
# Emerging threats in ICS Systems

Matthew Angle

Laboratory for Electromagnetic and Electronic Systems

Massachusetts Institute of Technology

# Cyber to Physical Risks with Major Consequences

Most Violent Cyber Attack Noted To Date: 2008 Pipeline Explosion Caused By Remote Hacking

Reporting by Jordan Robertson and Michael Riley in Bloomberg is scheduling soon

**German steel mill suffered "massive damage" following a cyber attack**

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

**DHS: Hackers targeted the grid 79 times this year**

By Gavin Bade | November 18, 2014 print

share tweet post email

U.K. Power Grid is Under Attack From Hackers Every Minute, Says Parliament

By Jillian Ward Jan 9, 2015 12:50 PM ET · Comments Email Print

The U.K. government is one step ahead of hackers trying to turn off the country's lights -- for now.

The prospect of cyber-attacks on the nation's power network is a major threat to the country's security, according to James Arbuthnot, a member of parliament who chaired the Defense Select Committee until last year. He plans to visit **National Grid Plc (NG/)** next month to discuss the issue.

"Our National Grid is coming under cyber-attack not just day-by-day but minute-by-minute," Arbuthnot, whose committee

# Unique Aspects of Attack on Cyber-Physical Systems

- **Real, Physical Damage can occur**
- **Not always Possible to Convert to Manual Control**
- **Often the Safety is in Software**
  - Which can be turned off or changed
- **Failures no Longer Independent**
  - If 8 generators, one might fail mechanically …

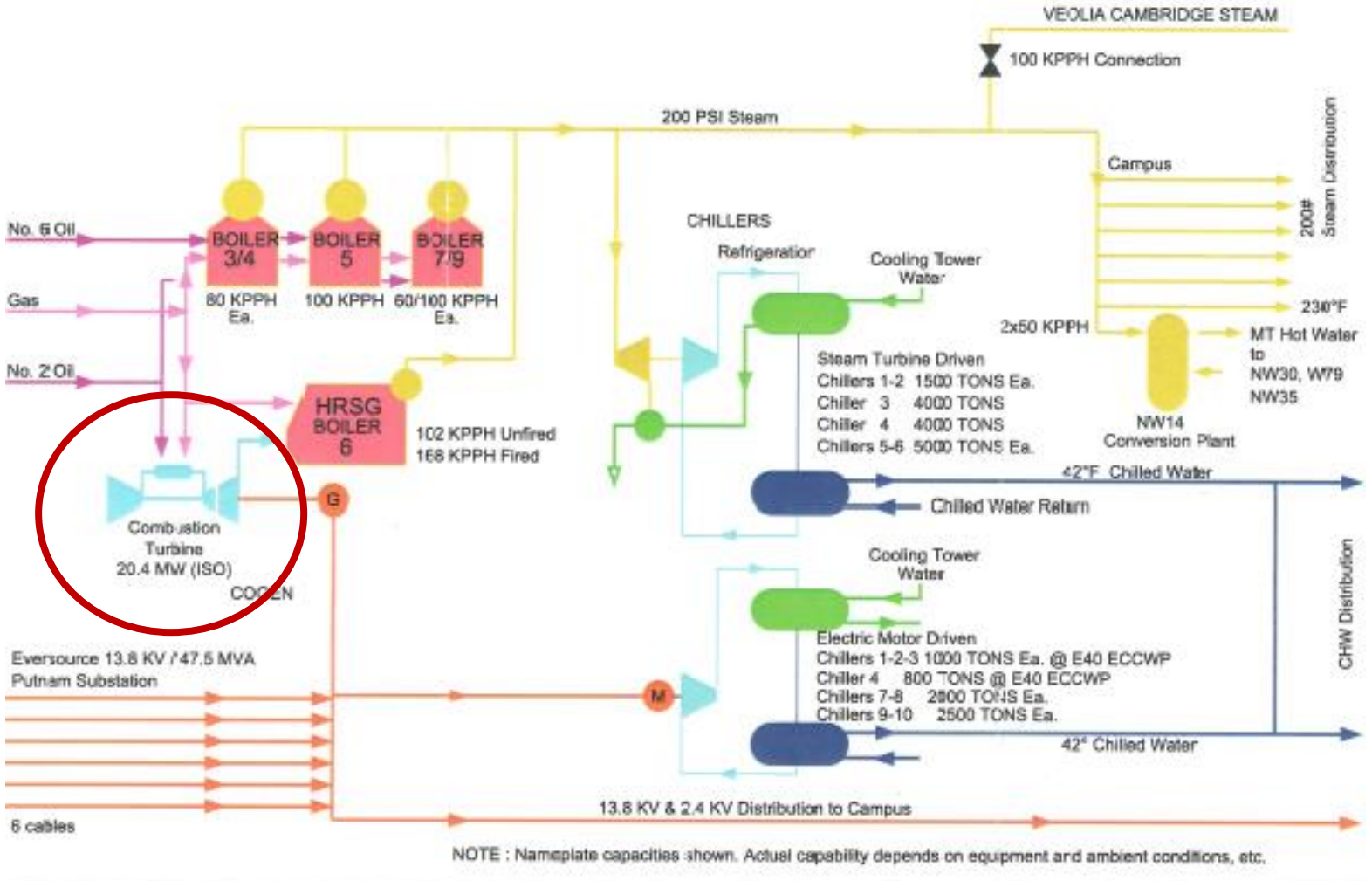
    The other 7 should continue to operated
  - But, a cyber-attack that damages one generated can just as easily damage the other 7 at the same time
- **“Recovery” from physical damage can take long time**

