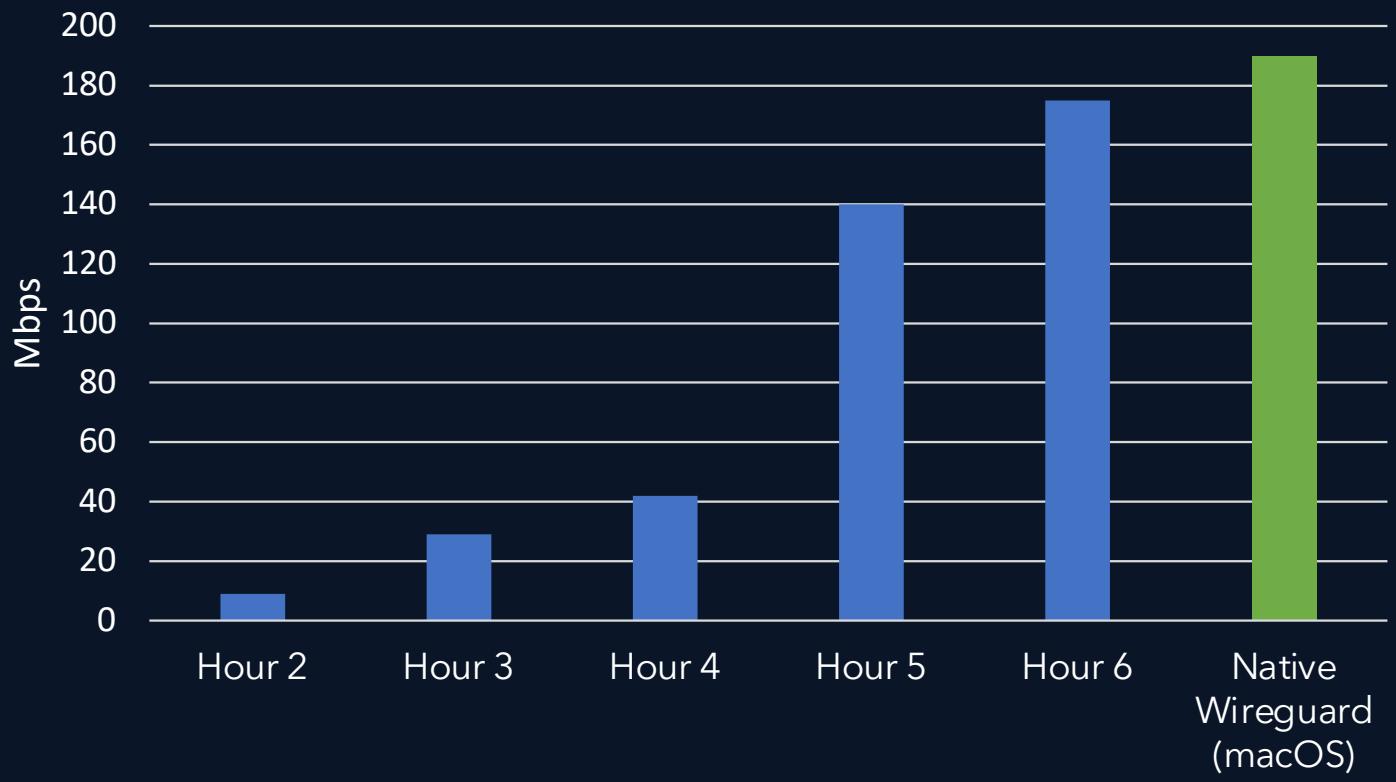
KRYIO

# What we're trusting

| Relied on, proven | Relied on, unverified | No claims made |
|---|---|---|
| seL4 | Manifest + tooling | Physical access |
| HACL* outputs | Handshake state machine code | Side channels / timing |
| EverParse outputs | Boot chain & firmware | Board supply chain |
| WireGuard protocol | Hardware | Red-side laptop |
| | F* extraction toolchain | |

KRYIO

## Martin & Claude Code vs. Native WireGuard on macOS




- ~93% of WireGuard's native throughput
- 5–6 hours' human work, over a weekend

KRY10

# Where Claude confidently wasted my afternoon

- Confident wrong diagnosis of a boot loop
- Diagnostic deadlock
- Silent packet loss

