Trisis Malware

Sulaiman Alhasawi

https://www.linkedin.com/in/alhasawi/

Kuwait OWASP Chapter

Real Name ? Does it matter !

- Trisis
- Triton
- Hatman

When ? Where?

- Mid November 2017
- Middle East

Target

- Schneider Electric's Triconex safety instrumented system (SIS) (PLC) (Triconex 3008 processor modules)
- Software and hardware safety standard ((IEC-61508)

Goal

- replace logic (IEC-61131) in SIS controller , target operation safety

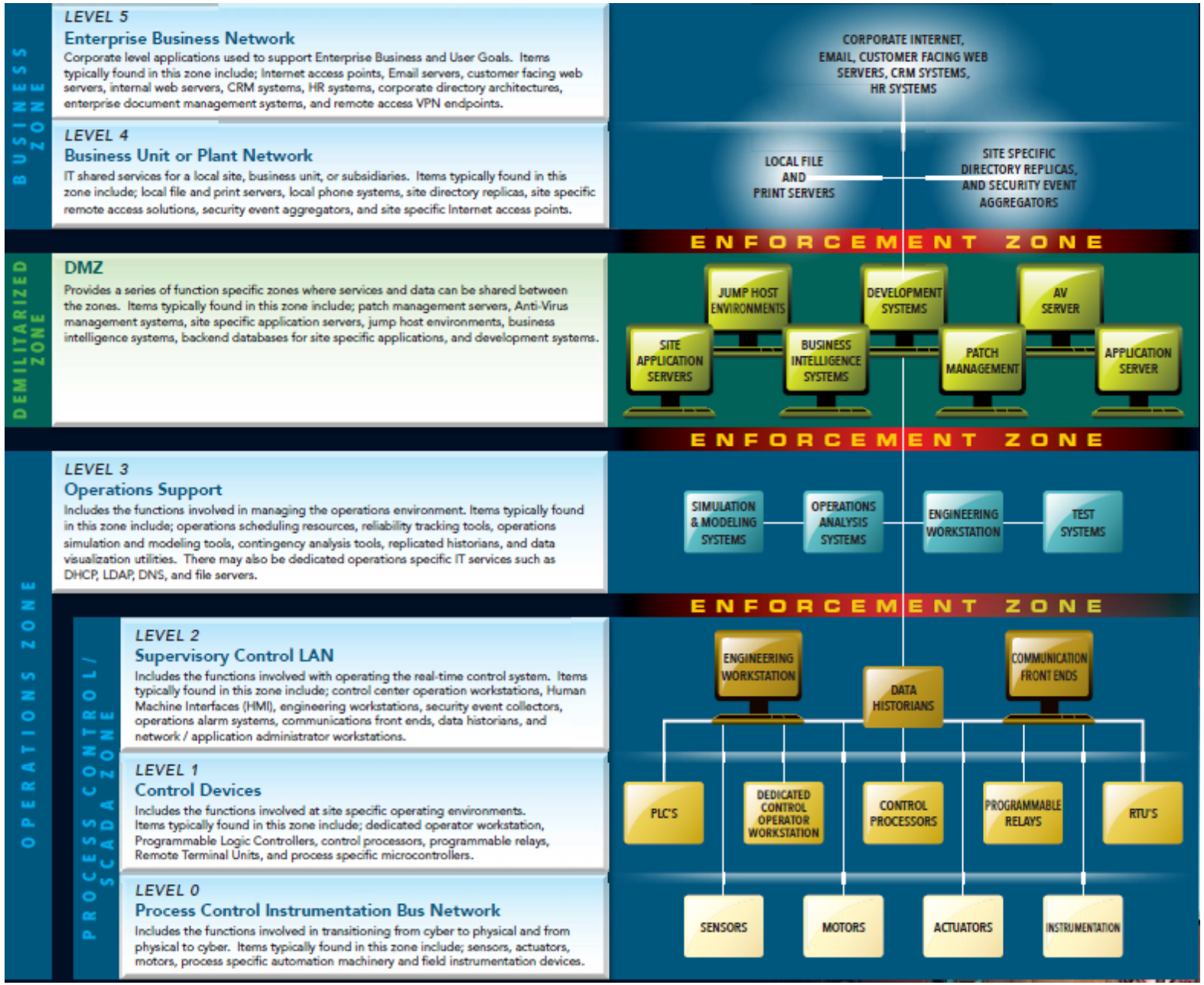

Image Reference (4)

