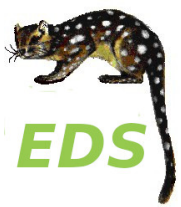
Laot - man in the middle defence for critical infrastructure using the seL4 Core Platform

A gentle introduction covering the projects aims, outcomes and future directions. It is intended for a general audience. See Laot Pub for some more information or contact the speakers.

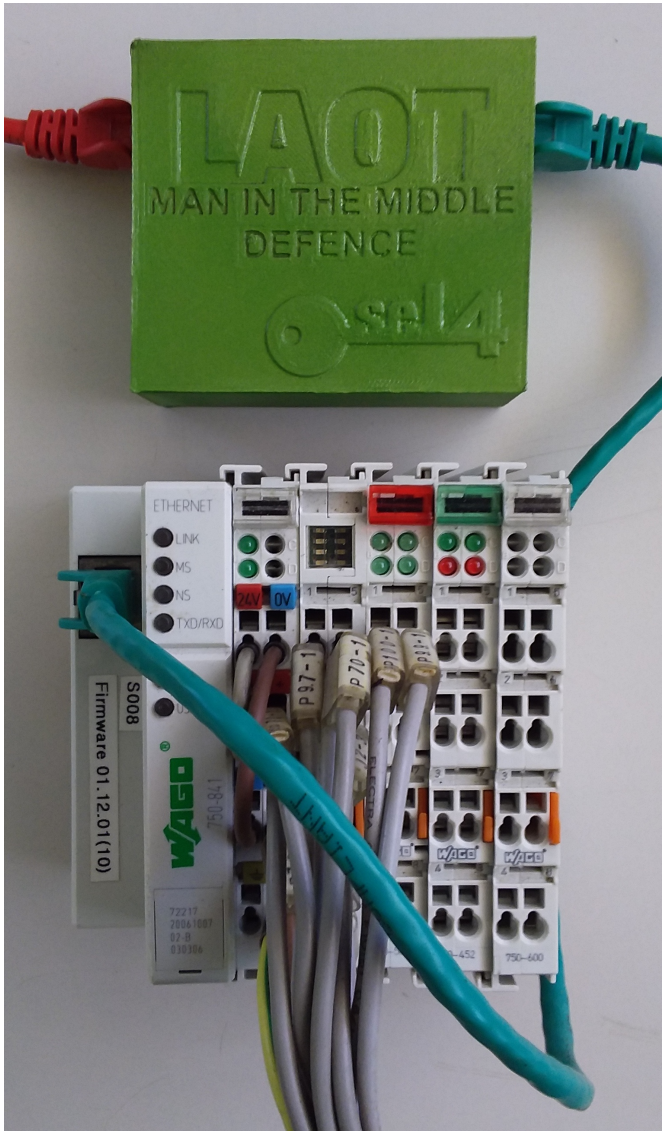
Phil Maker, EDS



Sydney, 2022-08-15T11:05+10:00[1]

