The Nightmare of Securing a Multi-Purpose Computer Centre

Dr. Stefan.Lueders@cern.ch
CERN Computer Security Team

pre-GDB workshop on
data-centre network architectures
2021/6/7

The Three Mantras of Cyber-Security

1. “Convenient, cheap, secure --- Pick two”:
No wonder that “security” looses as it brings no immediate benefits.

2. “KISS --- Keep it simple, stupid”:
Avoid over-complication, too much complexity & too many deviations from or exceptions to the “standard”.

Unfortunately, it is the **complexity of today’s IT infrastructures which makes security a nightmare.**

3. “Defense in Depth”:
Protective means must be deployed at every level of the H/W & S/W stack, e.g.

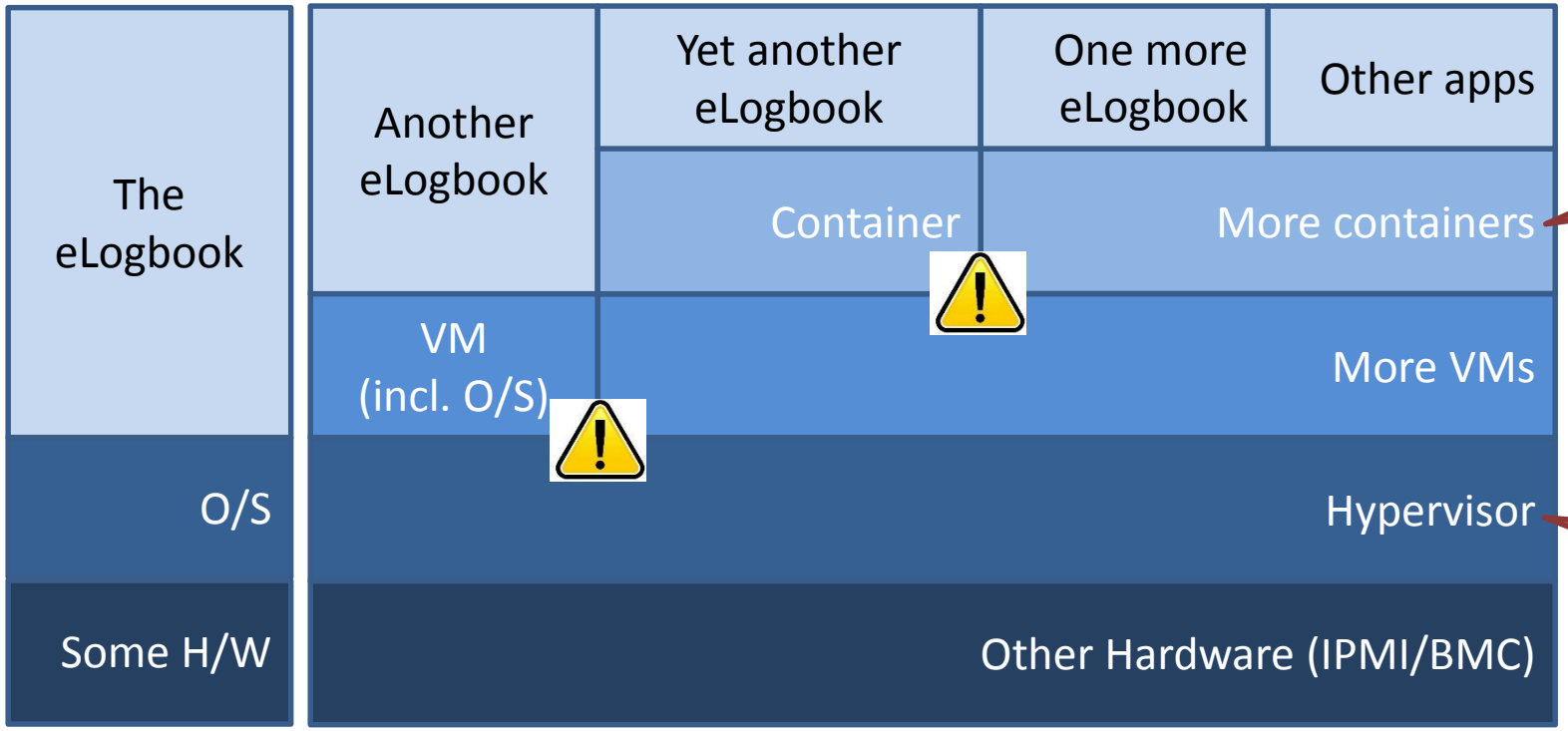
- Agile and timely updating, secure & professional S/W development, tested business continuity plans & disaster recovery means, logging & IDS, …
- Network segregation & compartmentalization, firewalls, bastion hosts, gateways & proxies