# Skill files are the new documentation

- How did you get Claude not just to produce slop?
- ‘KOS Context’
- "Making your platform legible to a model is now part of making it adoptable.”
- Teaching models what you want is key

KRYIO

# What's actually *in* KOS Context?

Not really API docs, more describing the gaps

- Decision guidance
- Anti-priors
- Silent footguns
- Measured platform behaviour
- Composition & security wiring
- Hardware / driver mechanics
- Toolchain & workflow

# Show & tell

*Is high assurance now something you can build in an afternoon?*

# 05

# We already have the thing

The whole point of a microkernel is that *the code on top matters less.*

Let's use that.

A safer world needs more deployments.

"More deployments" needs easier retrofit

…and *one* fast way to get there is LLMs.

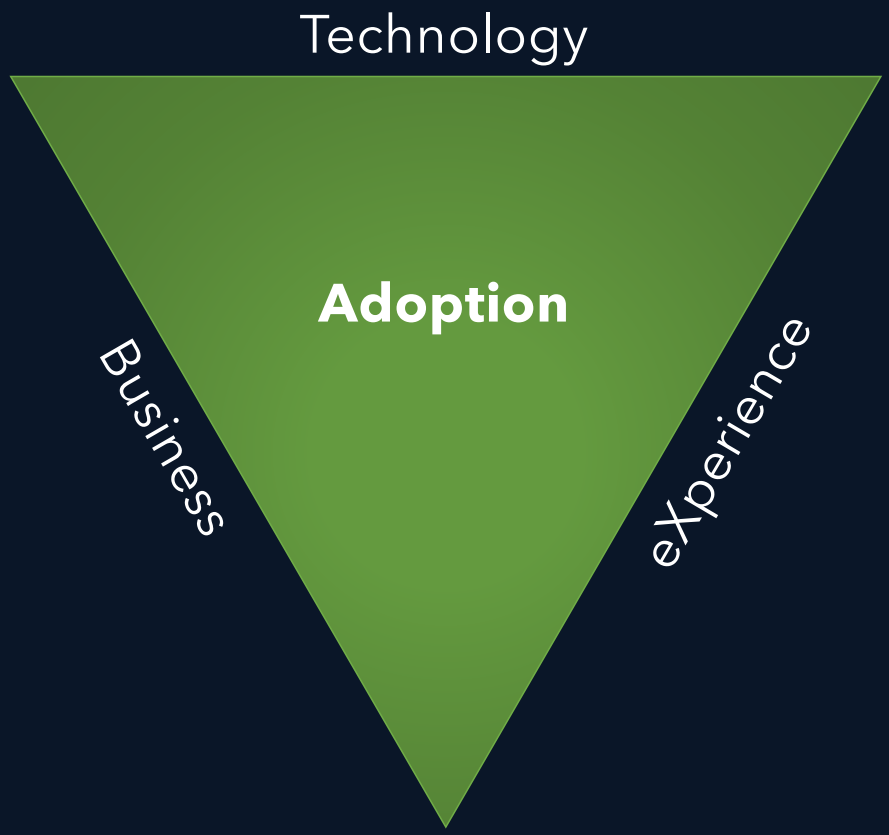
KRYIO

# 06
# Ship and iterate

You can't predict every environment you'll deploy into.

So you have to be able to update it – live.

Adoption needs all three. We're currently only great at one.




KRYIO

"Build what customers will actually buy, not what we think they need."

# The unglamorous question

- FOSS security infrastructure is maintained by people who find it *interesting*
- Security work is mostly gruelling, boring, and never finished
- So: **who pays for the boring parts?**

