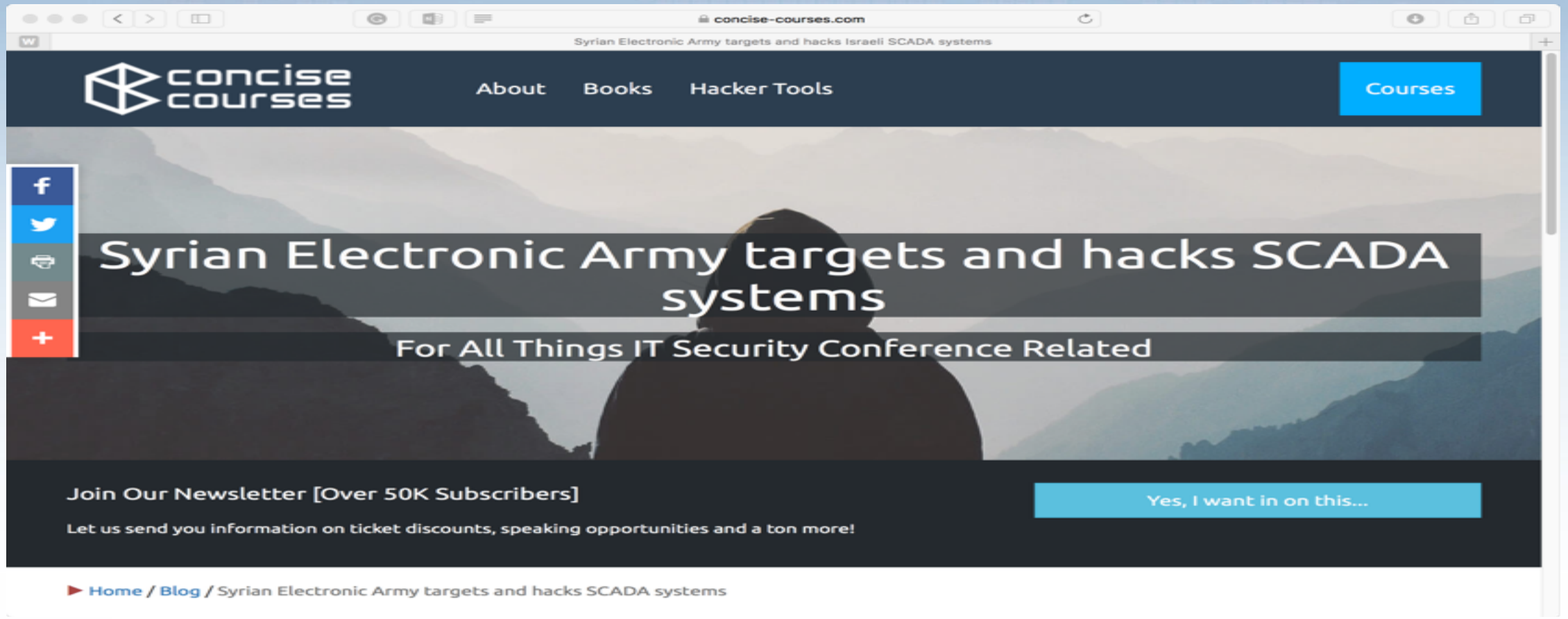
OWASP
Open Web Application Security Project

SCADA and Other Dangerous Things

Professor Andrew Blyth, PhD.
University of South Wales, UK.
E-Mail: andrew.blyth@southwales.ac.uk

