Case Study

Equipment Resiliency in a Critical Infrastructure environment

-Achieving millisecond failover times in a critical process environment

Kirk Reid

Industrial Controls & Cybersecurity specialist

TC Energy

Agenda

- Introductions
- Safety Moment
- What is this all about?
- History of the issue / What has changed
- Typical site diagram
- Options:
  - Flex Links
  - Spanning Tree
  - REP
  - Routing ECMP/OSPF/IS-IS/EIGRP
  - VX Lan
  - Switch Stacking/Etherchannel
- Final Solution & Conclusions

Introductions

Kirk Reid

Industrial Controls & Cybersecurity Specialist

- 30 years of experience in IT, specializing for the past 20 years of networking and security.
- For the last 8 years at TC, Kirk has been leading the modernization of their IT and OT networks across 7000 sites in North America.

Dangers of Li-on/Rechargeable Batteries

Lithium rechargeable batteries have made rechargeable devices increasingly common, but poor manufacturing practices of such batteries have caused numerous accidents and fires.

Examples of these include:

- The infamous **Samsung Note 7**s. After 35 reported overheating incidents, they are now "considered a hazmat product, and are prohibited from being taken on-board at many airlines and bus stations."[1]
- **Hoverboards**. The U.S. Consumer Product Safety Commission(CPSC) claims there have been more than 250 incidents caused by hoverboard fires since 2015, resulting in 2 deaths, 13 burn injuries, three smoke inhalation injuries, and more than $4 million in property damage. By June of 2016, 501,000 self-balancing scooters had been recalled.[2]

As of May 22, 2019, **258** air/airport incidents involving lithium-ion batteries carried as cargo or baggage have been recorded since March 20, 1991.[3]

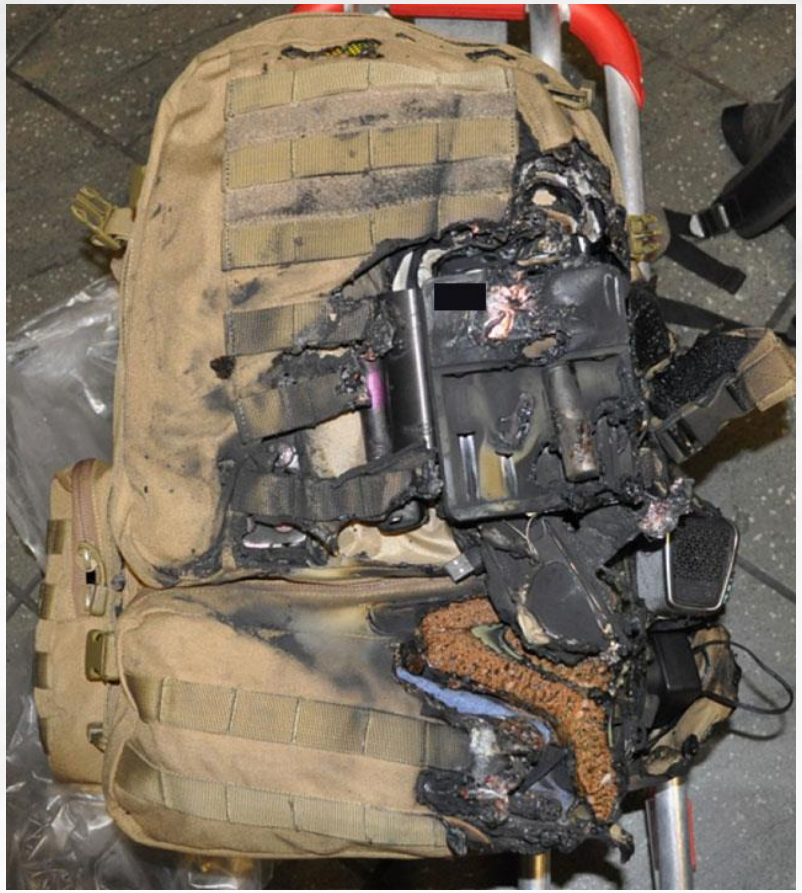
[1] https://en.wikipedia.org/wiki/Samsung_Galaxy_Note_7
[2] https://www.cpsc.gov/Safety-Education/Safety-Education-Centers/hoverboards
[3] https://www.faa.gov/hazmat/resources/lithium_batteries/media/Battery_incident_chart.pdf

C-GWJT, Calgary, Alberta, 14 June 2018

Flight WJA113 declared a **MAYDAY** emergency and returned to YYC airport 3 minutes after takeoff after a cargo fire was detected.

One passenger inadvertently packed 2 spare lithium-ion batteries for his e-cigarette, in the charger, in the front pocket of his checked bag. He, aware of WestJet's policies of restricted items in checked baggage, had carried-on his e-cigarette and 2 other lithium-ion batteries.

The Transportation Safety Board of Canada (**TSB**) conducted an investigation following the incident. The engineering report concluded that 1 battery in the charger experienced a **thermal runaway** and the interior material of the battery was completely burnt out.



http://www.bst-tsb.gc.ca/eng/rapports-reports/aviation/2018/a18w0081/a18w0081.html

What is this all about?

About 650 km east of here

This supplies gas to Eastern Canada

BIG site (almost 1km wide)

How was this done before?