Disclaimer: No, I don’t have the ultimate truth. I hardly even understand 100% of the problem.

Just one Example: A web-based eLogbook

Another Disclaimer: I will not discuss best-practices of securing H/W & S/W components themselves:

- Vulnerability management & patching, business continuity & disaster recovery
- Secure software development, input sanitization & filtering
- Access control, AuthN & AuthZ, eligibilities, …



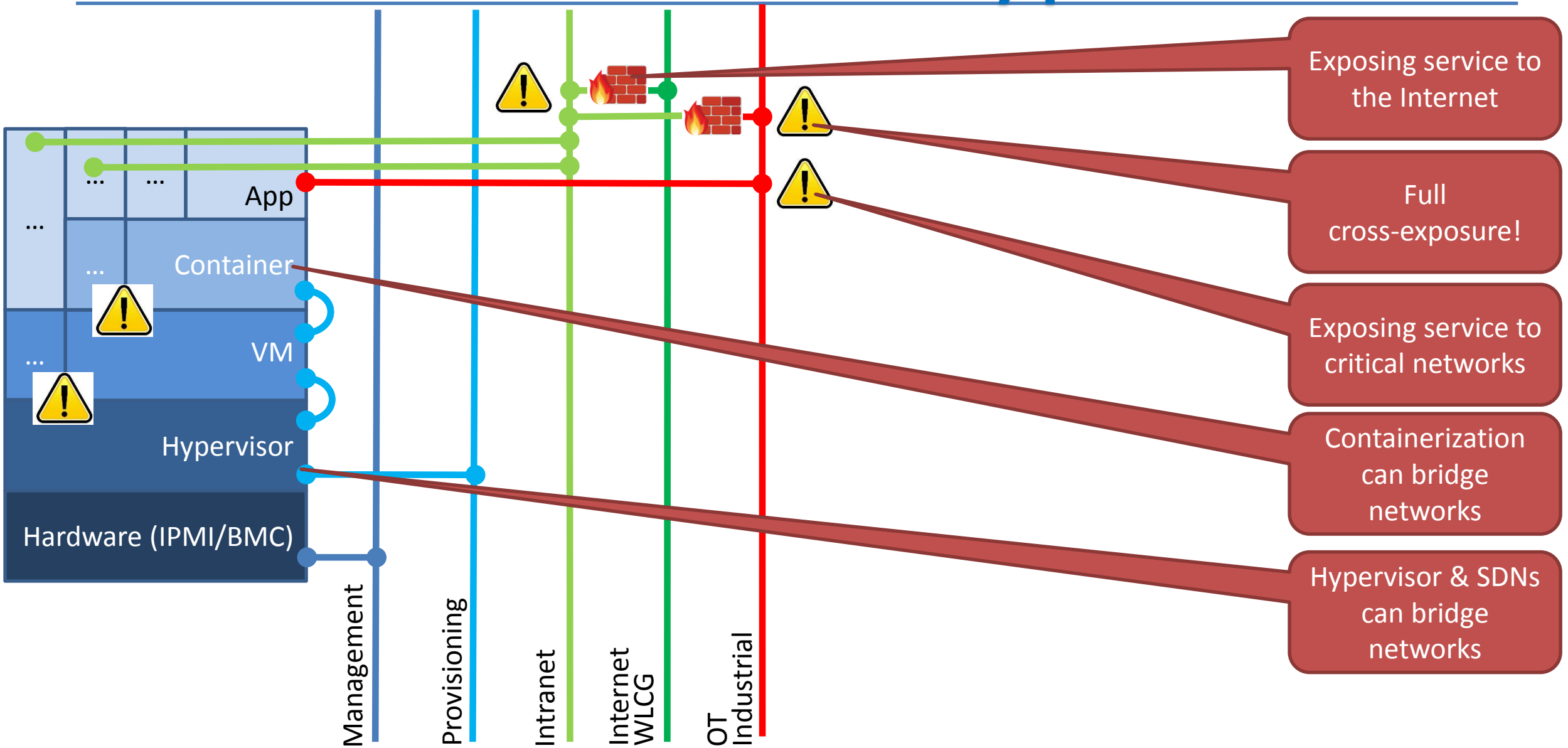
Containerization can host completely different services