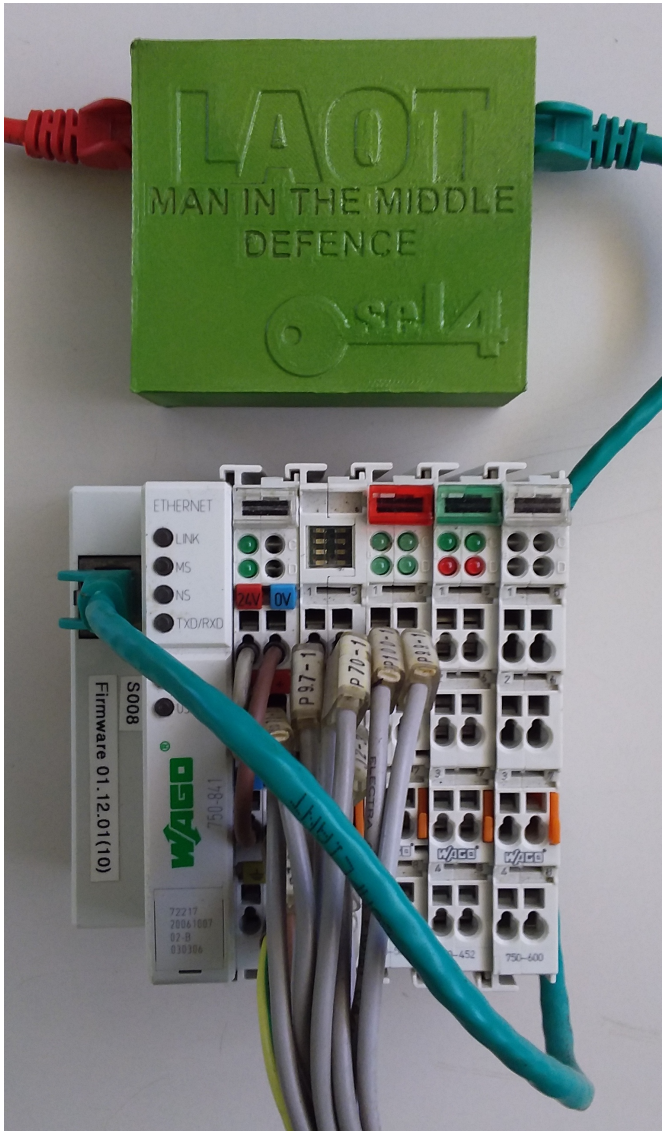
[1] And yes all times must be in ISO8601

What



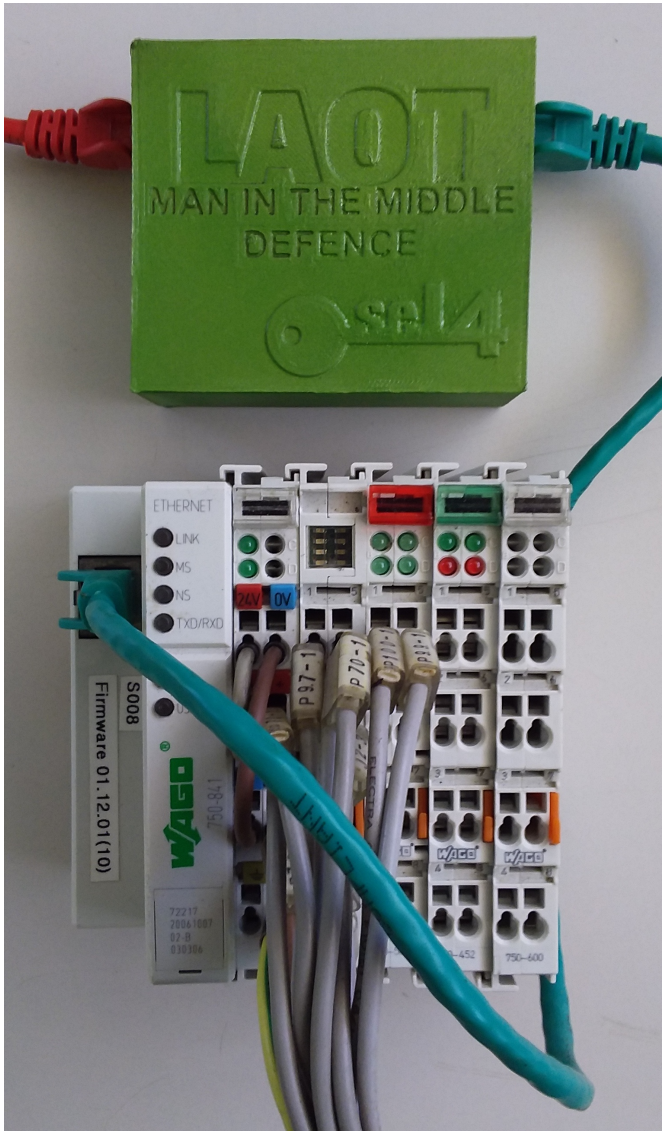
- What: Edge of Network Protection Device for Critical Infrastructure.