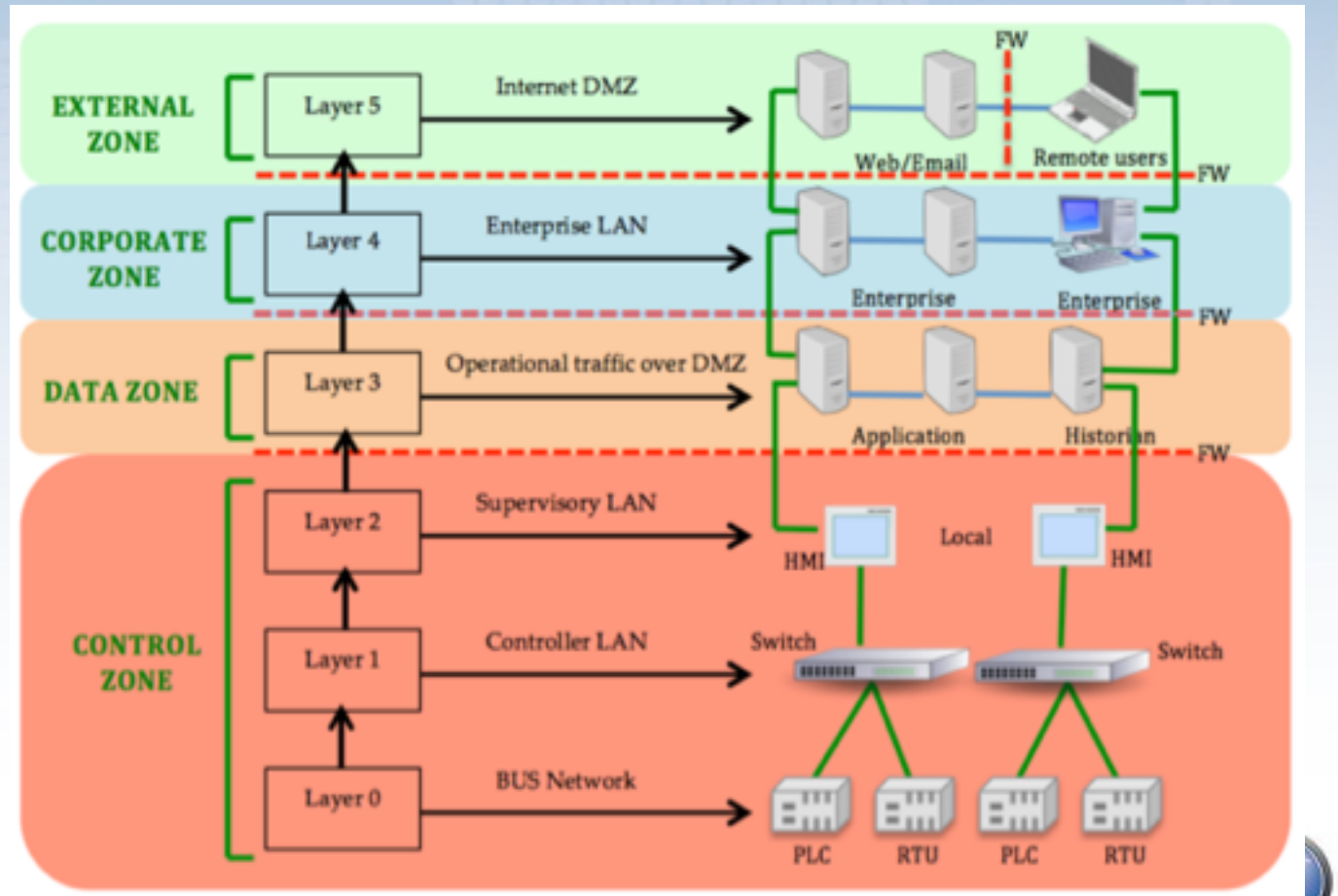
SCADA and Ukraine

SCADA Hacking



OWASP
Open Web Application Security Project

Typical SCADA Critical Infrastructure Architecture



SCADA and IPC Forensic Challenges

- Why do challenges exist?
  - IPC/SCADA systems designed to automate, monitor and control Critical Infrastructure were originally designed for isolated, air gapped networks
  - Now interconnected with many networks and communicating via Internet
  - Span huge geographical areas
  - Include many proprietary and legacy devices and protocols
  - Lack of security mechanisms in SCADA protocols
  - No real guidance or methodologies for data acquisition at the control level

SCADA Forensic Challenges

- **Data Sources**
  - **Variety of data sources, amount of data sources**
- Live Acquisition
- Verification
- Response Time
- Logging and Storage
- Absence of Dedicated Forensic Tools

SCADA Forensic Challenges

- Data Sources
- **Live Acquisition**
  - **Latency, interference and OOV (Order of Volatility)**
- Verification
- Response Time
- Logging and Storage
- Absence of Dedicated Forensic Tools

SCADA Forensic Challenges

- Data Sources
- Live Acquisition
- **Verification**
  - **Calculating hash values**
- Response Time
- Logging and Storage
- Absence of Dedicated Forensic Tools

SCADA Forensic Challenges

- Data Sources
- Live Acquisition
- Verification
- **Response Time**
  - **Span huge geographical areas, many field sites**
- Logging and Storage
- Absence of Dedicated Forensic Tools

