



### **High Availability and Reliability**

- Triple Redundancy of PCs in DMZ
- Assigned PCs for Operations and Traders
- Additional T3000 Licences
- Monitoring of user login limits
- Limited Access to key users
- Network Redundancy

Together we can  
make a difference.™

origin

Security  
measures  
considered &  
implemented



## Security measures considered and implemented

Together we can  
make a difference.™



### **Security measures considered:**

- Network security
- Operational security
- Physical Security

## Network security

Together we can  
make a difference.™



- OEM Advice: Siemens White paper - T3000 Security
- IT Vulnerability Assessment
  - Application security
  - Intrusion detection
  - Regulation of physical access to the SCADA network
- I&C Guideline - Remote operation of peaking power station



### Asset Management Guideline

### Remote Operation and Monitoring setup for Peaking Power Stations

Released on June 22<sup>nd</sup> 2009

Revision: 1.0

GEN-AMS-GDL-104

## Network security - Contd.

Together we can  
make a difference.™



### Password Authentication Model:

- **Authentication** is the software process of identifying a user who is authorized to access the SCADA system.
- **Authorisation** is the process of defining access permissions on the SCADA system and allowing users with permissions to access respective areas of the system

### Password Compliancy:

- User name specific instead of common practice of Generic usernames.
- Passwords changes periodically.
- Logins disabled immediately for anyone leaves company or moves from within functional area.

### Network Topology:

- Simple networks are at less risk than more complex, interconnected networks. Keep the network simple and, more importantly, well documented from the beginning.
- A key factor in ensuring a secure network is the number of contact points. These should be limited as far as possible.

## Network security - Contd.

Together we can  
make a difference.™



- Standard Architecture with Network security Zones

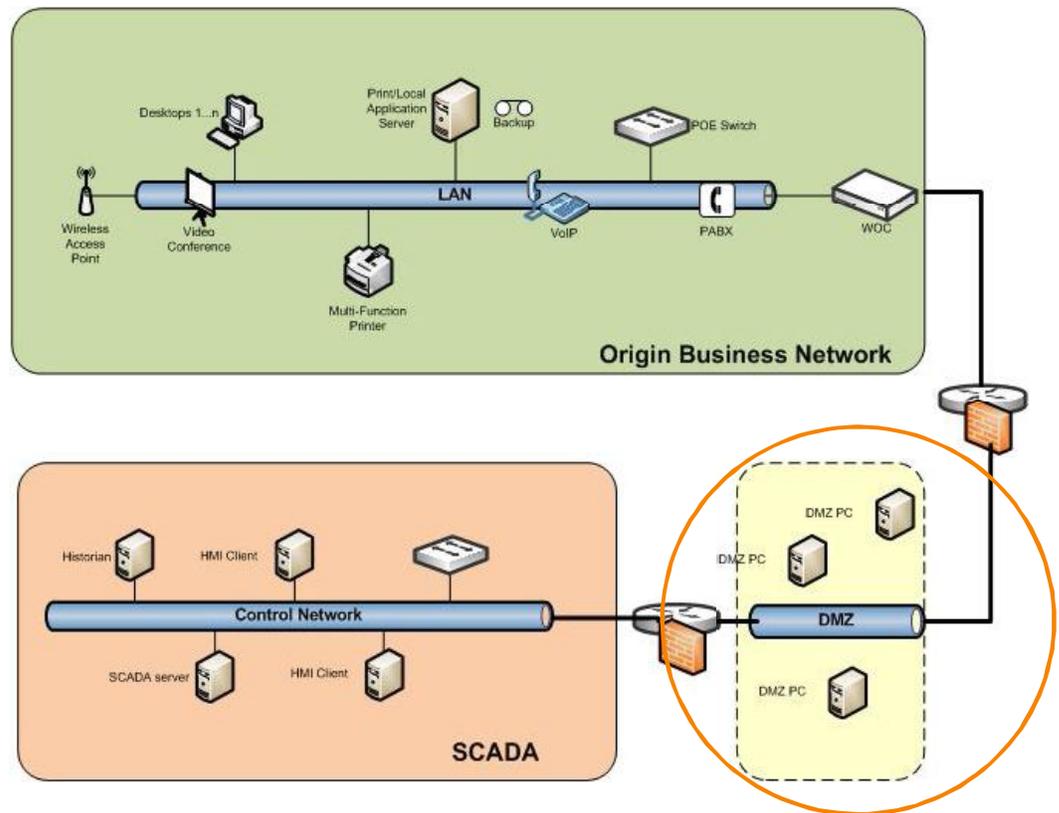
- This network is considered a "Restricted" zone in accordance with Origin Enterprise Security Architecture - Logical Network Zone Model.
- The security of the SCADA DMZ Network shall include a network firewall device that is compliant with Origin architecture
- Restrict access to the SCADA DMZ Network and Applications to only authenticated users and specified network communication protocols required for the applications running on the host computers
- SCADA DMZ Network communication shall be given priority over general Origin Business Network communications
- The SCADA DMZ consists of 2 network security zones; the SCADA DMZ being restricted and the Control System being secured

# Network security - Contd. Standard Architecture

Together we can  
make a difference.™

origin

- Firewalls
- RDP access to DMZ PCs.