What



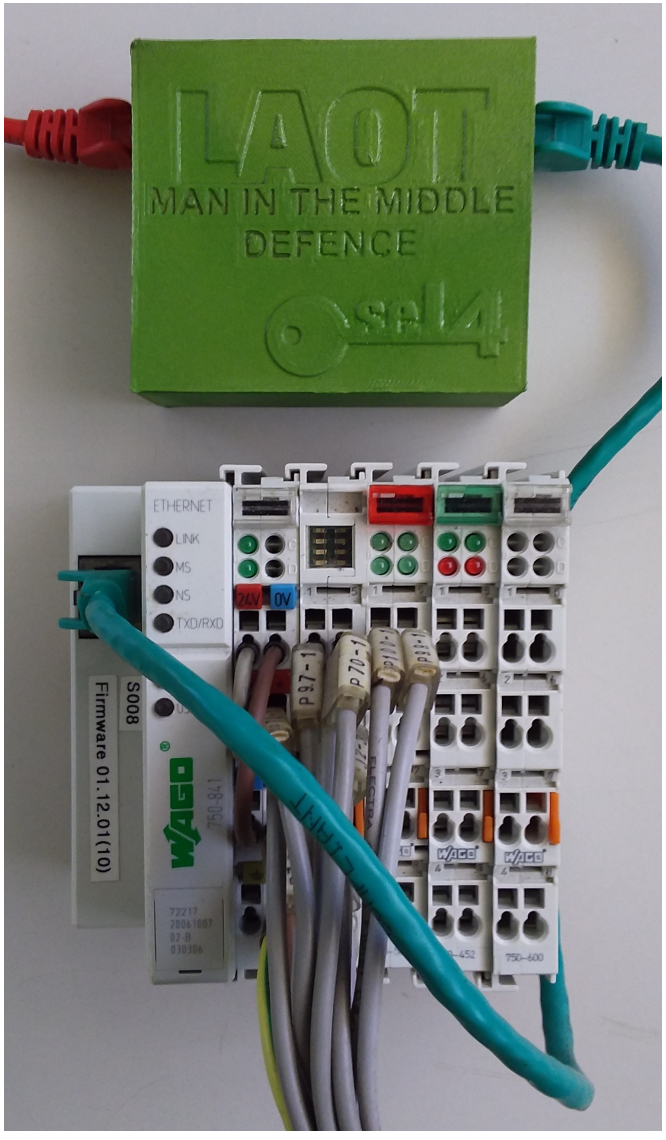
- What: Edge of Network Protection Device for Critical Infrastructure.
  - Based on seL4 and Core Platform
  - Edge of Network: 1 device per Device Under Protection (DUP).
  - Left hand/red cable is the outside/threat.
  - Right hand/green cable is the Device Under Protection.

What



- What: Edge of Network Protection Device for Critical Infrastructure.
  - Based on seL4 and Core Platform
  - Edge of Network: 1 device per Device Under Protection (DUP).
  - Left hand/red cable is the outside/threat.
  - Right hand/green cable is the Device Under Protection.
- Why: existing protection methods are broken, e.g. Essential Eight, or hoping that $20x10^6$ lines of code can be correct. Patching older systems is often impossible.

What



- What: Edge of Network Protection Device for Critical Infrastructure.
  - Based on seL4 and Core Platform
  - Edge of Network: 1 device per Device Under Protection (DUP).
  - Left hand/red cable is the outside/threat.
  - Right hand/green cable is the Device Under Protection.
- Why: existing protection methods are broken, e.g. Essential Eight, or hoping that $20x10^6$ lines of code can be correct. Patching older systems is often impossible.
- Who: Benno, Gernot and Phil with support from Defence.

What are we protecting?

- Critical Infrastructure:
  - Generator Controllers, Wind Turbines.
  - IoT for the Darwin Grid.
  - Water Supply Systems

What are we protecting?

- Critical Infrastructure:
  - Generator Controllers, Wind Turbines.
  - IoT for the Darwin Grid.
  - Water Supply Systems
- These devices have a life span of 20+ years and have often been produced by companies that no longer exist.
- Attacks include:
  - Aurora Generator Attack - simple attack to destroy generators.
  - Stuxnet - attack on the nuclear program in Iran.
  - Log4Shell - Log4j vulnerability.

seL4

To quote from Chapter 1 of the seL4 whitepaper:

1. seL4 is an operating system microkernel.
2. seL4 is proved correct: seL4 comes with a formal, mathematical, machine-checked proof of implementation correctness, meaning the kernel is in a very strong sense "bug free" with respect to its specification.
3. Besides implementation correctness, seL4 comes with further proofs of security enforcement [Klein et al., 2014].
4. seL4 improves security with fine-grained access control through capabilities.
5. seL4 is the world's only OS kernel (at least in the open literature) that has undergone a complete and sound analysis of its worst-case execution time (WCET) [Blackham et al., 2011, Sewell et al., 2017].

seL4 Core Platform

The purpose of the seL4 Core Platform (sel4cp) is to enable system designers to create **static** software systems based on the seL4 microkernel.