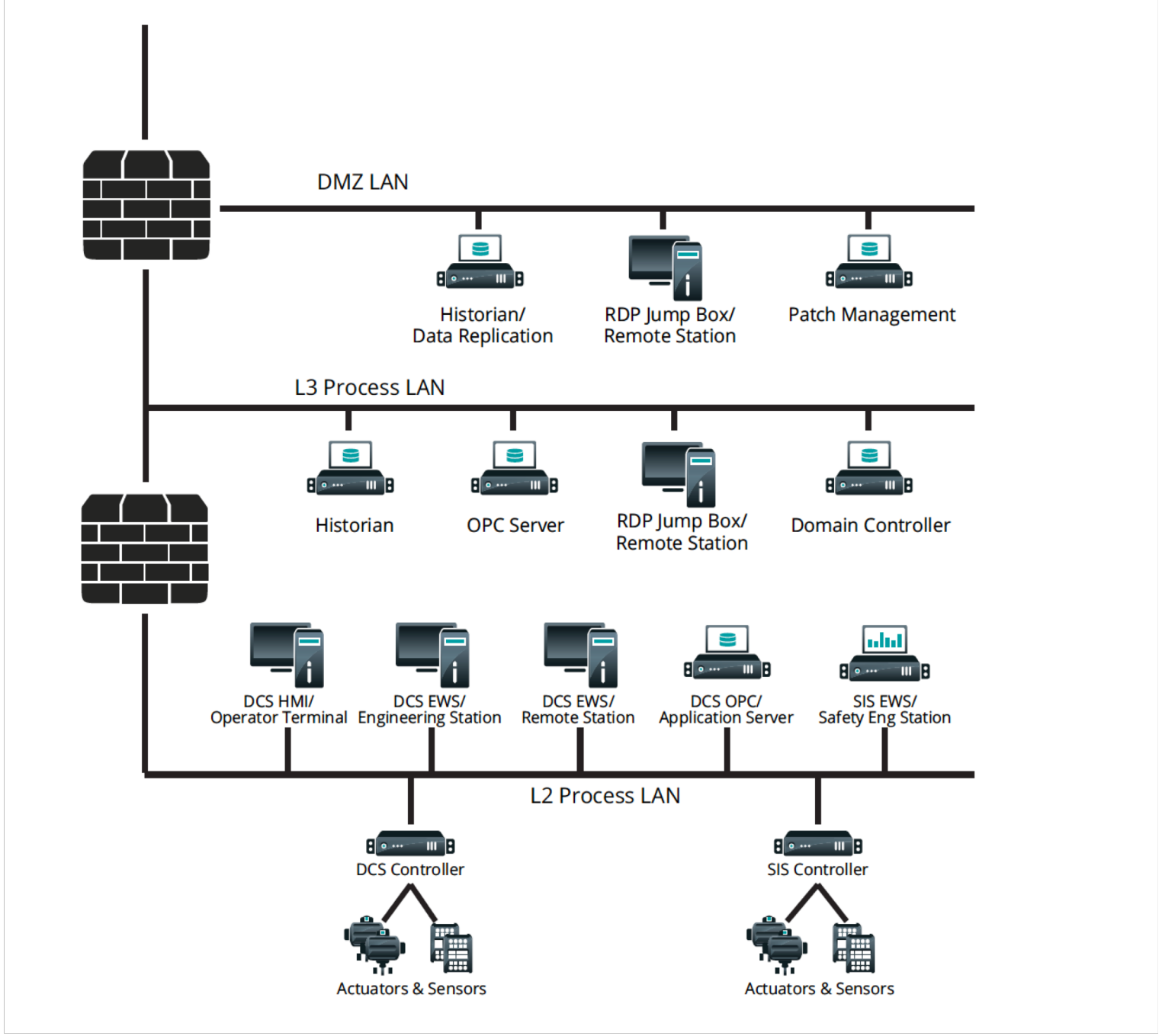

Image Reference (2)