### Operational Security measures considered:

- Enable and Disable remote operation of Gas Turbine to avoid inadvertent operation of GT
- Provide Emergency GT Trip

# Operational Security - Contd.

- Below are examples of different operational access rights.
- Remote Operations may be blocked by the Uranquinty Duty Operator.

Together we can make a difference.™

origin

The screenshot displays the SPPA-T3000 Workbench interface for remote operation. It features four turbine control panels (GT 11, GT 12, GT 13, and GT 14). Each panel includes a 'START/STOP CONTROL' section with 'SQC GAS TURBINE' and 'GT START/STOP' buttons, a 'TURB CTRL INDICATIONS' section with various status lights, and 'ACTIVE POWER SETPOINT' and 'REACTIVE POWER SETPOINT' sections with numerical displays and control buttons. A legend at the bottom indicates that red indicates 'OK, ON, Run, Open, Active' and green indicates 'Not Available, OFF, Closed'. A legend at the bottom right shows 'REMOTE OPERATION' (grey), 'REMOTE TRIP' (black), and 'STATION SERVICES' (red, yellow, blue).

RED = OK, ON, Run, Open, Active.

Green = Not Available, OFF, Closed.

# Operational Security - Contd.

## EMERGENCY TRIP

Together we can  
make a difference.™

origin

The Emergency Trip system is not to be used unless advised to do so by the Duty Operator.

Only under extreme circumstances will the Duty Trader need to use this page.

This page should not be opened or used except for it's intended purpose.

Double click on SLC as previously shown to open faceplate

By activating this function will shutoff gas to the unit and the unit will trip.

Alternatively if the whole station is to be tripped off the main Gas ESD will need to be shutdown via here.



