Clean Up Your MES:
The Bridge Between IT & OT

Khalid Ansari
MES & Automation Engineer
Qatar Aluminium Ltd

Image credit: @eventyr; reddit.com/r/roads/comments/bokb4d
Aluminum
- Facilitate, Track, and document transformation of raw materials into finished goods

- Real-time order status, equipment status, and inventory visibility

Image credit: wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture
MES talks to IT
- Customer orders from ERP
- Finished goods back to ERP
- Certificate of Analyses

MES talks to OT
- Recipes to production cells
- Monitoring of production steps
- Logging process data for quality assurance
- Finished goods data

... and MES talks to other things

Image credit: https://marvel-battlelines.fandom.com/wiki/Doctor_Octopus
OPC Classic

- Dynamic ports → open firewalls
- Excessively open access rights
- DCOM & RPC vulnerabilities

Image credit: Yours truly
OPC-DA Tunneling

- Single TCP port
- Option to encrypt, authenticate
- Proprietary

Image credits: Automation.com & Cogent Real-Time Systems
- Secure by design.. but..
- Authentication and authorization
- Encryption and PKI

Image credit: opcfoundation.org
OPC-UA

Add Server

Configuration Name:

Discovery

Server Information
Endpoint URL: opc.tcp://
Reverse Connect:

Advanced

Security Settings
Security Policy: Basic128Rsa15
Message Security Mode: Sign & Encrypt

Authentication Settings
- Anonymous
- Username
- Password
- Certificate
- Private Key

Session Settings
Session Name:

Connect Automatically

OK Cancel

Credit: UaExpert; Unified Automation GmbH
Network Segmentation

Level 4 – ERP

Level 3 – MES, LIMS

Level 2 – Supervisory Control

Level 1 – Basic Control
Security Controls
- Segregation of duties
- Application security
- Database security
- Hardening of system components
- Vulnerability scanning
- Logs,... etc.
**DRP & BCP**

- Develop together with Operations & Management
- Manual workarounds
- Printed copies
- Drills

Image credit: dilbert.com (licensed)
Thank you!

شكراً!