It provides:

1. Tool that weaves ELF excutables plus an XML description into a single image.
2. Protection Domains: priority scheduling, interrupt handling, ...
3. Channels
4. Shared Memory Regions
5. Protected Procedure Calls

Summary: simple, easy to use, limited functionality.

10 Anti-assumptions!

The following critical assumptions have **not** been made:

1. Common off the shelf is good enough, just update it.
2. $20x10^6$ Lines Of Code can be made error free with testing when typical error rates are in the region of one per 500-2000 Lines Of Code with perhaps 20% being exploitable.[2]
3. The Essential Eight is the answer, just give me the budget please?
4. VPNs, Air Gaps and Network Filtering are enough!
5. Two Factor Authentication (2FA) will protect us!
6. Support of legacy systems is easy.
7. Formal methods have no place in this, they are too expensive!
8. Micro Kernels are too slow for real time systems
9. The hardware does not need to validated.
10. Version control and accurate logging: who needs it

[2] And yes the author does believe we can produce reliable systems.

Assumptions!

1. seL4 provides a sound base for Laot and is *unique*, **but** seL4 is necessarily complicated whence seL4 Core Platform.
2. So we have built seL4 Core Platform which *weaves* a set of ELF executables and a description in XML into a simple **static** seL4 system.
3. And then Laot is built as a static layer on top of core platform.
4. These ideas can be applied to both protection and active distributed control.

"Newton was a genius, but not because of the superior computational power of his brain. Newton's genius was, on the contrary, was his ability to simplify, idealize, and streamline the world so that it became, in some measure, tractable to the brains of perfectly ordinary men"' - Gerald Weinberg (General Systems Thinking).[3]

[3] Everyone should read this book.

Examples!

1. Flinders Island Wind Turbine: only allow changes to the power setpoint between 0 and 300kW varying at up to 10kW/s.
2. Breakway PLC: what changed in the last week between the demo working and not.
3. Darwin Grid: distributed control of renewable resources in order to get to 100% solar by day no later than 2030 without Amazon Web Services.