### Power Stations and Control Rooms

- Physical Lockout and Swipe Card Access
- Operator Alarm

Together we can  
make a difference.™

origin

Centralised  
Remote  
Operations -  
Tangible  
Benefits and  
security threats



## Tangible Benefits of remote operations setup

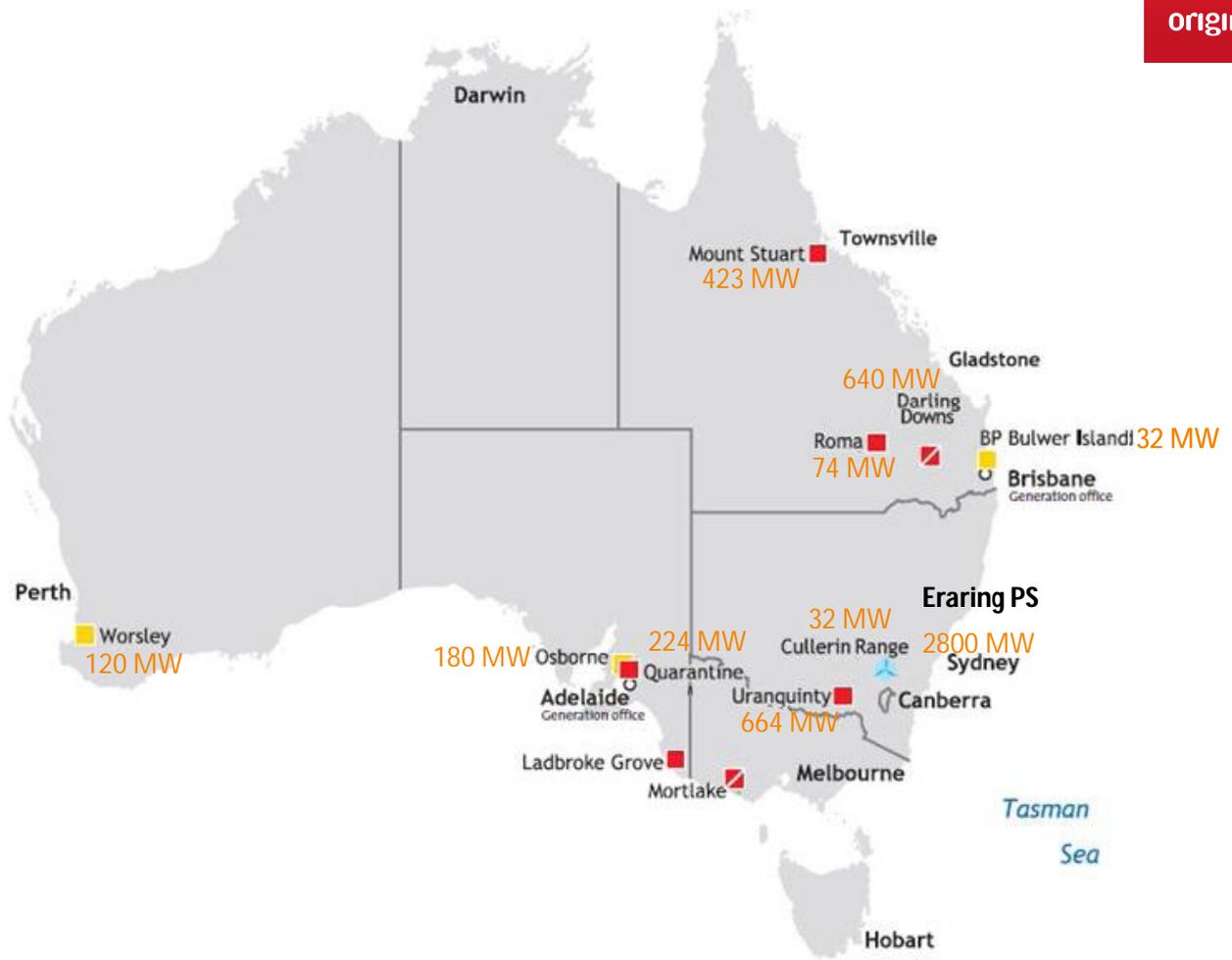
Together we can  
make a difference.™



- Significant Cost Saving
- In-house skill uplift
- Scalability
- Competitive Advantage
- Monitoring and Support Centre Project Evolution