Alternative: Full separation, but this kills elasticity

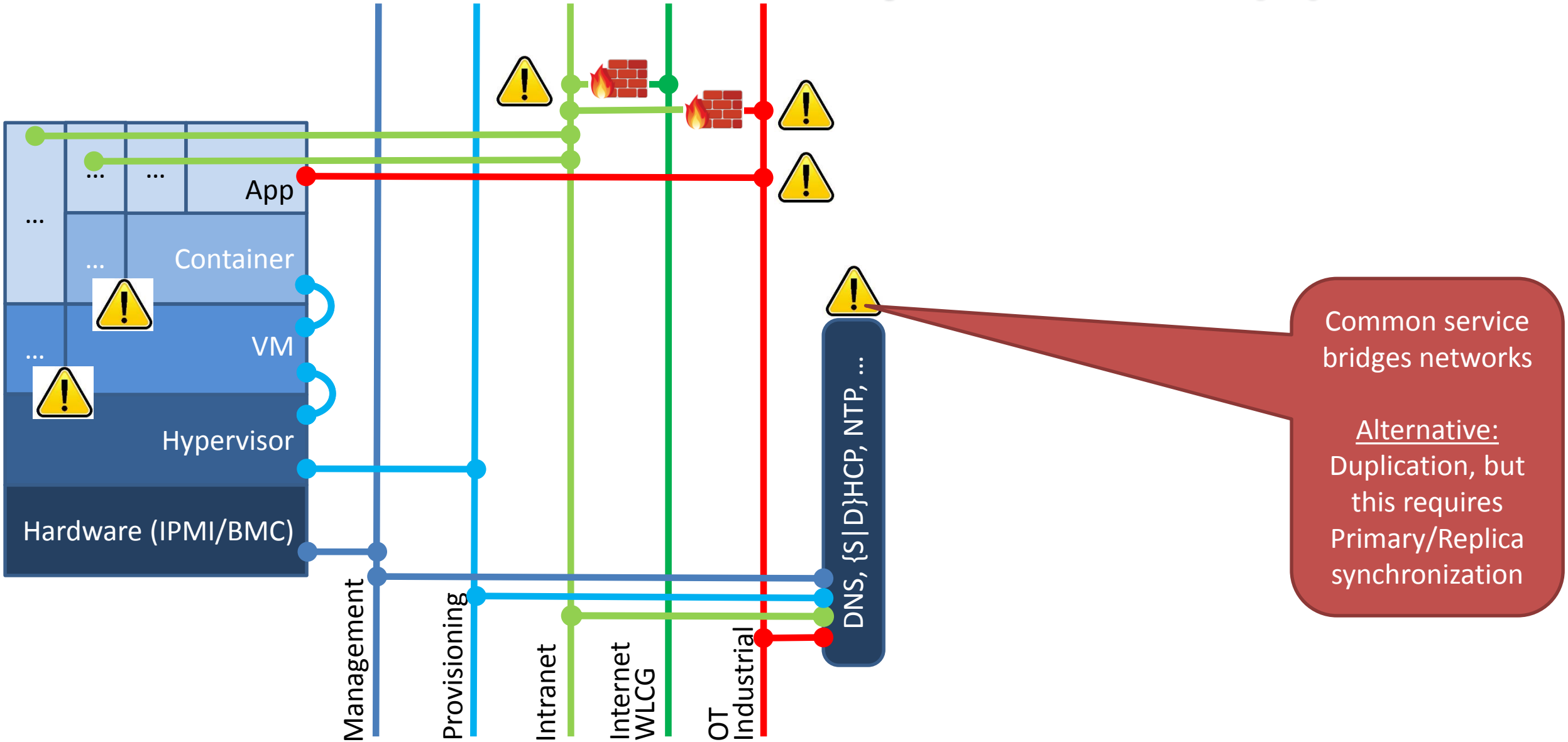
Hypervisor can host completely different services