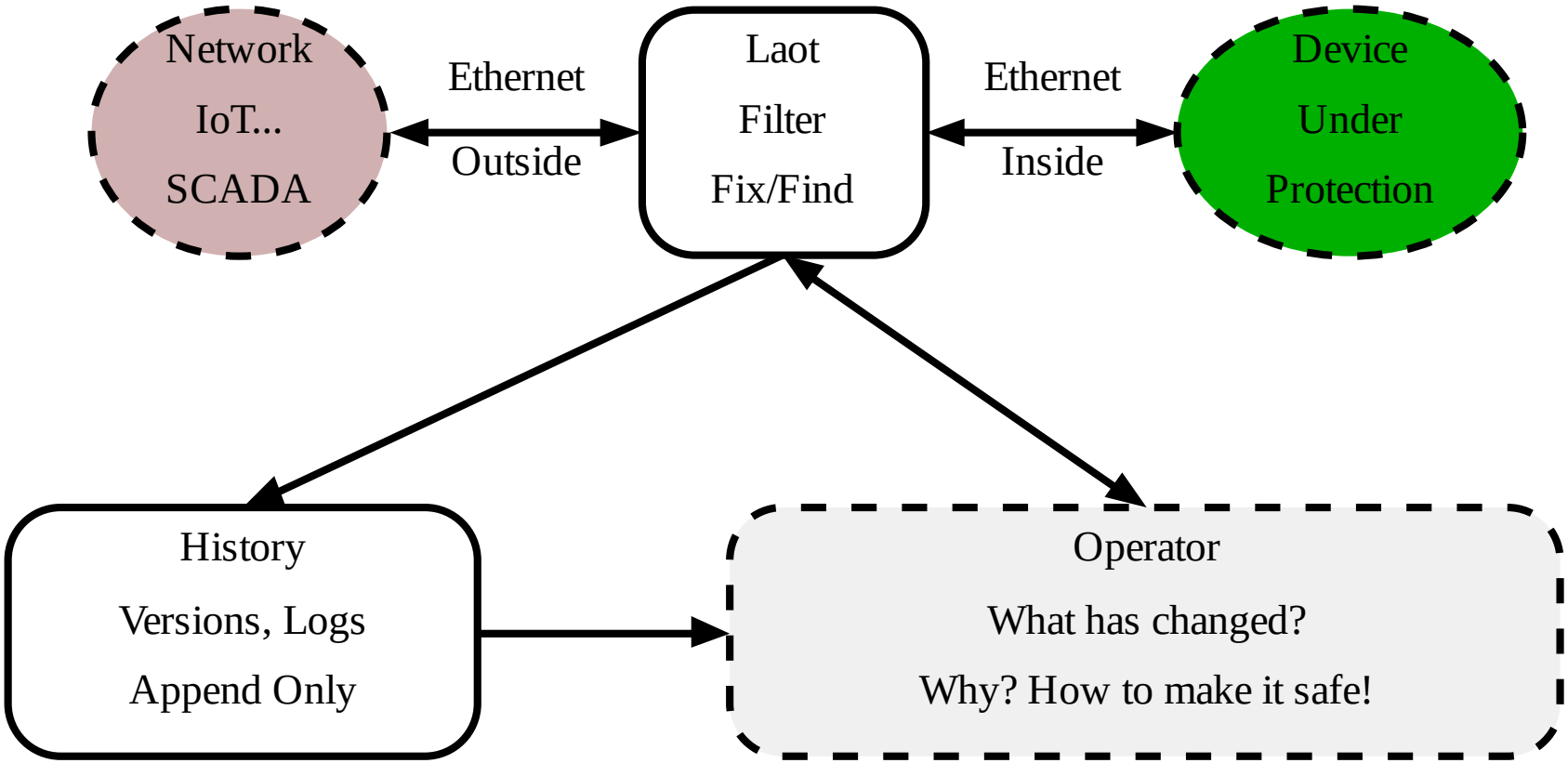
And yes this is a NT talk so we have to have the video/picture of a wee gecko