# Centralised Remote Operations and Monitoring

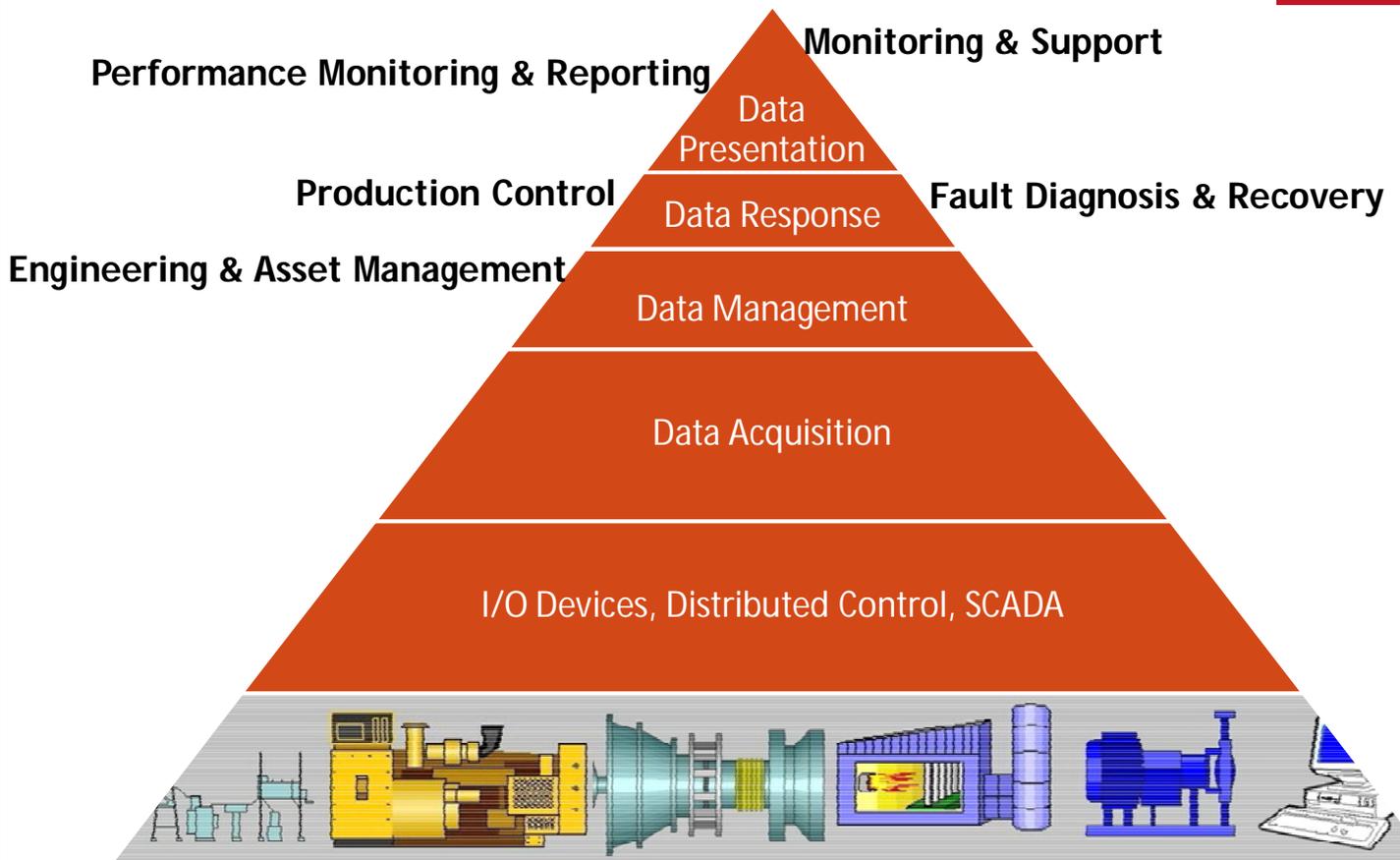
origin



# Benefits of Centralised Operations

Together we can  
make a difference.™

origin



## Security Threats of Centralised Remote Operations and Monitoring

Together we can  
make a difference.™

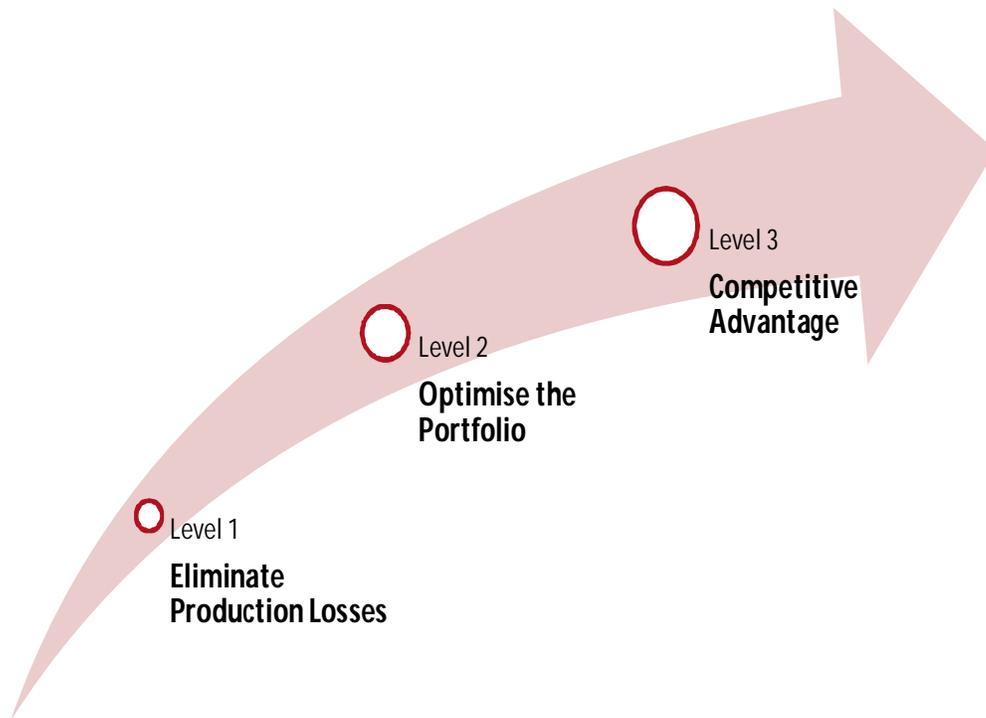


- Data Warehouse at Centralised location
- Vulnerable to cyber attack – prime energy sector
- More transparency across business to multitude of stakeholders  
- possible misuse of info
- Physical security threat
- More prone to human errors due to similarity of displays across different sites
- Linkage between IT and Control network
- Potential of exposing information to external world
- Easy propagation within integrated modules with SSO (Single Sign On) model