07

# Money where our mouth is

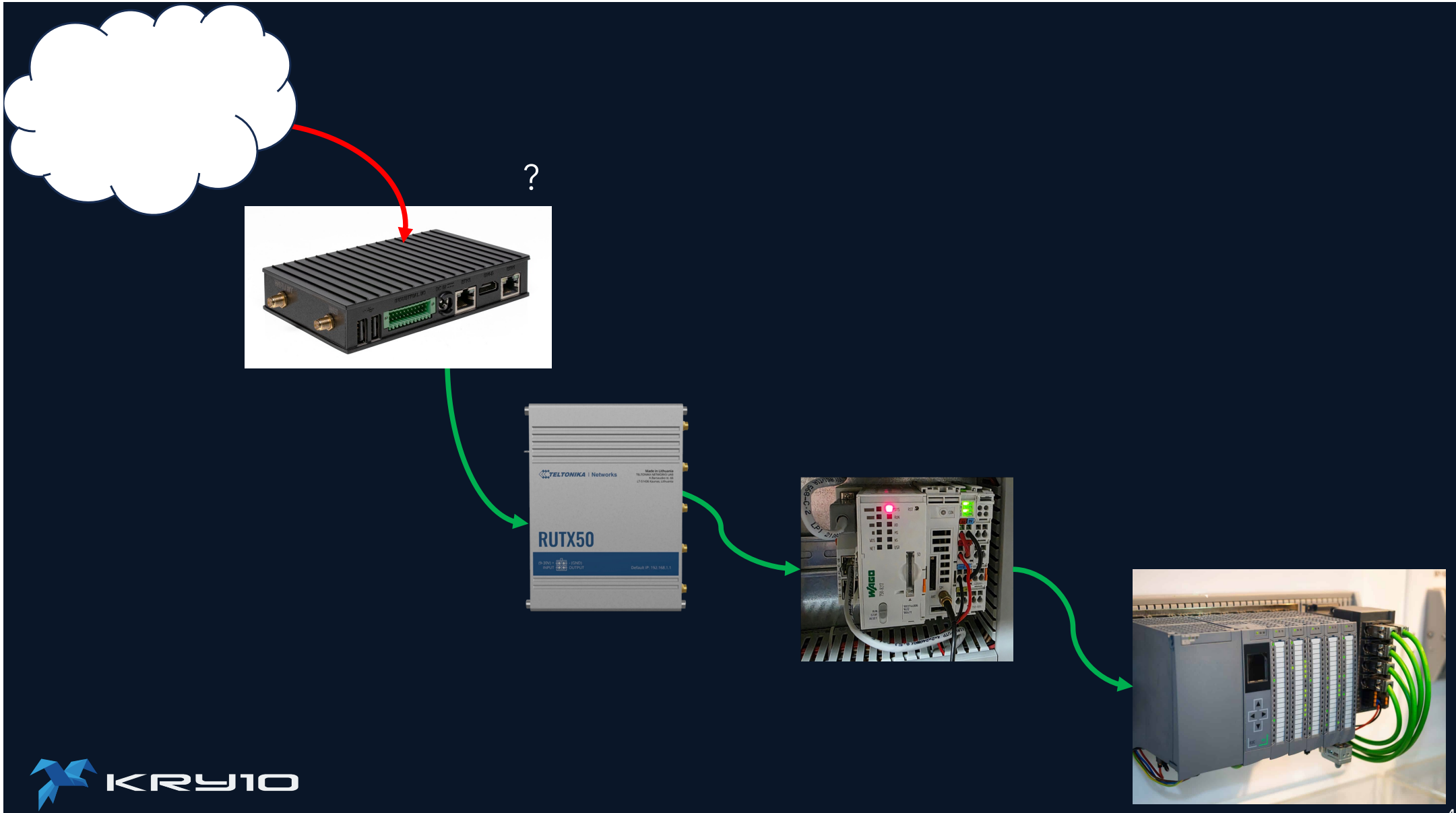
# What are Kry10 building?

- **Healthcare:** devices you can't patch or take offline
- **Manufacturing:** an IT/OT bridge to protect factories
- **Maritime / Defence:** designed assuming isolation, now not!
- **Power grids:** Poland, again
- **Drones:** PX4 onto KOS in about six engineer-months

# 08
# Now what?

This isn’t “deploy because we can,”

It’s “deploy because we have to.”




KRYIO

# Recap

1. Security is economics, and the attacker's costs are collapsing.
2. We already have the thing: verified foundations, isolation, boring architectures.
3. What’s left is deployment.

*"We don't have time to get this wrong."*

*– Kathleen Fisher, CEO ARIA, former Director I2O @ DARPA*

KRYIO