Intended and unintended Consequences

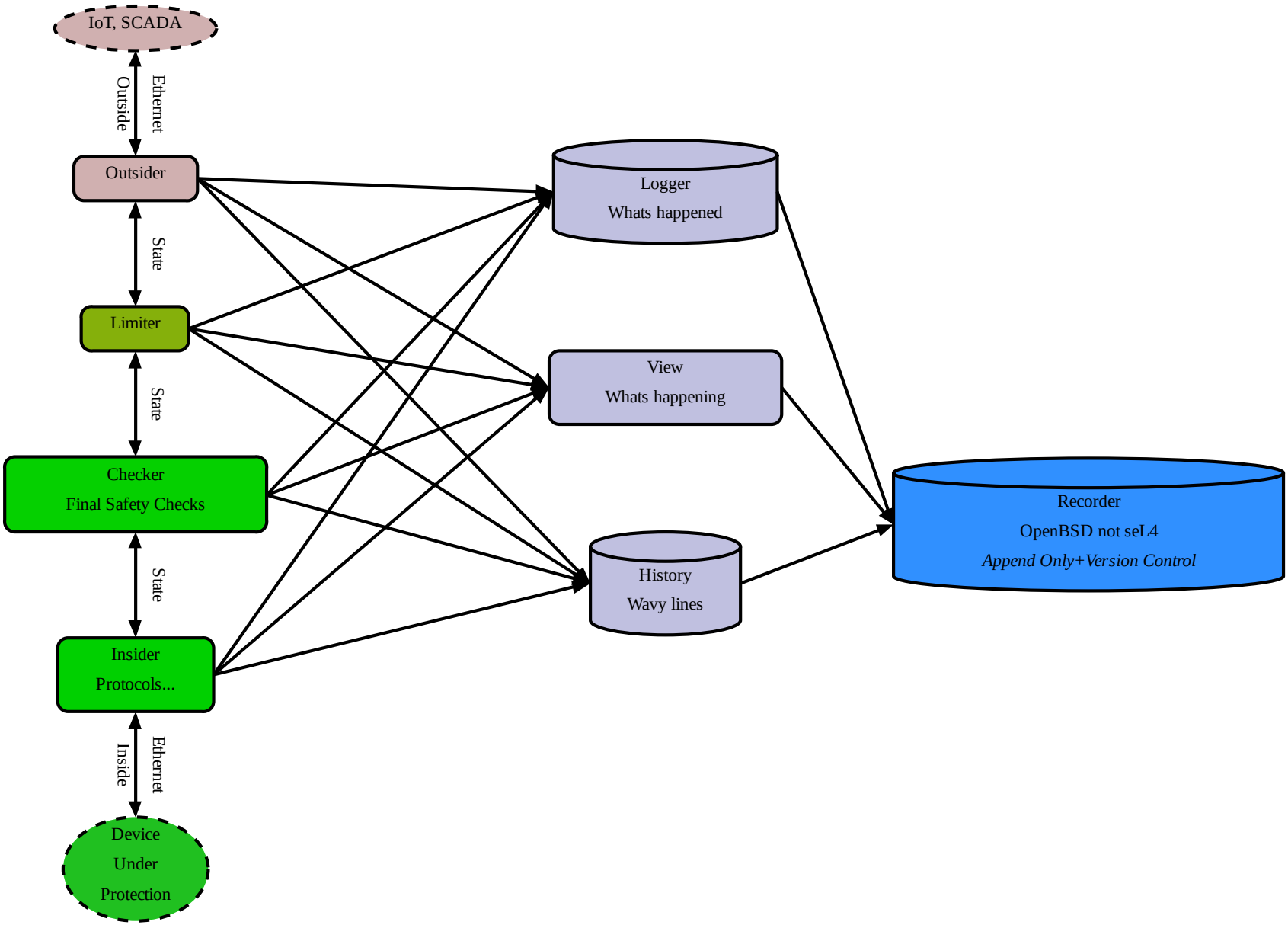
1. **All** traffic goes though the laot device so measurements are reliable, there are no missed samples. (This is unusual!!).
2. System updates can be enabled if and only if someone has physical access.
3. Another use case is a edge of network analyser using the web server.
4. Wireshark on the edge becomes plausible.
5. Safe/limited IEC61131 PLC programming could be implemented.
6. Finally it provides a test for protocol implementations which are often poor.[4]

[4] For example Marc M points out the issue with timing for various non-timing dependent protocols during testing at ACEP.

How


Network
IoT...
SCADA
Ethernet
Outside
Laot
Filter
Fix/Find
Ethernet
Inside
Device
Under
Protection
History
Versions, Logs
Append Only
Operator
What has changed?
Why? How to make it safe!

Details


IoT, SCADA
Outside
Ethernet
Outsider
State
Limiter
State
Checker
Final Safety Checks
State
Insider
Protocols...
Inside
Ethernet
Device
Under
Protection
Logger
Whats happened
View
Whats happening
History
Wavy lines
Recorder
OpenBSD not seL4
Append Only+Version Control

Lessons

On the non-technical side:[5]

[5] Which is the important one!

Lessons

On the non-technical side:[5]

1. When presented at the operator level: great.
2. When presented at the middle manager level: fair enough.

[5] Which is the important one!

Lessons

On the non-technical side:[5]

1. When presented at the operator level: great.
2. When presented at the middle manager level: fair enough.
3. When presented to the IT department: feel free to die.

As an ex-academic (well as an older one) I think that we have *failed* in teaching people about the importance of reliability, simplicity or formal methods.

[5] Which is the important one!

Questions for the audience?

1. What are the key questions/critical assumptions?

[6] FWIW there is a theme running from OS-ACS in the 80's, GNU Nana in the 90's, MAGPIE in the 2000's and Laot in the 2020's.

Questions for the audience?

1. What are the key questions/critical assumptions?
2. Have they been answered, if so by who?

[6] FWIW there is a theme running from OS-ACS in the 80's, GNU Nana in the 90's, MAGPIE in the 2000's and Laot in the 2020's.