Alternative: Full separation, but this kills elasticity

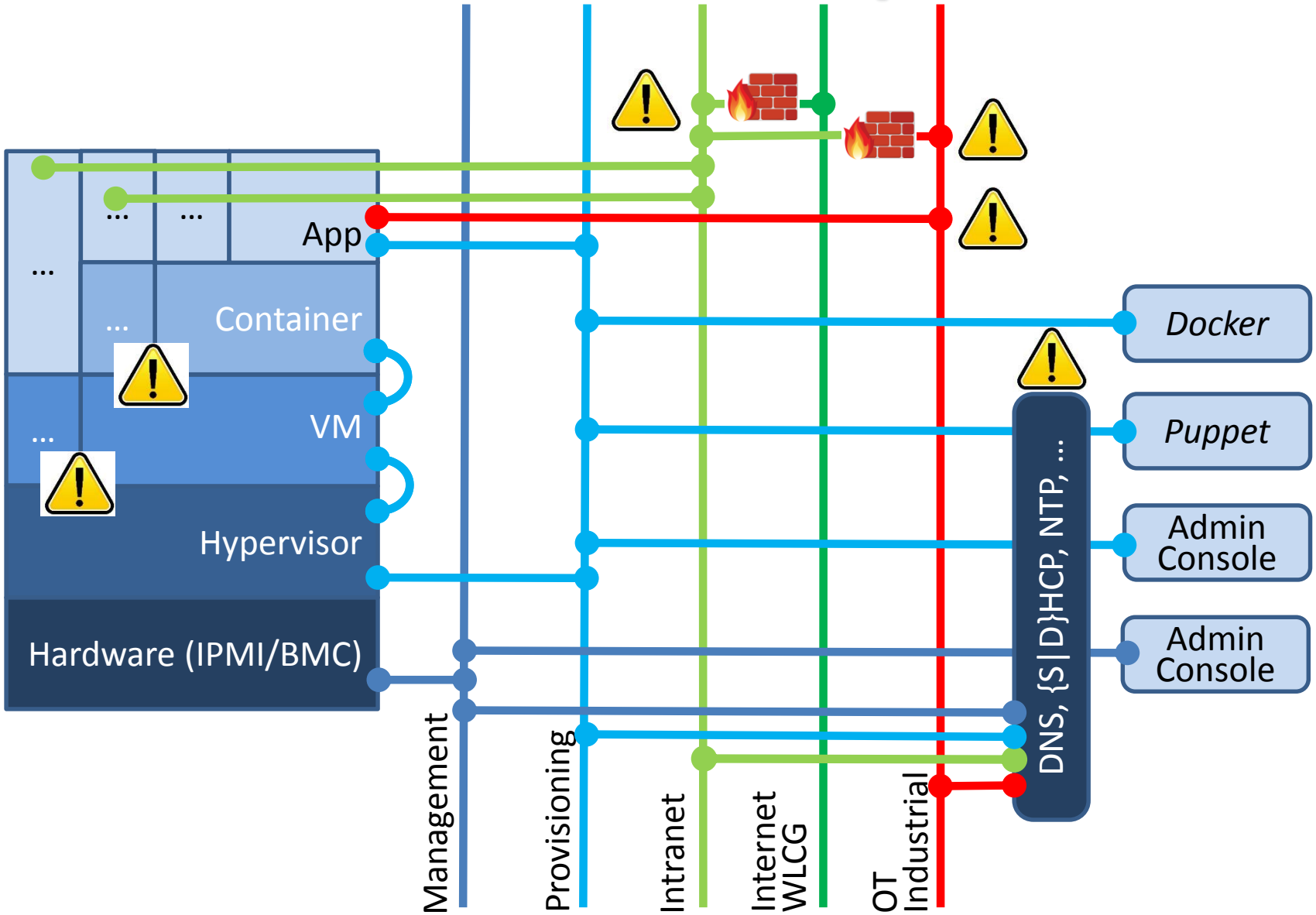