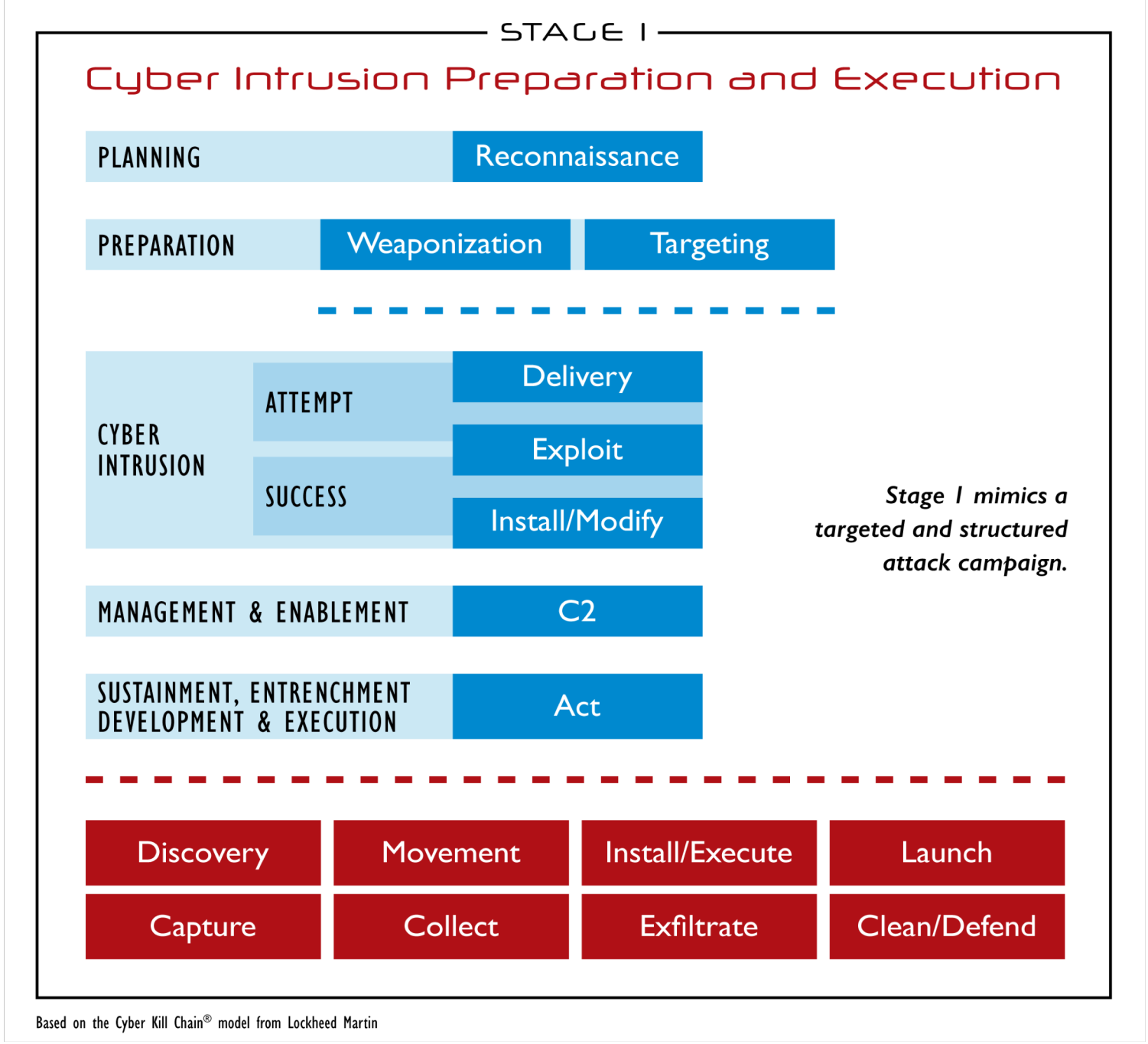

Image Reference (3)