# Monitoring and Support Centre (MSC) Project Milestones

Together we can  
make a difference.™

origin



## SCADA/DCS installed at Origin Generation sites

Together we can  
make a difference.™

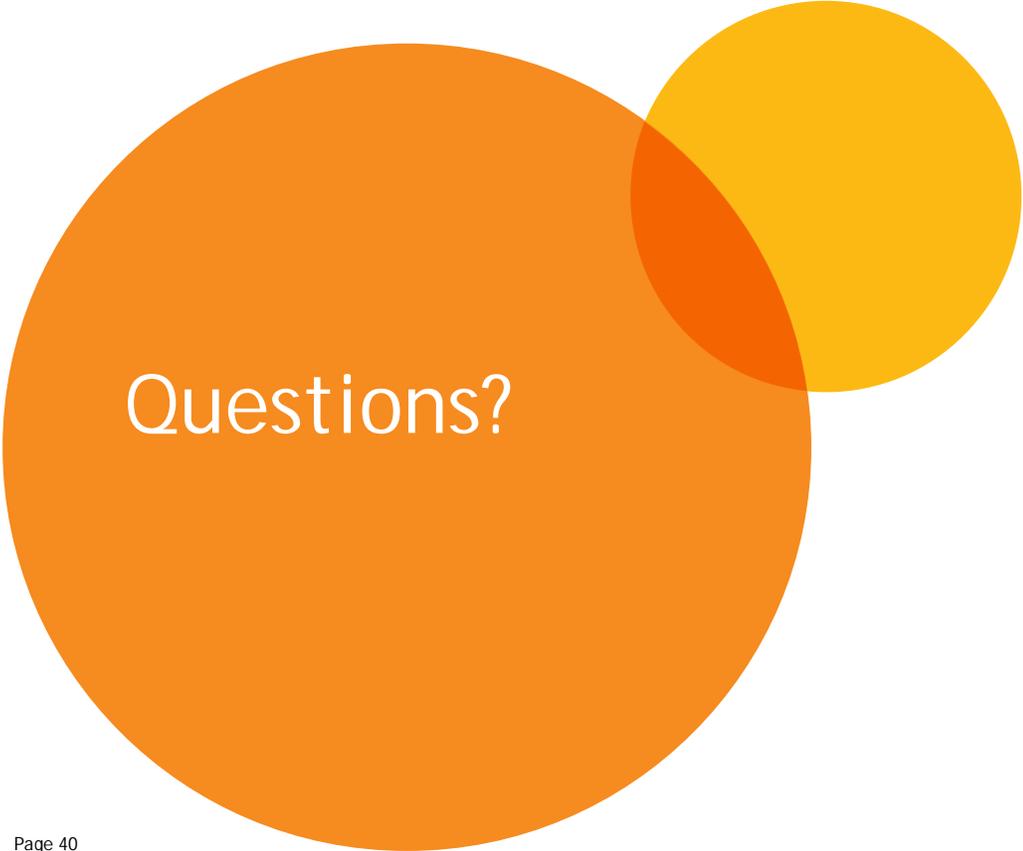
origin

Generation Site	
Mt Stuart Power Station	Mitsubishi Netmation & GE Mark Vles
Roma Power Station	Citect/Triconex
Darling Downs Power Station	GE Mark Vles
Uranquinty Power Station	Siemens T3000
Mortlake Power Station	Siemens T3000
Ladbroke Grove Power Station	Citect/Woodwards
Quarantine Power Station 1-4	ABB Advant
Quarantine Power Station 5	GE Mark Vles
Cullerin Range Wind Farm	Citect/Foxboro

origin



Together we can  
make a difference.™



Questions?



## Case Study - Remote Operations and Monitoring of Power Station and Managing security with remote access.

origin



Presentation: ISA POWAT  
2012

Location: The Grand, New  
Delhi

Date : 13-14<sup>th</sup> Jan. 2012

Together we can  
make a difference.™

# Overview

Together we can  
make a difference.™



Origin – Generation portfolio

Remote operational capability at Origin Power Stations

Establish remote operation for Peaking Power Station

Security measures considered and implemented

Centralised Remote Operations – Tangible Benefits and security threats.