Ideal network stack already problematic



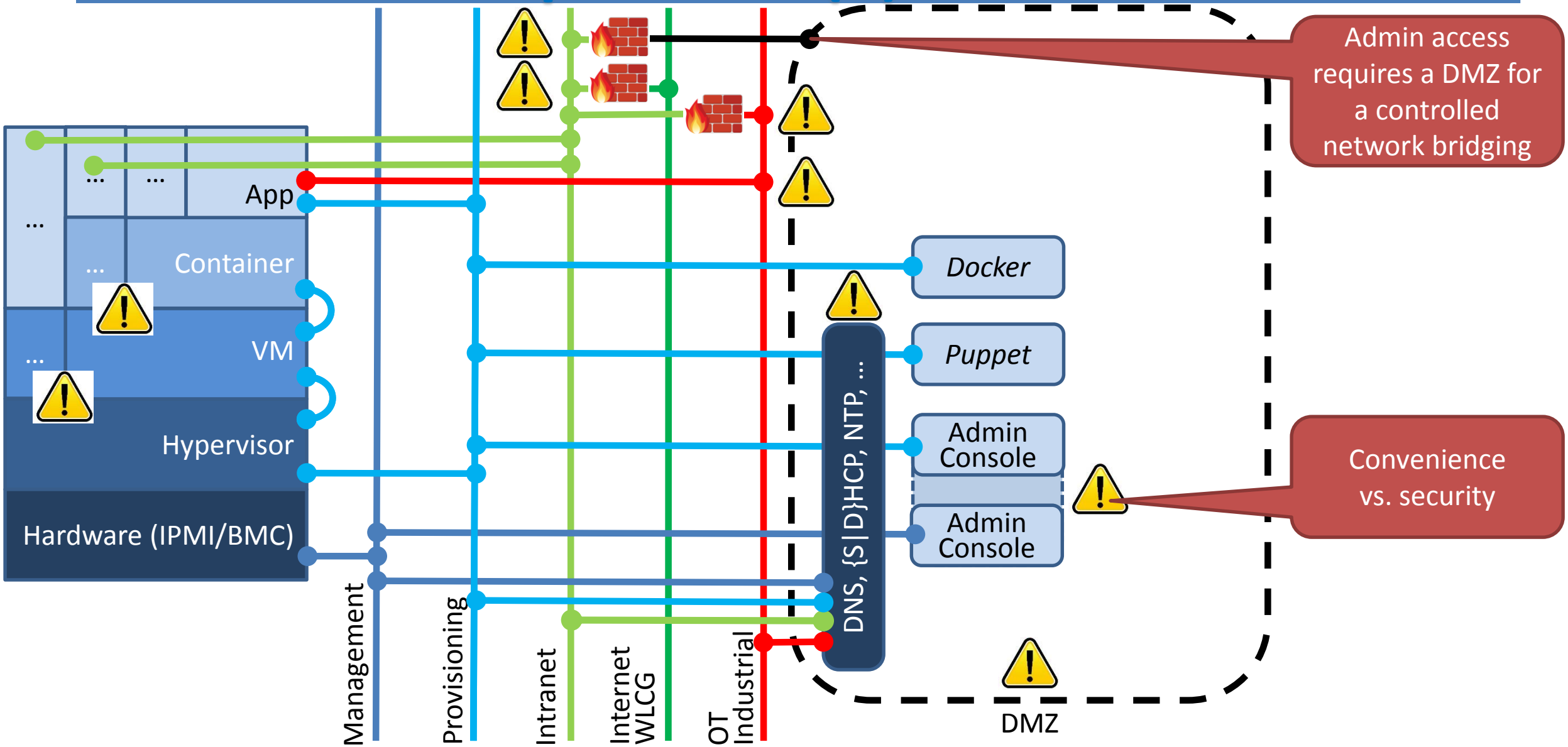
Here come some Dependencies (1)