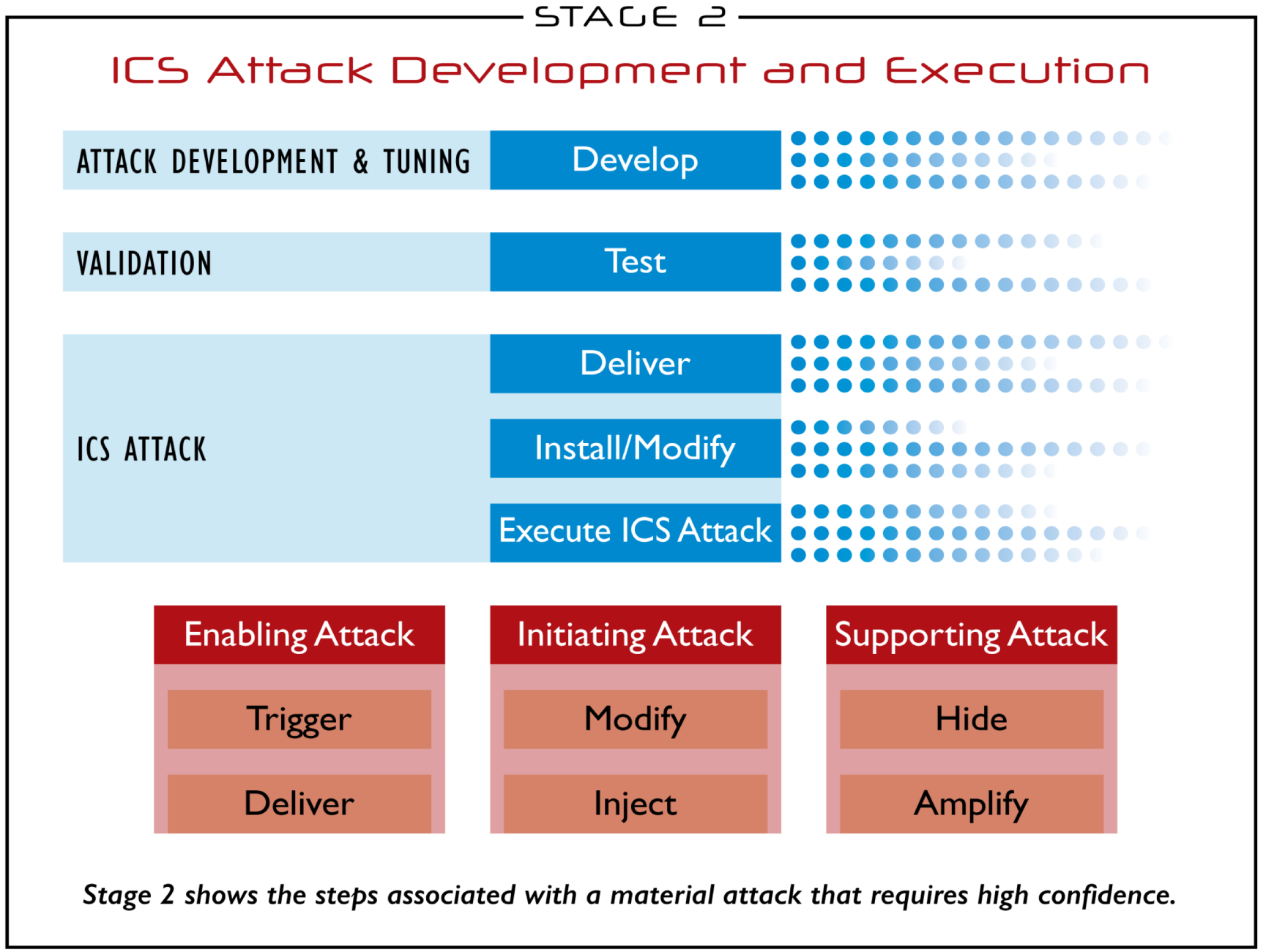

Image Reference (3)