- Everything hard wired
- Onsite spares
- Onsite support

What has changed,

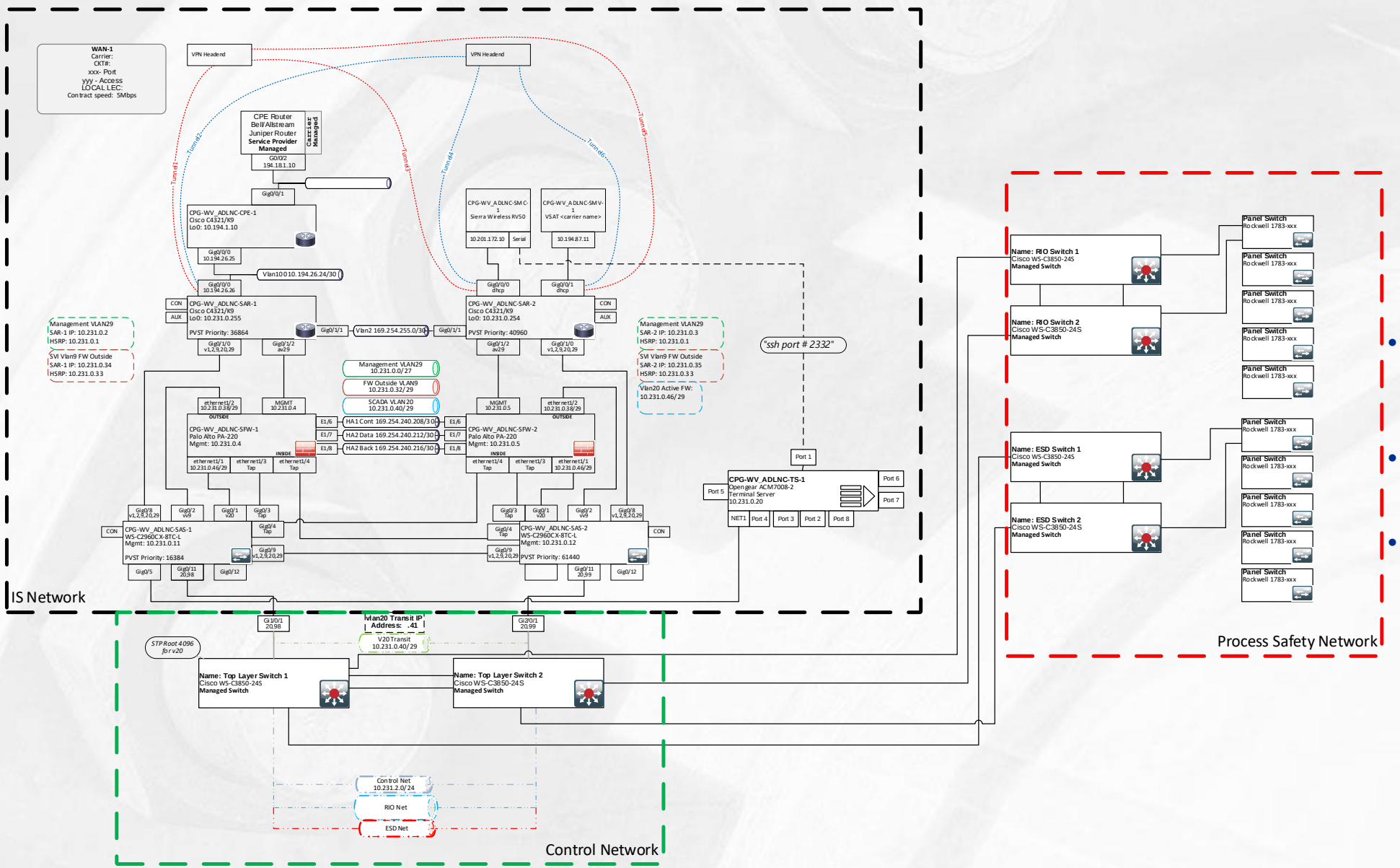
Changes over the past 20 years

- Wiring skills are becoming uncommon
- Drive to improve reliability and do more with less (people and $)
- Automation & instrumentation is moving to more and more to communication via ethernet
- Fiber failures are common (30+ year old fiber)
- Copper failures are common, failover convergence take seconds
- Switch full failures are more common than switches hanging

