My Personal ICS Cyber security Vulnerabilities Notes.

- The vulnerability lies with the transparency of the OSI model, as opposed to the obscure proprietary ICS frameworks known only to those who had designed them, or to those with specialized training.
- Whether the system can be compromised is dependent on whether the vulnerability is exploitable. In other words, any system can be attacked, but not every attack will be successful.

__DIGITAL ASSETS CAN BE TARGETED BY A CYBER ADVERSARY:__

Networking devices
Programmable logic controllers (PLCs)
Remote terminal units (RTUs)
Human-machine interface (HMI) workstations
Data acquisition servers and historians
Engineering workstations
Remote access devices
Authentication and authorization servers

__COMMON WEAKNESSES CAN RESULT IN POTENTIALLY SIGNIFICANT CYBER RISK.__

POOR CODE QUALITY

-Unauthorised directory traversal allowed
-Services running with unecesary priviledges.

VULNERABLE WEB SERVICES

-Poor authentication
-Directory traversal enabled
-Unauth access to web server
-SQL injection

NETWORK PROTOCOL IMPLEMENTATIONS

-Lack of input validation(Buffer_overflow)
-Weak auth
-Control system protocol using weak integrity checks-
-Poorly implemented encryption

POOR PATCH MANAGEMENT

-Unpatched or old software
-Unpatched OS
-Older OS

WEAK AUTHENTICATION

-Use of standard protocol auth with cleartext auth
-Client-side enforcment of server side security
-Improper security configuration
-No password required
-User names and passds printed in user manuals.

LEAST USER PRIVILEGES VIOLATION

-Unauth directory traversal allowed
-Services runnig unnecessary privileges.

INFORMATION DISCLOSURE

-Unencrypted proprietary/non-proprietary control system comms
-Unencrypted services common in IT systems
-Open network shares on control system
-Weak protection of creds
-Infomation leak through unsecured services.

NETWORK DESIGN

-Firewall bypassed
-Lack of network segmentation.

NETWORK COMPONENT CONFIGURATIONS

-Acccess to speific ports on host not restricted to required IP adressses
-Port security not implemented on network equipment.