Together we can  
make a difference.™

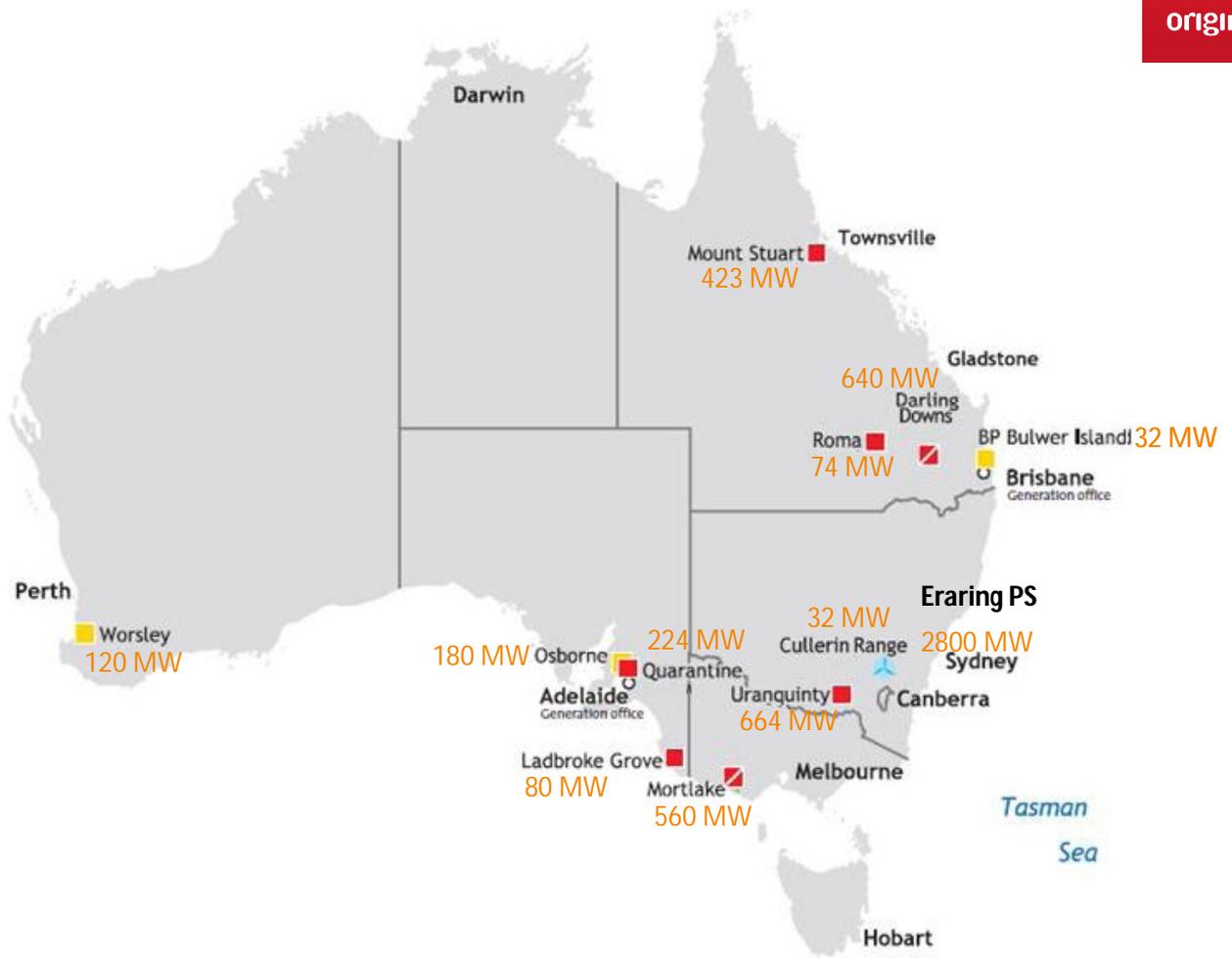
origin

# Origin – Generation Portfolio



# Generation Portfolio

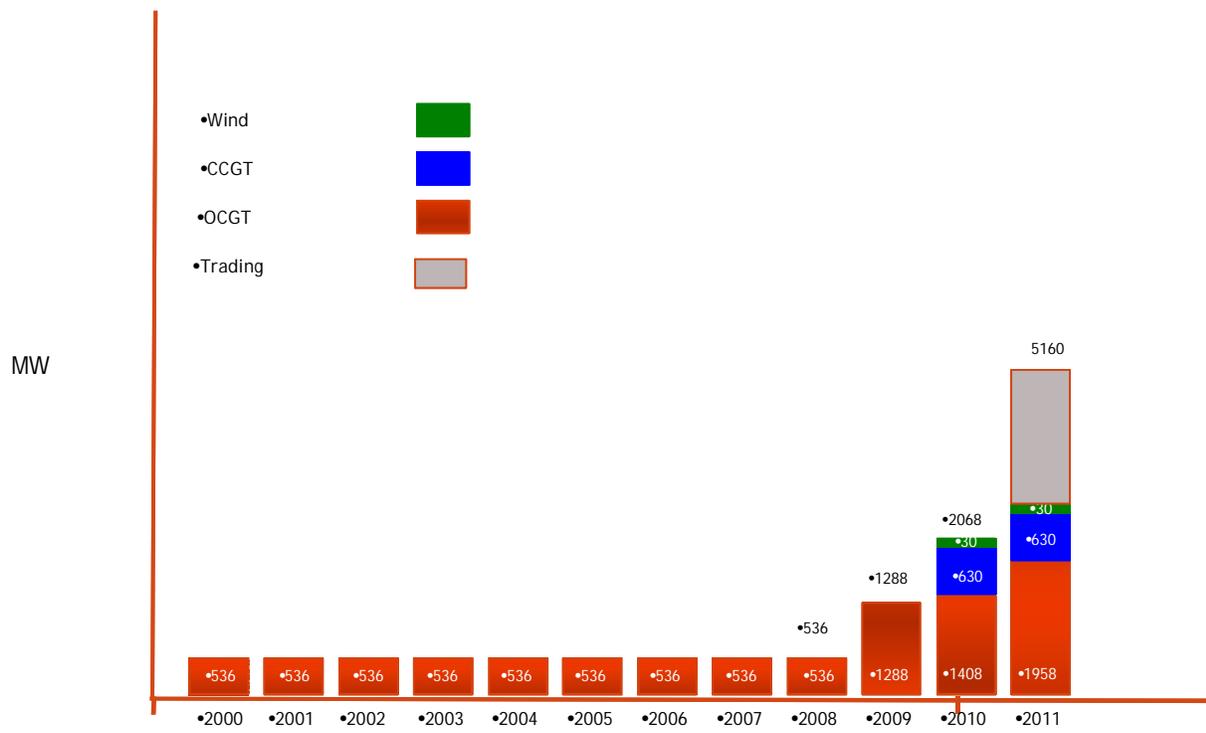
origin



# Generation portfolio

Together we can  
make a difference.™

origin



Together we can  
make a difference.™

origin

Remote  
operational  
capability  
at power  
stations



## Remote Operational Capability

Together we can  
make a difference.™



- Operated by NSPs like Powerlink and Electra-net
  - Roma Power Station
  - Ladbroke Grove Power Station
  - Quarantine Power Station
- Operated by Origin Generation
  - Mt Stuart Power Station (*Local operation*)
  - Darling Downs Power Station (*Local operation*)
  - Uranquinty Power Station (*operated by Traders - interim measure*)
  - Mortlake Power Station (*will be commissioned in early 2011*)

## Remote Operation of peaking power station

Together we can  
make a difference.™

origin

- Uranqui
- Siemens
- Control



## Remote operational Requirements

Together we can  
make a difference.™



- Minimise reaction time to have units available and run up to full load.
- Maximise opportunity to trade electricity in volatile market.
- Optimise site resources.
- Increase availability and start reliability.
- Reduced risk of human intervention and error which has potential to cause delays.
- Buildup in house capability.
- Pilot trial project to support large scale growth in future.