Guiding Principles

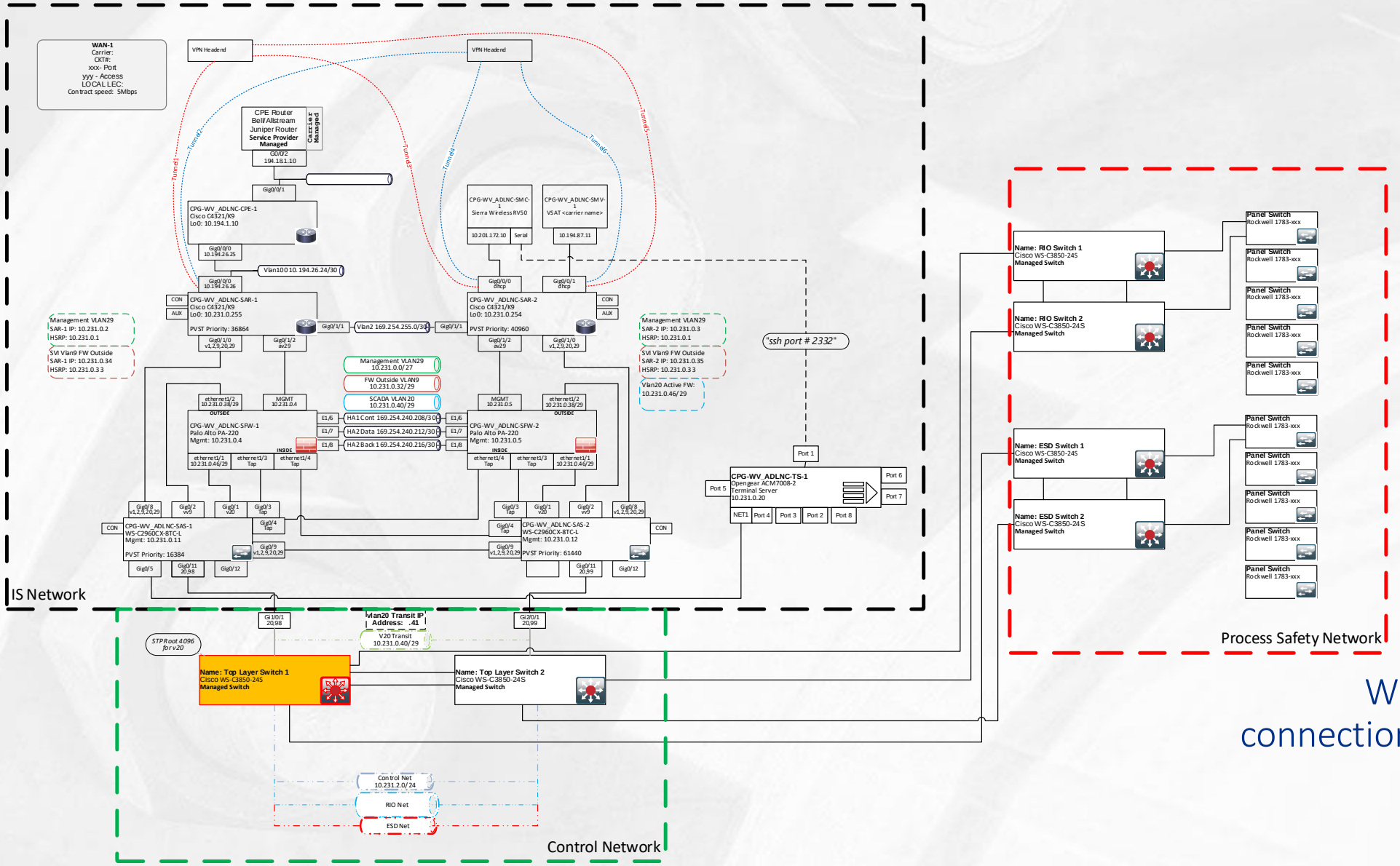
- Simple, supportable solutions are essential for Critical Infrastructure environments
- What works in a lab doesn’t necessarily work in practice