Questions for the audience?

1. What are the key questions/critical assumptions?
2. Have they been answered, if so by who?
3. Is Microsoft Azure the answer?

[6] FWIW there is a theme running from OS-ACS in the 80's, GNU Nana in the 90's, MAGPIE in the 2000's and Laot in the 2020's.

Questions for the audience?

1. What are the key questions/critical assumptions?
2. Have they been answered, if so by who?
3. Is Microsoft Azure the answer?
4. Should the Darwin Katherine Grid be controlled by AWS.

[6] FWIW there is a theme running from OS-ACS in the 80's, GNU Nana in the 90's, MAGPIE in the 2000's and Laot in the 2020's.

Questions for the audience?

1. What are the key questions/critical assumptions?
2. Have they been answered, if so by who?
3. Is Microsoft Azure the answer?
4. Should the Darwin Katherine Grid be controlled by AWS.
5. How should we build a distributed power system and why was MAGPIE a semi-failure :-).[6]

[6] FWIW there is a theme running from OS-ACS in the 80's, GNU Nana in the 90's, MAGPIE in the 2000's and Laot in the 2020's.

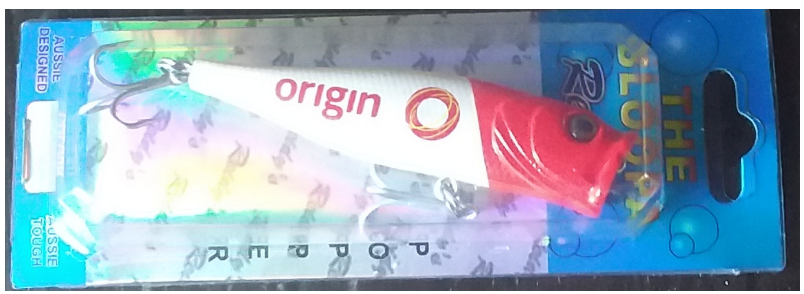
Questions for the audience?

1. What are the key questions/critical assumptions?
2. Have they been answered, if so by who?
3. Is Microsoft Azure the answer?
4. Should the Darwin Katherine Grid be controlled by AWS.
5. How should we build a distributed power system and why was MAGPIE a semi-failure :-).[6]

[6] FWIW there is a theme running from OS-ACS in the 80's, GNU Nana in the 90's, MAGPIE in the 2000's and Laot in the 2020's.

Questions for the audience?

1. What are the key questions/critical assumptions?
2. Have they been answered, if so by who?
3. Is Microsoft Azure the answer?
4. Should the Darwin Katherine Grid be controlled by AWS.
5. How should we build a distributed power system and why was MAGPIE a semi-failure :-).[6]
6. **Who gets the lure?**



[6] FWIW there is a theme running from OS-ACS in the 80's, GNU Nana in the 90's, MAGPIE in the 2000's and Laot in the 2020's.

Conclusion/Summary

1. So where are we up to? (prototype exists, initial deliverables complete, seL4 Core Platform ready to go).
2. Is this a good idea? (Phil thinks so).
3. Do we need a *Trusted Power Systems Group*, perhaps with ACEP or . . . ?
4. Happy to do a detailed technical presentation at your convenience today or later.

"We do not influence the course of events by persuading people that we are right when we make what they regard as radical proposals.
Rather, we exert influence by keeping options available when something has to be done at a time of crisis." – Milton Friedman

Further Reading

Any links will be accepted as Master Po would expect.

1. seL4 - seL4 project page.
2. Core Platform - well worth a read, it is short.
3. Laot Pub - project overview
4. EDS - some projects on energy related things.
5. ACEP - the Alaska Center For Energy and Power.
6. Goto Fail: and Phil as the accumulator
7. REMHART - Charles Darwin University noting that Laot was first tested here.
8. Laot Quotes - well a reference to our masters.
9. EWD397: Self Stablising Systems with Distributed Control - this relates to the use of Laot in distributed power grids.
10. EDS Talks - a few talks on power systems including SET-101, PV-DIESEL-101. EDS Books might also be of interest.

Finally feel free to drop the author an email or call.