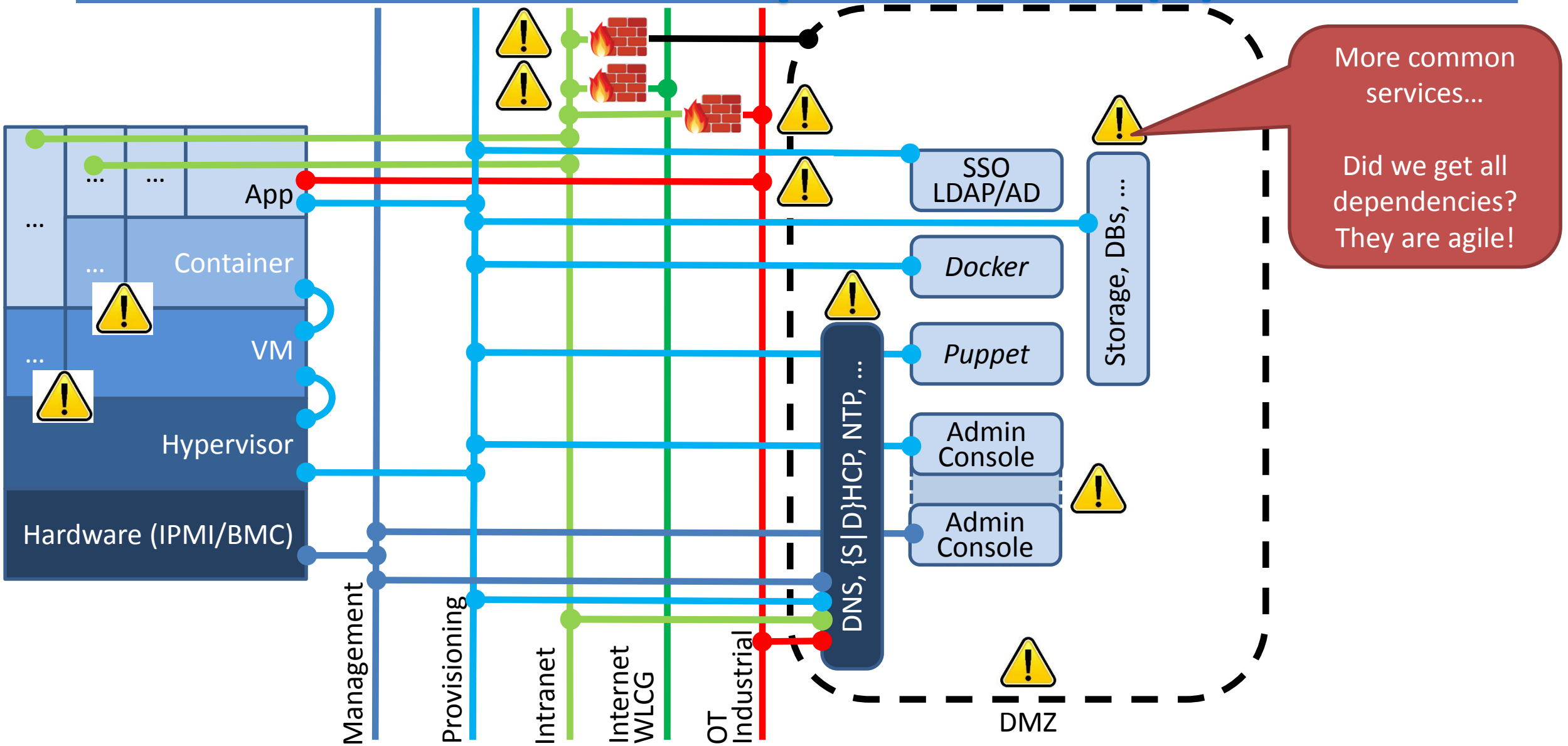
More Dependencies (2)