Typical site diagram

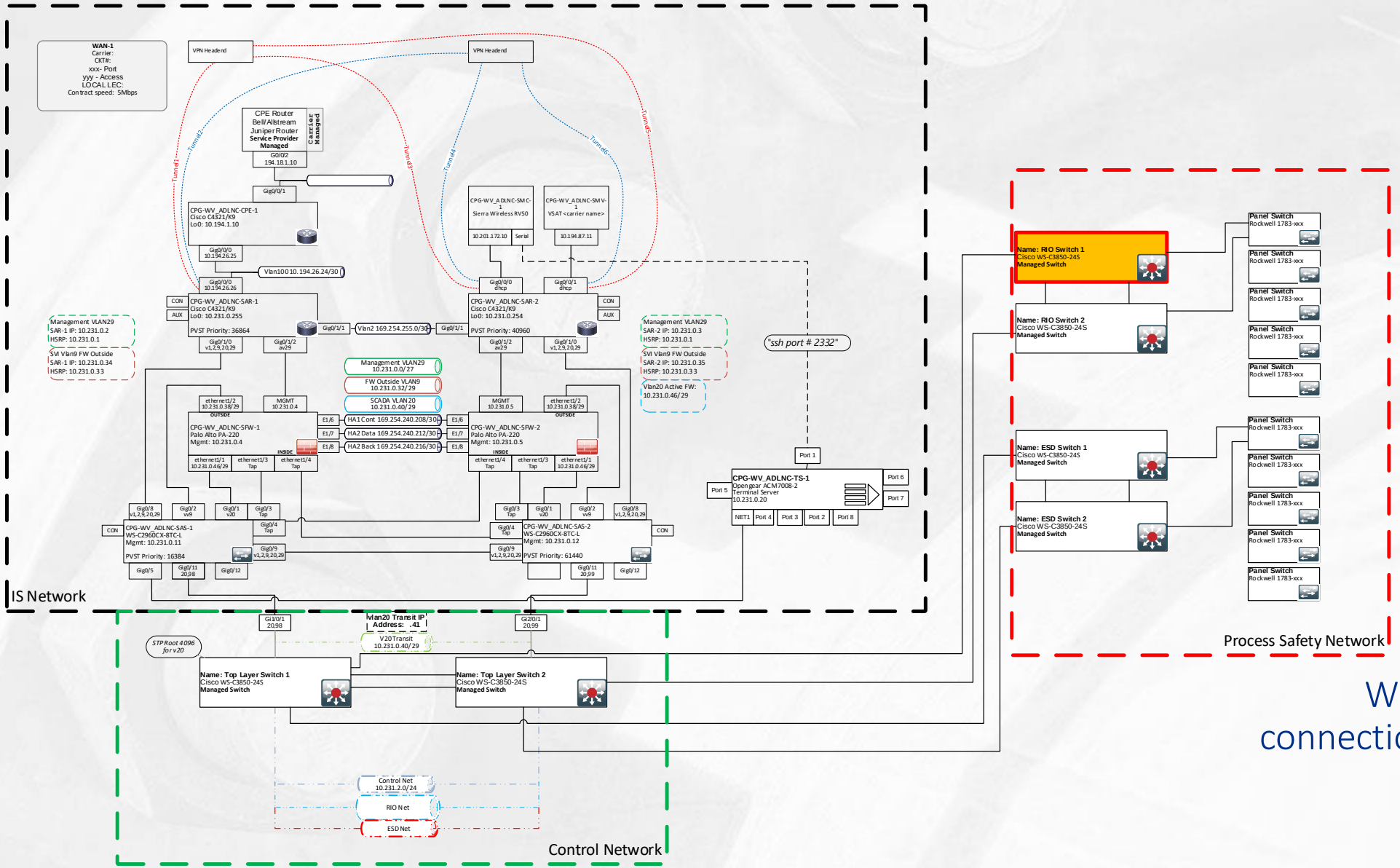


- IS Network: Connectivity to SCADA
  - MTTR: 30 mins
- Control Network: HMI
  - MTTR: 1 min
- Process Safety Network: PLC, RIO, ESD, MCC
  - RIO: Remote IO
  - ESD: Emergency Shutdown
  - MCC: Motor Control
  - MTTR: 100 ms

Problem: What if a core switch fails?

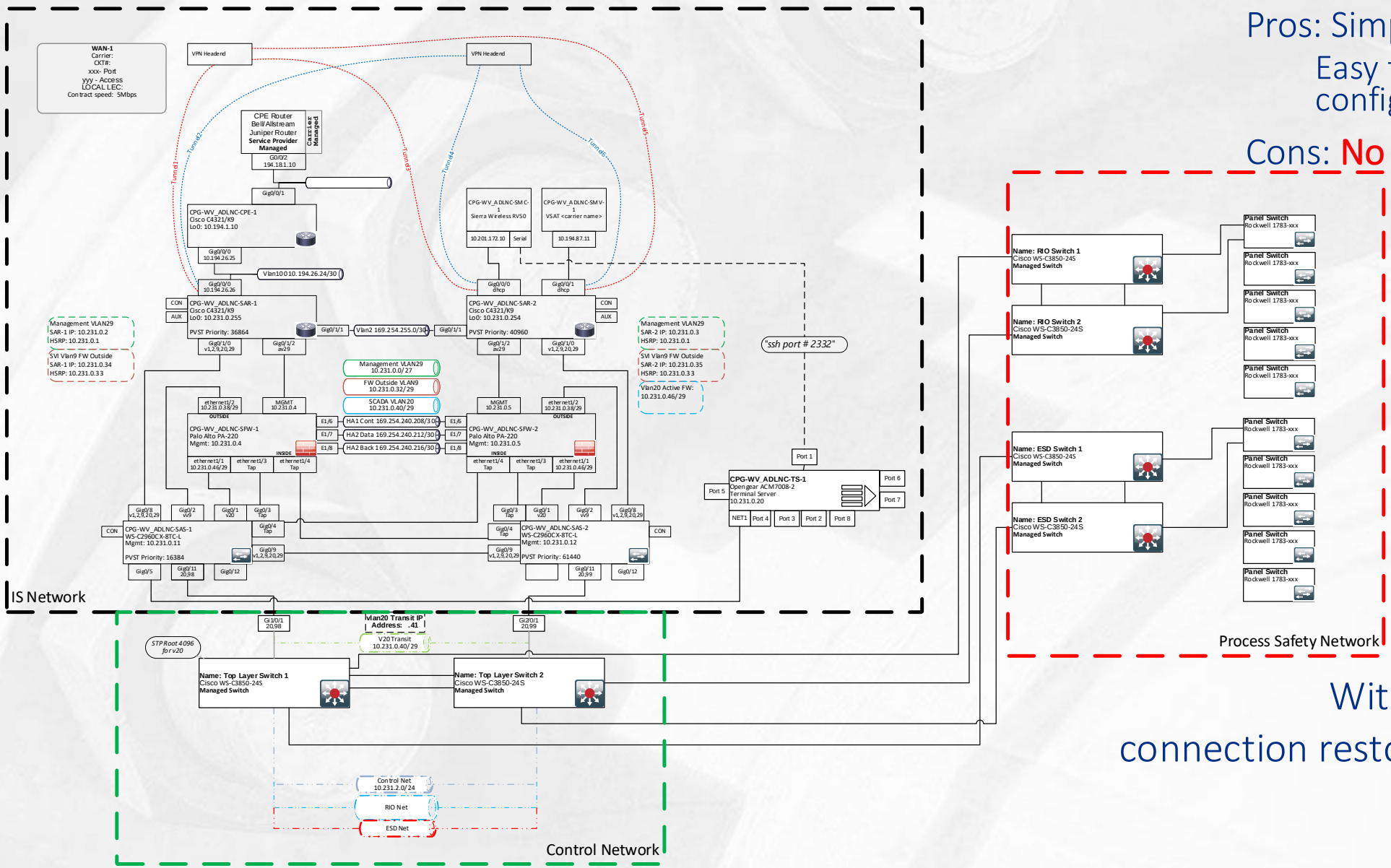


Problem: RIO switch failure



Without configuration,
connection restored in 45 sec
Site will shutdown

Option: Flex Links (Cisco)