Trisis is a Python Compiled text (py2exe)
Trilog.exe : payload
Inject.bin : Triconex memory – 0-day (backdoor injector)
Imain.bin : RAT code (backdoor code)

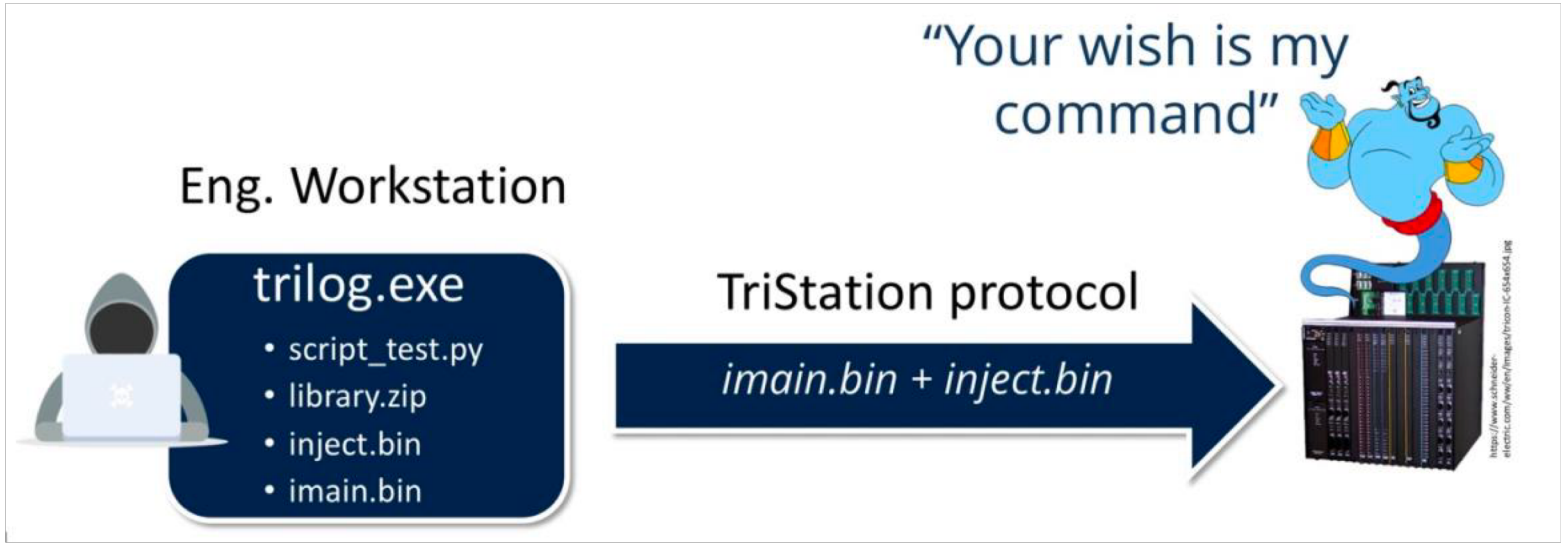

Image Reference (1)