# Example: MIT Cogen Plant

- 21 MW Natural Gas Turbine Generator
- Waste heat used to produce steam that is then used to heat and cool campus

http://web.mit.edu/facilities/about/maint-util/utilities/cup.html

# MIT Cogen Plant



# Example of “Recovery” Time

- **At MIT Co-Gen, one turbine failed …**
  - Not cyber-attack, just a defective nozzle that allowed unpurified water in
- **How long did it take to repair?**
  - 3 months !
- **Why?**

# Cybersafety Analysis

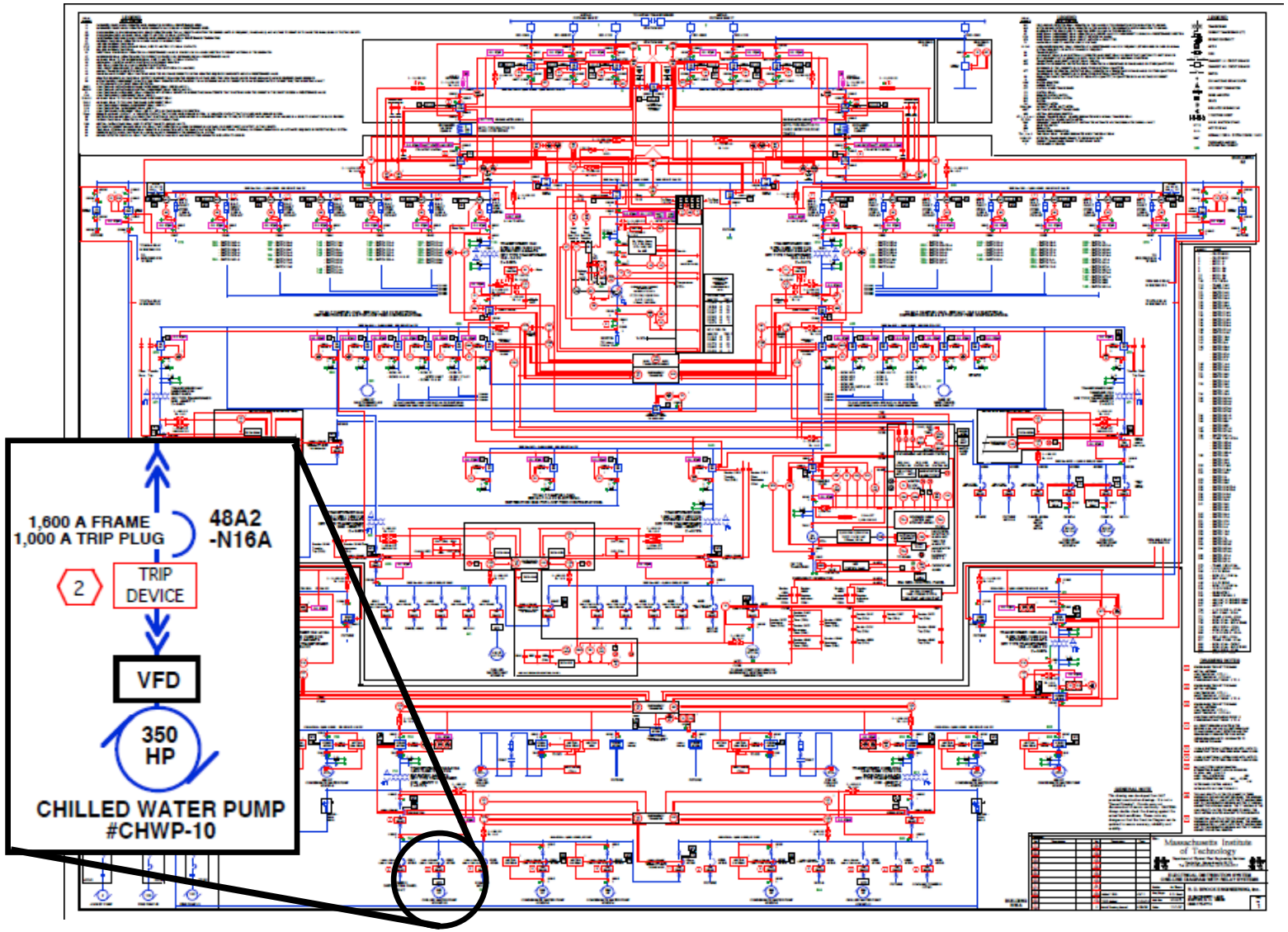
- Start top-down …
- What are you trying to protect / prevent
- Version 1: Make sure that the lights do not go out …
- Version 2: **Make sure that the lights do not go out … for a long time**!
- How can that happen?