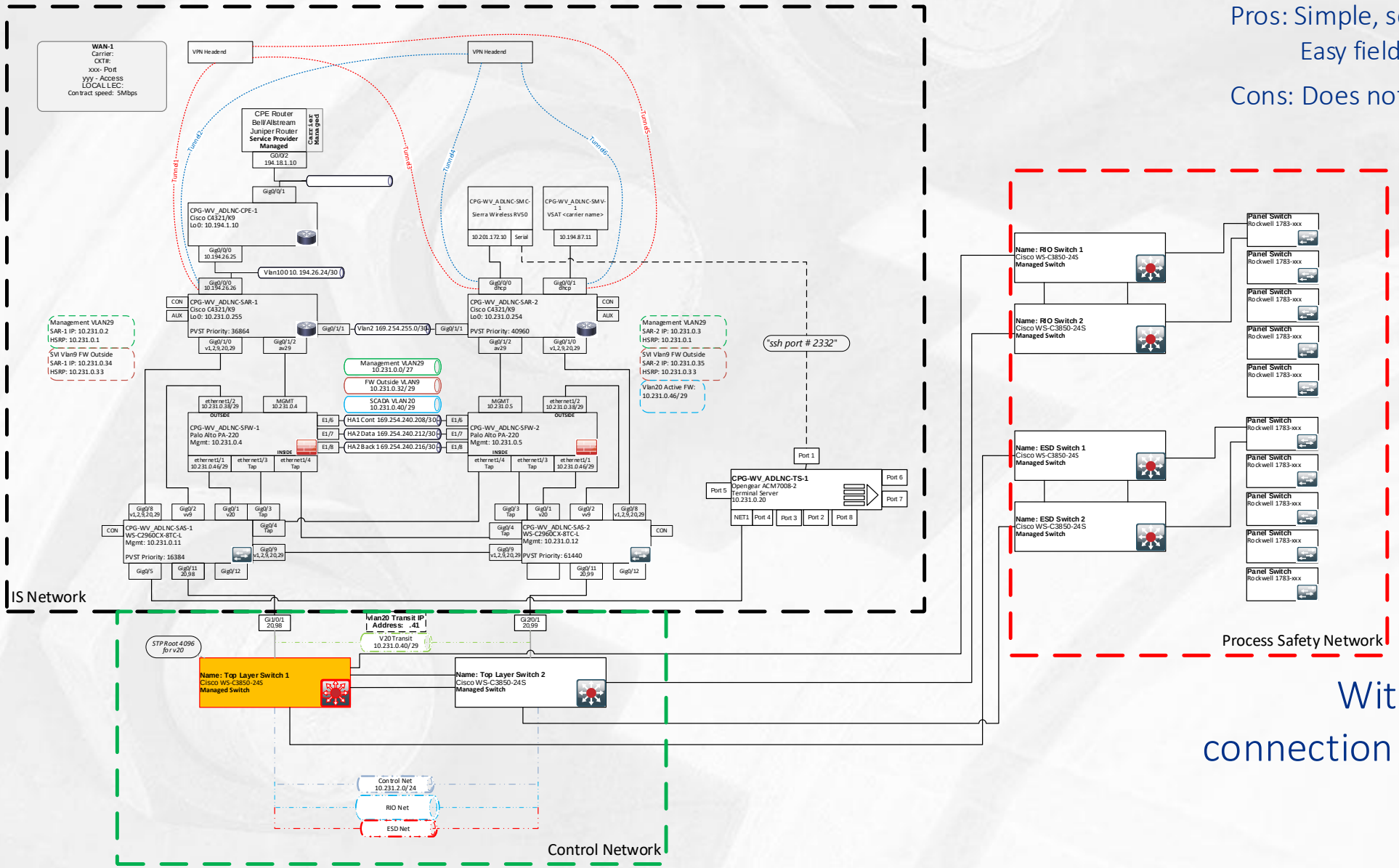


Pros: Simple, scalable, Easy field device configurations

Cons: No longer supported

With configuration, connection restored in <100 ms

Option: Spanning Tree (MST/Rapid)

