



## Cybersecurity and Critical infrastructure

*Lawrence Kravets*



Lawrence Kravets

IT Director

---

My story:

- University of Illinois at Chicago, 94
- Certified Information Systems Security Professional (CISSP)
- Global Industrial Cyber Security Professional (GICSP)
  - 25+ years in Information Technology
- 12+ years in IT / OT @ Concentric Integration

# SCADA

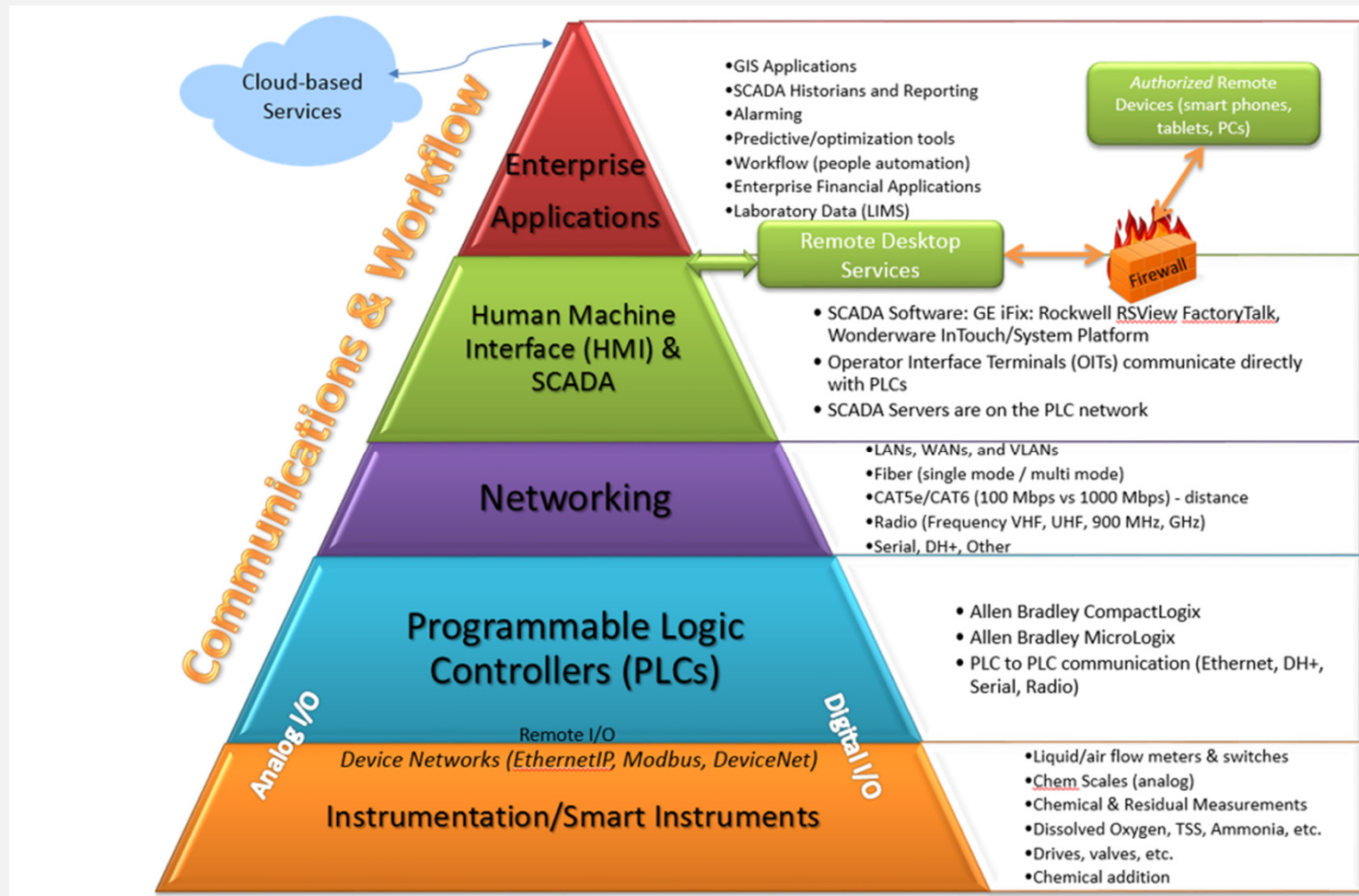
## Supervisory Control and Data Acquisition