# Interesting target: Pumps

- **Used in all kinds of Industrial Control Systems**
  - Gas pipelines
  - Nuclear plants
  - Water treatment

  - ***Others?***

# CoGen Vulnerability – Pumps and VFD

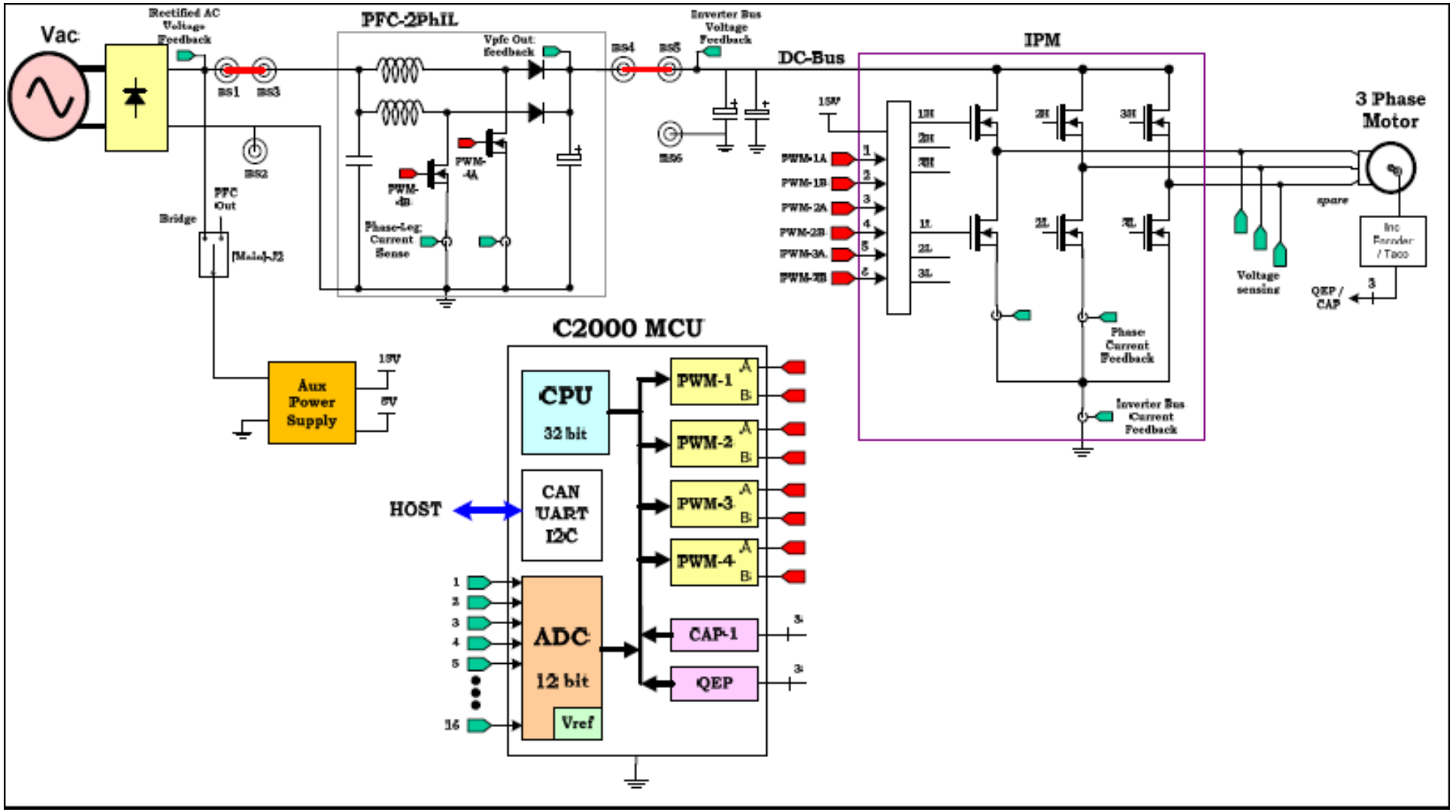


# Variable Frequency Drive

- **Used on most pumps**
  - Allows operation of induction (AC) machines at different speed
- **Component that was attacked by Stuxnet**
- **Usually have programmable limits to protect machinery they drive**
  - Controlled by software
- **Contain capacitors used to store energy on the DC bus**