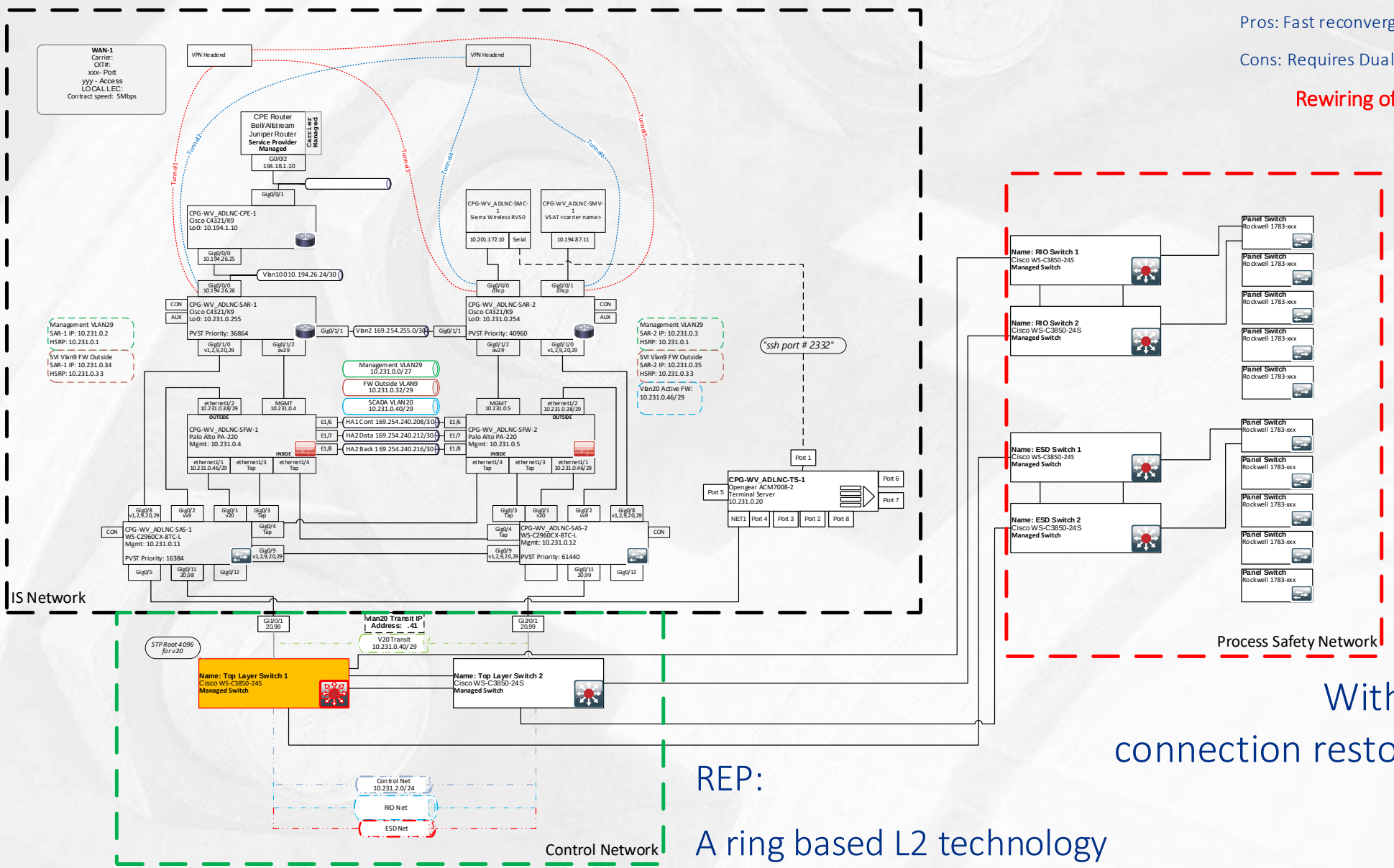


Pros: Simple, scalable,
Easy field device configurations

Cons: Does not converge fast enough

With configuration,
connection restored in <1 s

Option: REP



Pros: Fast reconvergence

Cons: Requires Dual ring topology, not star wiring.