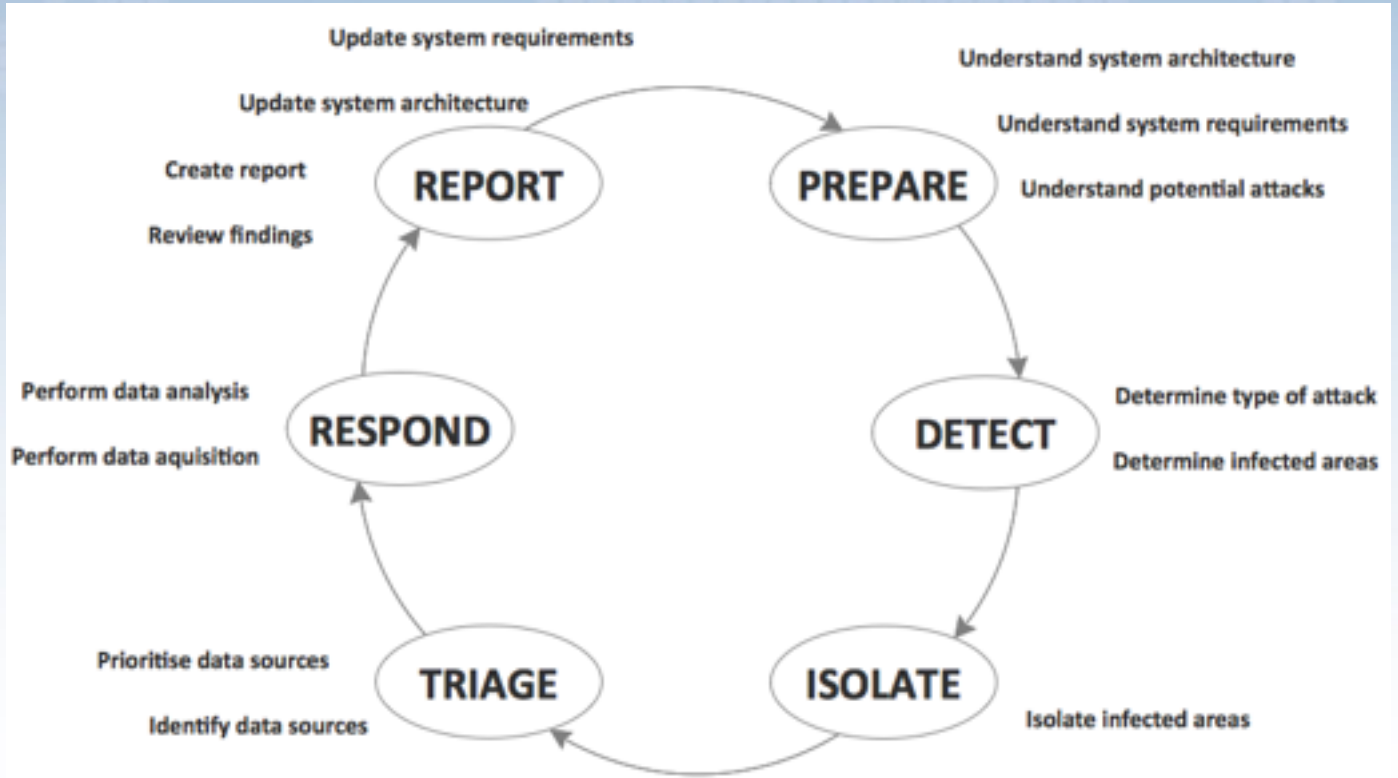
SCADA Forensic Challenges

- Data Sources
- Live Acquisition
- Verification
- Response Time
- **Logging and Storage**
  - **Audit/logging functions disabled, minimal storage**
- Absence of Dedicated Forensic Tools

SCADA Forensic Challenges

- Data Sources
- Live Acquisition
- Verification
- Response Time
- Logging and Storage
- **Absence of Dedicated Forensic Tools**
  - **No real methodologies for data acquisition from PLCs**

IPC/SCADA Forensic Incident Response Model



SCADA Forensic Incident Response Model

- Stage 1: **Prepare**
  - Understand system architecture
  - Understand system requirements
  - Understand potential attacks

SCADA Forensic Incident Response Model

- Stage 2: **Detect**
  - Determine type of attack
  - Determine infected areas
- Stage 3: **Isolation**
  - Containment of infected areas in relation to business operations

SCADA Forensic Incident Response Model

- Stage 4: **Triage**
  - Identify data sources
  - Prioritize data sources
- Stage 5: **Respond**
  - Perform data acquisition
  - Perform data analysis

SCADA Forensic Incident Response Model

- Stage 6: **Report**
  - Review findings
  - Create report
  - Update system architecture
  - Update system requirements

Questions