- Critical Asset
- Not just a computer or computers
  - PLCs, Servers, Instrumentation
- High value targets



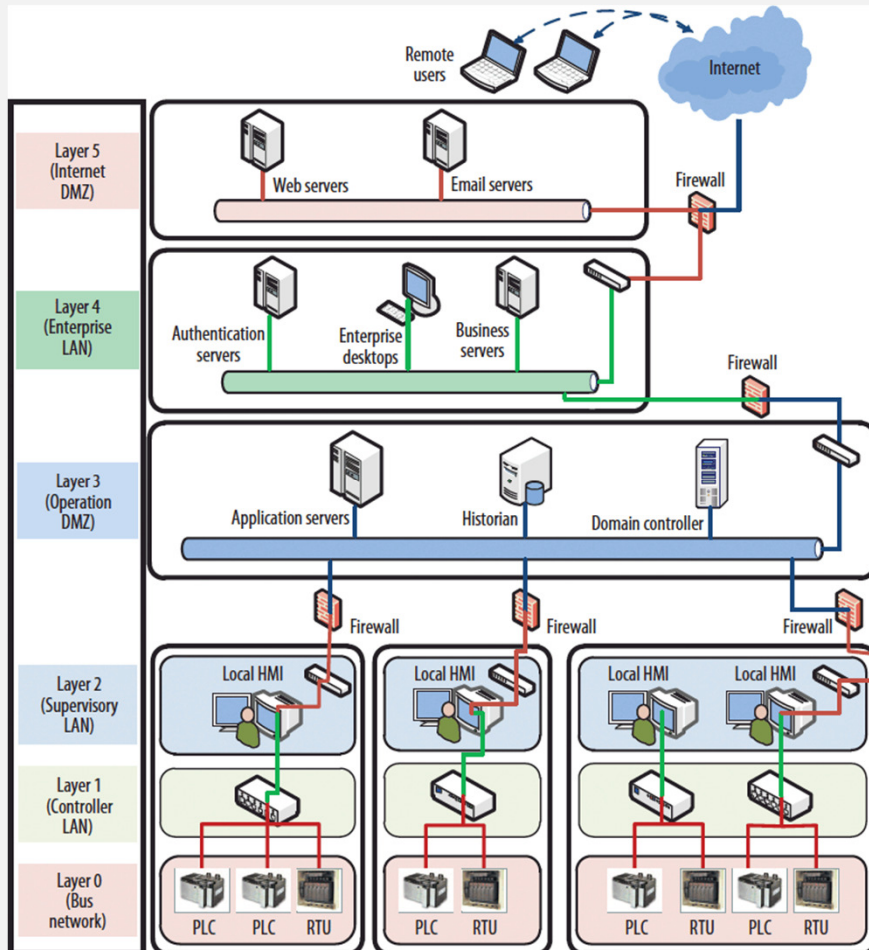
# SCADA

## Lots to protect



## Purdue Model of Securing Industrial Control Systems

- Segment networks using a dedicated SCADA firewall
- Considered the gold standard but not always practical
- Start small and separate where you can
  - Risk vs Reward



# SCADA

## Protection

- Endpoint Security (PCs and PLCs)
  - Antivirus, Endpoint Detection and Response (EDR), Extended Detection and Response (XDR)
  - Read-only mode for PLCs
  - Updates and patching
  - System Hardening and baselines



# SCADA Protection



- Authentication
  - Dedicated usernames and passwords for staff and Multifactor authentication
- Virtualization and replication
  - Virtualization helps create faster restore times
- Replace end of life and unsupported systems and devices
  - Have a plan on how to replace aging equipment
- Supply Chain Management
  - Have a procedure for reviewing software before it comes into the network



# SCADA

## Protection to Recovery

- Backups can save you!
- Think about backups in two ways
  - Restore something that is lost
  - Disaster Recovery or Business Continuity
- Build a backup and a recovery strategy
- Ransomware best practices for protection
  - Offline and/or immutable
    - Immutable can't be changed or modified





# SCADA

## Recovery

- Planning
  - Incorporate into your maintenance management plan
  - Test backups
  - Test recovery
- Tabletop exercises
  - Engage the team and walk-through scenarios



Lawrence Kravets



8678 Ridgefield Rd, Crystal Lake IL 60012



815-788-3600



[www.goconcentric.com](http://www.goconcentric.com)



[lkravets@goconcentric.com](mailto:lkravets@goconcentric.com)