TriStation Protocol
UDP/IP port 1502

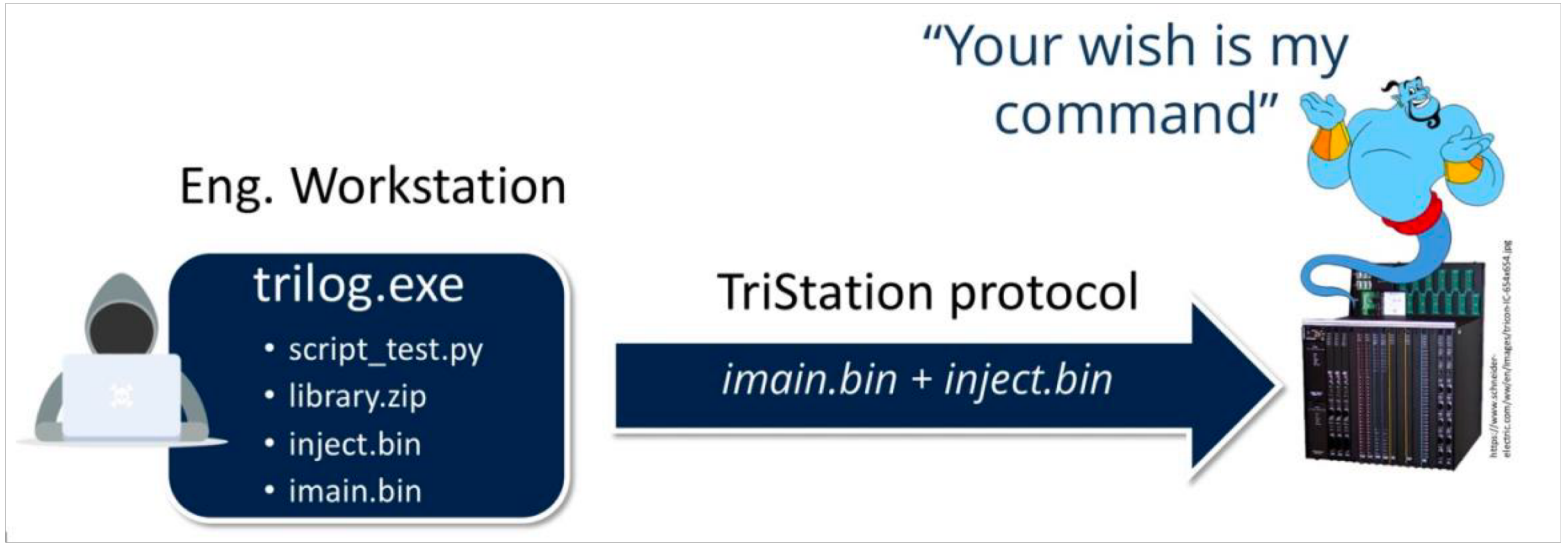

Image Reference (1)

How to build Trition

- Gather intelligence
- Build a shopping list
- Re software
- RE Tristation protocol

Schneider Electric Recommendations

- Safety systems should always be deployed on isolated networks.
- • Physical controls should be in place so that no unauthorized person would have access to the safety controllers, peripheral safety equipment, or the safety network.
- • All controllers should reside in locked cabinets and never be left in the “Program” mode.
- • All Tristation terminals (Triconex programming software) should be kept in locked cabinets and should never be connected to any network other than the safety network.
- • All methods of mobile data exchange with the isolated safety network such as CDs, USB drives, etc. should be scanned before use in the Tristation terminals or any node connected to this network.
- • Laptops that have connected to any other network besides the safety network should never be allowed to connect to the safety network without proper sanitation. Proper sanitation includes checking for changes to the system not simply running anti-virus software against it (in the case of TRISIS no major anti-virus vendor detected it at the time of its use).
- • Operator stations should be configured to display an alarm whenever the Tricon key switch is in the “Program Mode.”

Reflections

- This capability/methodology could target other asset owner (replication) , to other vendors not just that device type.
- learn the craft, don’t focus much on vendor name
- SIS failure ,not necessarily cause a collapse in the whole safety systems, as engineers are likely to have other steps. This type of PLC fails safely (eg in case power failure). Also this type of safety plc offers redundancy feature: All modules run the same logic, so if one

Tools

- **Tricotools** : https://github.com/NozomiNetworks/tricotools.
  (WireShark and honeypot]

Thank you

References

1. **TRITON: How it Disrupted Safety Systems and Changed the Threat Landscape of Industrial Control Systems, Forever. (Nozomi)**
2. TRISIS Malware - Analysis of Safety System Targeted Malware (Dragos)
3. The ICS Cyber Kill Chain: Active Defense Edition - Robert Lee (SANS)
4. https://ics.sans.org/blog/2016/05/08/detecting-the-siemens-s7-worm-and-similar-capabilities/