Together we can  
make a difference.™

origin

Establish  
remote  
operation  
for peaking  
power  
station



# Establish Remote Operation for Peaking Power Station

Together we can  
make a difference.™



- Challenges to establish remote operation for peaking power Station.
- Overview of control system

## Challenges to establish remote operation for peaking power Station.

Together we can  
make a difference.™



- Train Commercial traders to operate power plant:  
Plant Operational Competency Model which includes:
  - Plant Operational Training package
  - Customised trader HMI only for trader control.
  - Customized HMI for Traders
  - Customised and Limited DCS hands on operational training.
  - Theory and practical test.
  - Final signoff to allow unit operation from customised HMI.

# Challenges to establish remote operation for peaking power Station - Contd.

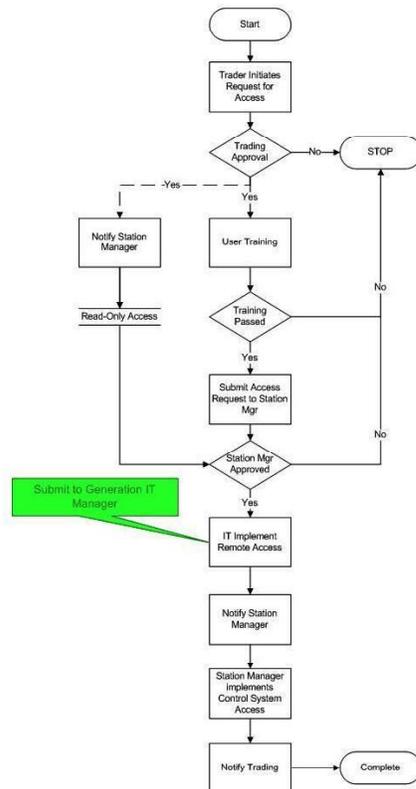
Together we can make a difference.™



- User Access Control
- Operational Procedures
- Customised logic design Strategy
- Documentation
- Alarm Escalation
- Emergency Trip situation
- Alarm Standardisation

## User Access to Control System Application

Wednesday, January 27, 2010

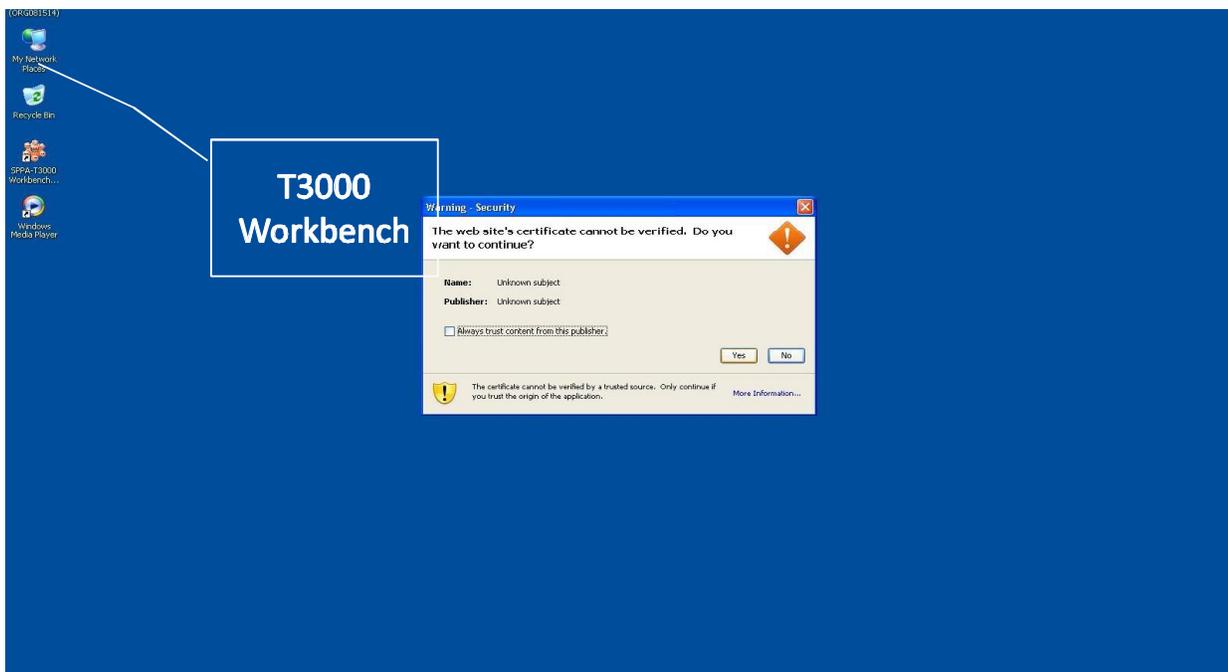


# Connecting to Plant Control System (SPPA T3000) - Overview

Together we can  
make a difference.™

origin

- Remote desktop into Client PC meant for dedicated T3000 workbench application.
- Open SPPA T3000 workbench application
- Only Authorised users can login.