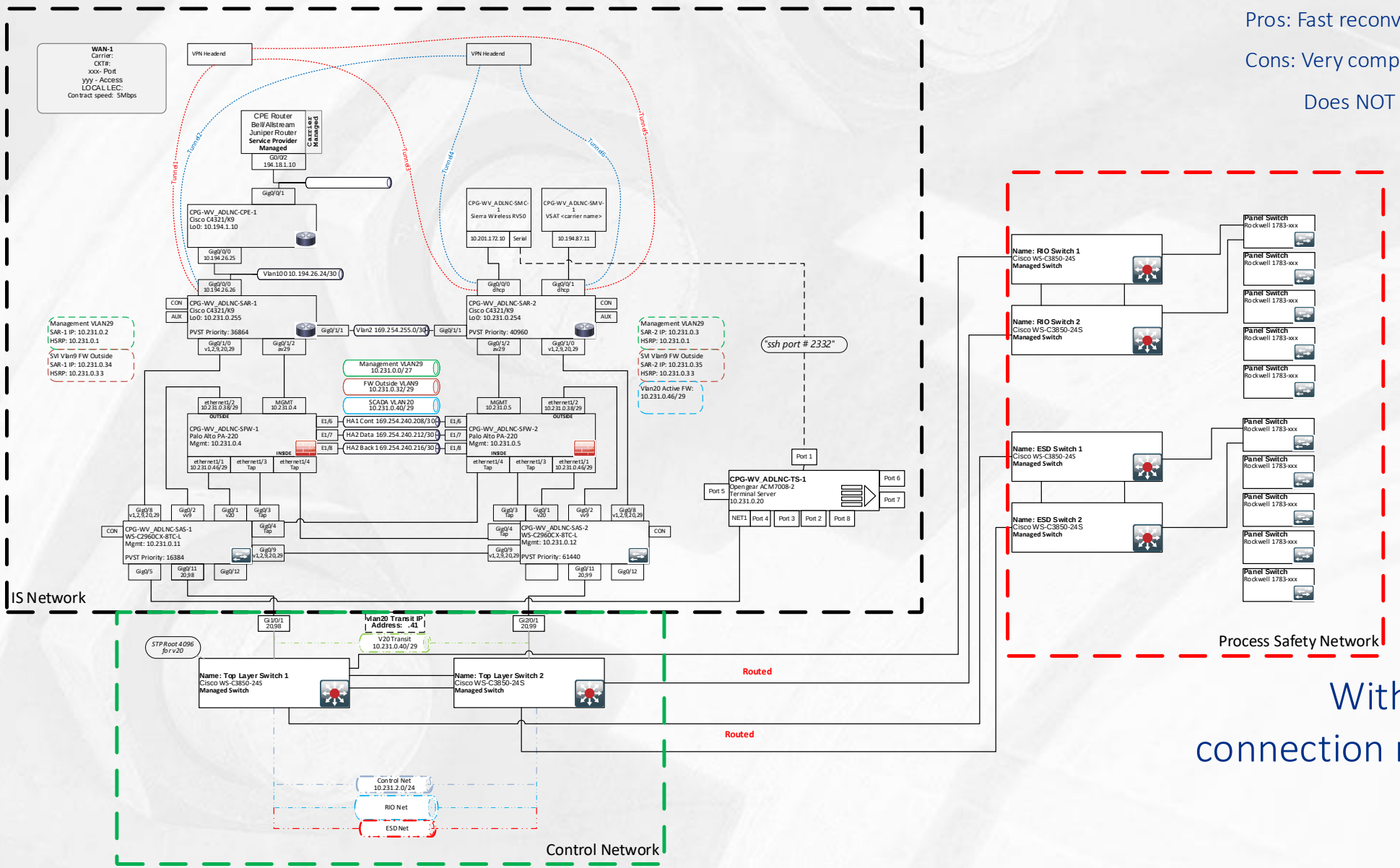
Rewiring of sites required $$$$

With configuration, connection restored in <150 ms

REP:

A ring based L2 technology

Option: Can we use micro-segmentation (ECMP/Routing)