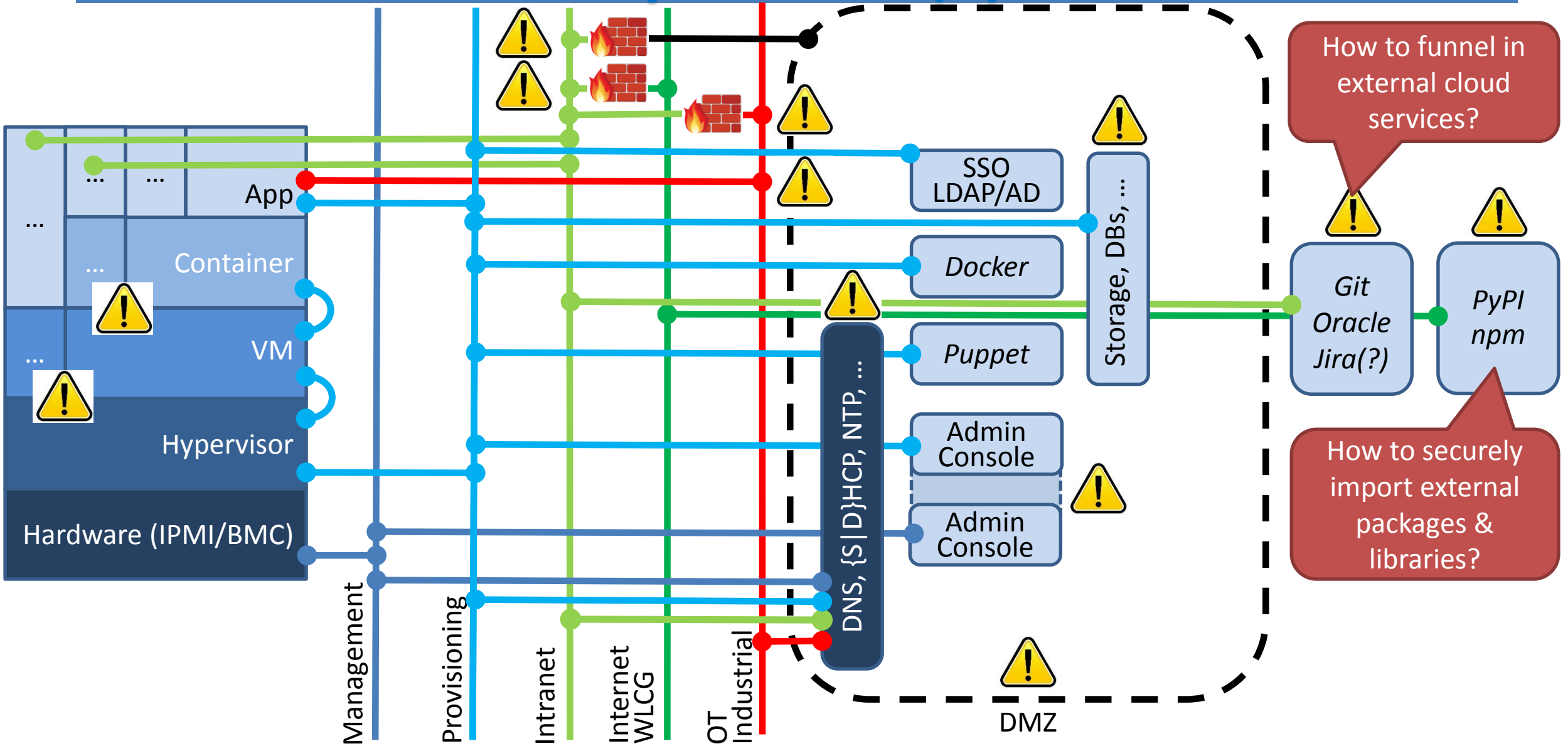
Complication (1): Admins!