# Small-Scale Demonstration

# Control Circuity for VFD



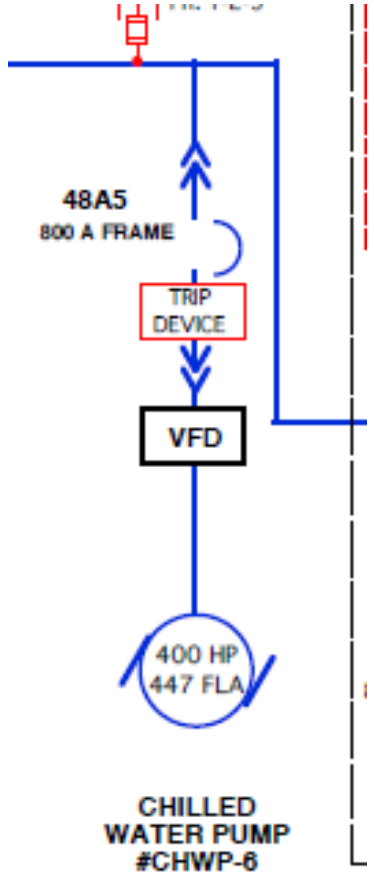
# Code Modification

```
340     /* DPlib initializatio
341     DPL_Init();
342
343 #if (INCR_BUILD == 1)  // (
344     // Module connections
345     // ADC connections
346     ADCDRV_1ch_Rlt4 = &Vbus
347     ADCDRV_1ch_Rlt5 = &Ipfc
348     ADCDRV_1ch_Rlt6 = &VL_f
349     ADCDRV_1ch_Rlt8 = &VN_f
350
351     // Math_avg block connections - Instance 2
352     MATH_EMAVG_In2 = &Vbus;
353     MATH_EMAVG_Out2 = &VbusAvg;
354     MATH_EMAVG_Multiplier2 = _IQ30(0.00025);
355
356     // Connect the PWM Driver duty to an input variable, Open Loop System
357     PWMDRV_2ch_UpDwnCnt_Duty4 = &DutyA;
358
359     // Variable initialized for open loop test
360     DutyA = _IQ24(0.5);
361 #endif // (INCR_BUILD == 1)
```

```
1021     }
1022 #endif
1023
1024     // Check for PFC over voltage
1025 #if(INCR_BUILD == 1)
1026     if(Vbus > VBUS_OVP_THRSHLD)
1027 #else
1028     if(VbusAvg > VBUS_OVP_THRSHLD)
1029 #endif
1030     {
1031         //OV_flag = 1;
1032         //EALLOW;
1033         //EPwm4Regs.TZFRC.bit.OST = 1;  // Software forced PWM trip
1034         //EDIS;
1035
1036         //VbusTargetSlewed = 0;
1037     }
1038
1039     // Calculate RMS input voltage frequency
1040     sine_mainsV.Vin = Vrect >> 9;           // IQ15 format
1041     SineAnalyzer_MACRO(sine_mainsV);
1042     VrectRMS = (sine_mainsV.Vrms) << 9;     // Convert from Q15 to Q24 and save as VrectRMS
```

# Industrial-Scale VFD


- Chilled Water Pump VFD
- 400 HP motor
- Energy storage scales roughly with rated power and inversely with switch frequency



# CoGen Vulnerability

- Switches on campus controlled from control room (like Ukraine attack)
- Turbine synchronization controlled from control room (Aurora demonstration)
- Turbine monitored remotely by Siemens
- Steam, chilled water valves controlled from control room
- Pump VFDs adjustable from control room (speed only)

# CoGen Vulnerabilities – Potential Ways In

- **Icetech connection**
  - Data from control room
  - Connection unknown
- **Siemens Turbine control hardware**
  - Remote diagnostic
  - System capable of remote engineering – mechanism for turning this off?
- **Combination of Trane and York chillers**
  - Modern chiller control systems, with network connectivity
- **Contractor maintains and updates systems**
- **Unhappy insider ?**

# CoGen Vulnerabilities

- **Turbine**
  - Must be kept spinning while it cools
  - Lead-acid battery bank provides power to motor that turns rotor
  - Natural gas pressure regulators step down from 300 PSI line to 25 PSI feed, pneumatic actuation
- **Lead-acid battery bank used to start backup diesels**
- **Icetech watches electricity and gas prices**
  - Makes recommendations on turbine throttling
  - Determines how much of campus power comes from grid vs. turbine
  - Changes turbine throttle up to 3 times per day


# Emerging threats in ICS Systems

Matthew Angle

Laboratory for Electromagnetic and Electronic Systems

Massachusetts Institute of Technology