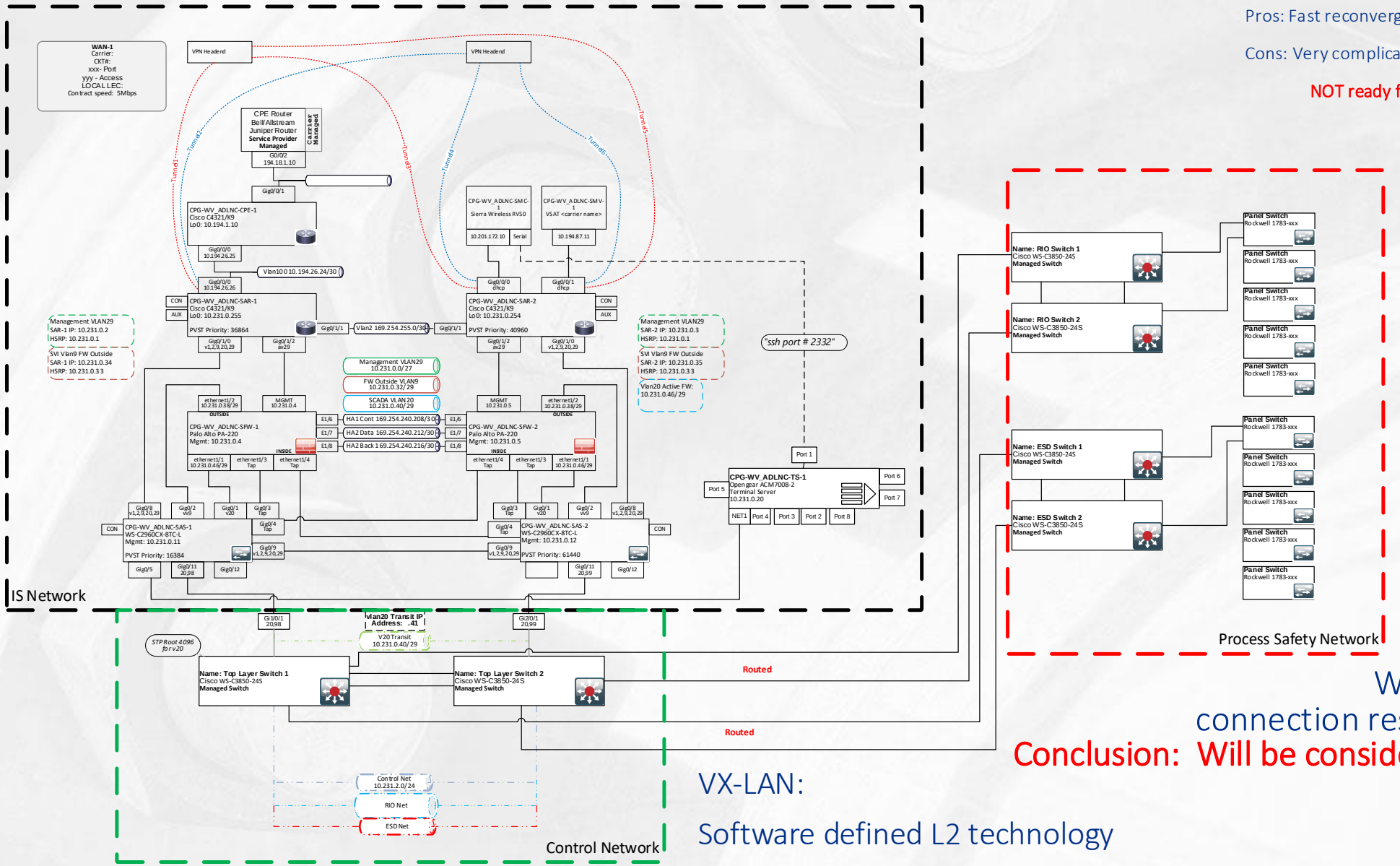
Pros: Fast reconvergence

Cons: Very complicated field device configs

Does NOT mitigate RIO device failure

With configuration, connection restored in <1 s

Option: VX-LAN



Pros: Fast reconvergence

Cons: Very complicated switch configurations

NOT ready for Life safety

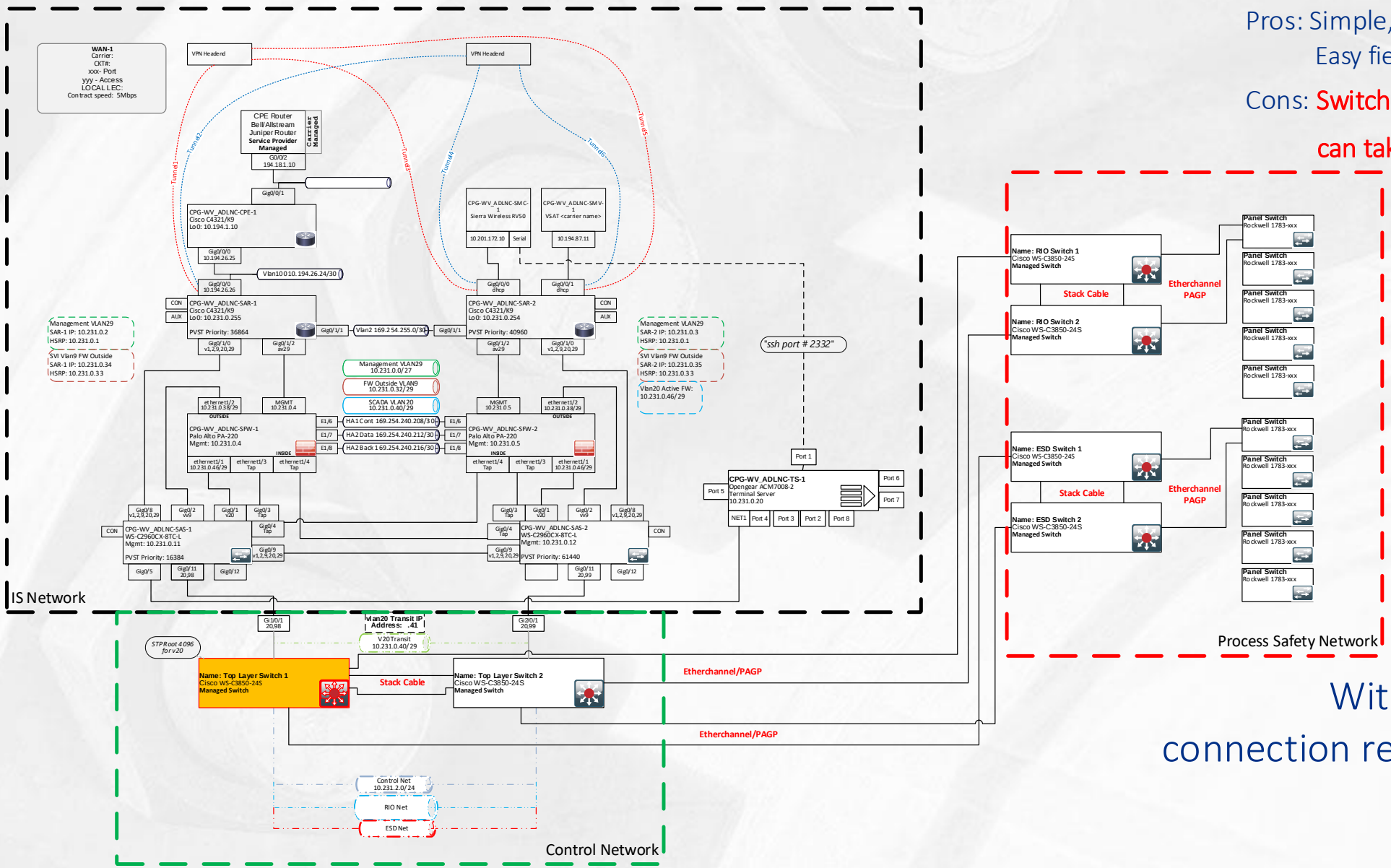
With configuration, connection restored in <1 s ***

Conclusion: Will be considered in the Future

VX-LAN:

Software defined L2 technology

Option: Switch stacking / EtherChannel



Pros: Simple, scalable,
Easy field device configurations

Cons: Switch cluster failure
can take entire site down

With configuration,
connection restored in 50 ms

Final Solution & Conclusions

- Due to simplicity and supportability, the switch stacking with EtherChannel solution was chosen.

Conclusions

- As VxLAN continues to mature, we will analyze when it can operate with the simplicity and stringent reliability required by Critical infrastructure.
- For now, the Stacking/EtherChannel represents the best operational option.