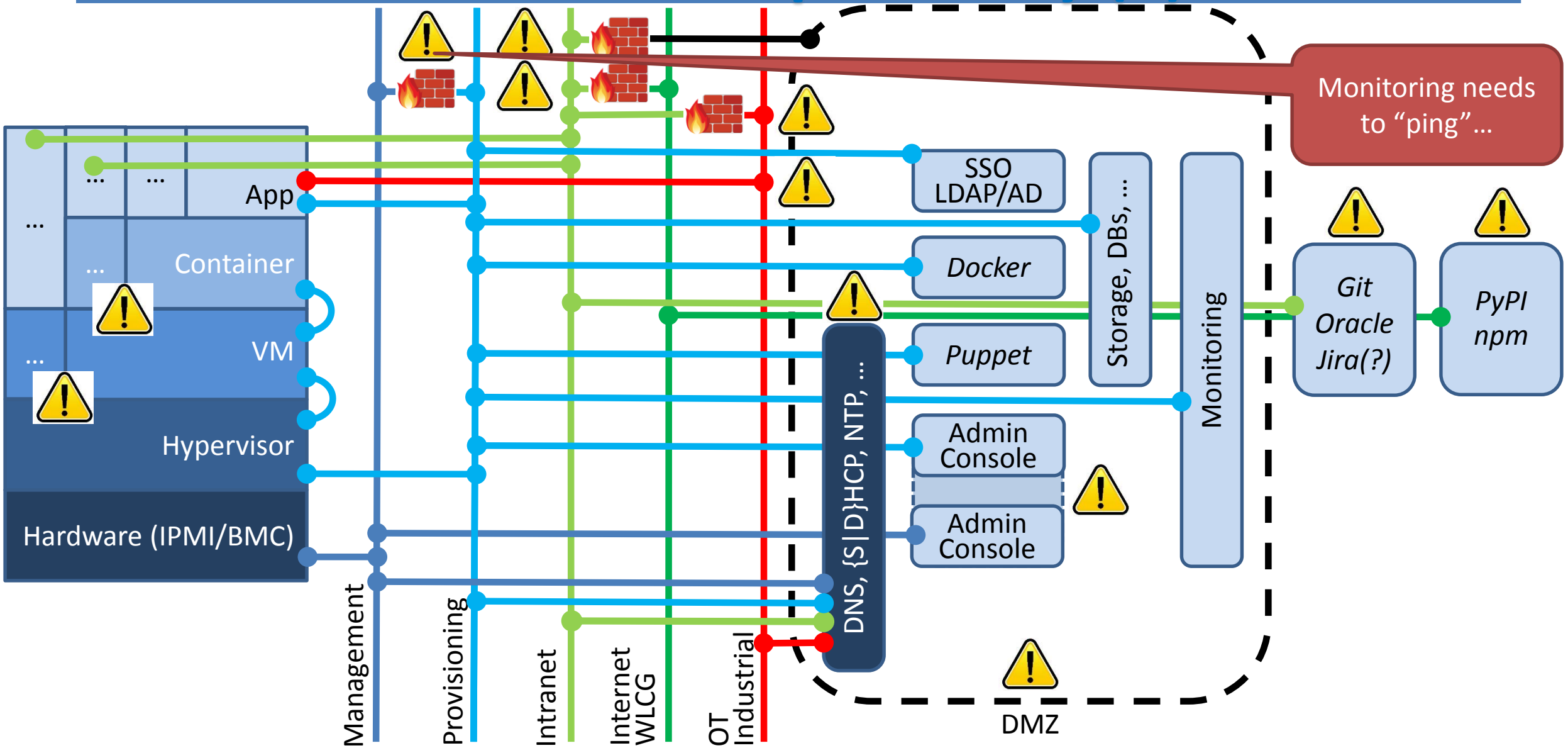
And more Dependencies (3)



Next Complication (2): Clouds



One final Dependency (4)



Summary (for your Nightmares)

This got damn complex, complicated and convoluted.

The Risks:

- Hypervisors, container platforms & alike when serving different networks as they bypass any firewalling
- Multi-purpose applications (Intranet, Internet, WLCG, OT) as those require tight firewalling
- High risk networks (e.g. OT) requiring even tighter firewalling, proxies, gateways, and data diodes
- Common services (e.g. for provisioning or monitoring) as they bridge different networks
- A quickly growing DMZ. At CERN, the Meyrin CC is considered to be *the* DMZ…
- …and a cacophony of dependencies, agile, quickly changing, and adding more complexity
- External cloud services (Git, Oracle, Jira?, …) adding uncontrolled complexity governed just by contracts
- External S/W dependencies (through Github or usage of PyPI/npm) unless S/W is verified and curated

The solution:

www.cern.ch

Thank you very much!