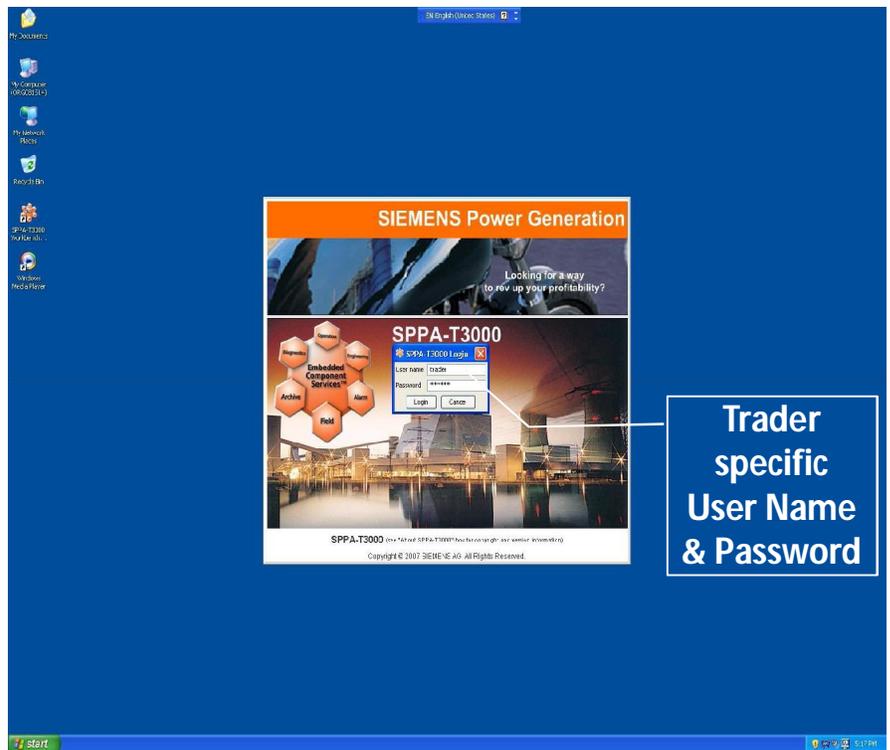


# Uranquinty Control System Access

Together we can  
make a difference.™

origin

- A login will be created for all authorized members of the trading team. Type in user specific Username and Password.
- User name: Specific to each individual trader
- Password: Specific to each individual trader



# Customised HMI for Traders

- REMOTE OPERATION Screen with all GT's at a glance for Operations and Monitoring

Together we can make a difference.™

origin

The screenshot displays a software interface for remote operation of four gas turbines (GT 11, 12, 13, 14). Each turbine's control panel is organized as follows:

- GT START/STOP CONTROL:** Includes 'SGC GAS TURBINE' status (63), 'RDY FOR START', 'BOP PERMISSIVE', and 'REM OPS ENABLE' indicators. A large green 'G' indicates the turbine is running. Below this, frequency (1.68 Hz) and power (0 MW, -0 Mvar) are shown.
- TURB CTRL INDICATIONS:** A list of status indicators for 'RUN UP FUNCTION ACTIVE', 'SPEED CTRL ACTIVE', 'LOAD CTRL ACTIVE', 'OTC CTRL ACTIVE', and 'LOAD LMT CTRL ACTIVE'.
- EVAP COOLER:** Shows 'ON/OFF' status, 'HUMIDITY' (44%), 'AMB AIR' (24.5 °C), and 'COMPR INLET' (34.7 °C).
- PAG WATER:** Shows 'ON/OFF' status, 'EON' (2302 h), and 'STARTS' (136).
- ACTIVE POWER SETPOINT:** Features a 'SETPOINT FROM AGC' slider (80 MW) and a 'RAMP RATE FAST' indicator.
- REACTIVE POWER SETPOINT:** Features a 'TO GT CTRL' slider (-0.5 Mvar) and a 'TRANSFORMER TAP POSITION' (11).
- CURRENT CONDITIONS:** Shows 'MAX LOAD' (141 MW).

At the bottom, a legend indicates: **RED = OK, ON, Run, Open, Active.** **Green = Not Available, OFF, Closed.** The interface also includes a status bar with 'Current user: trader', 'Operation Mode', and a date/time stamp 'January 27, 2010 06:23:39'.

**RED = OK, ON, Run, Open, Active.**

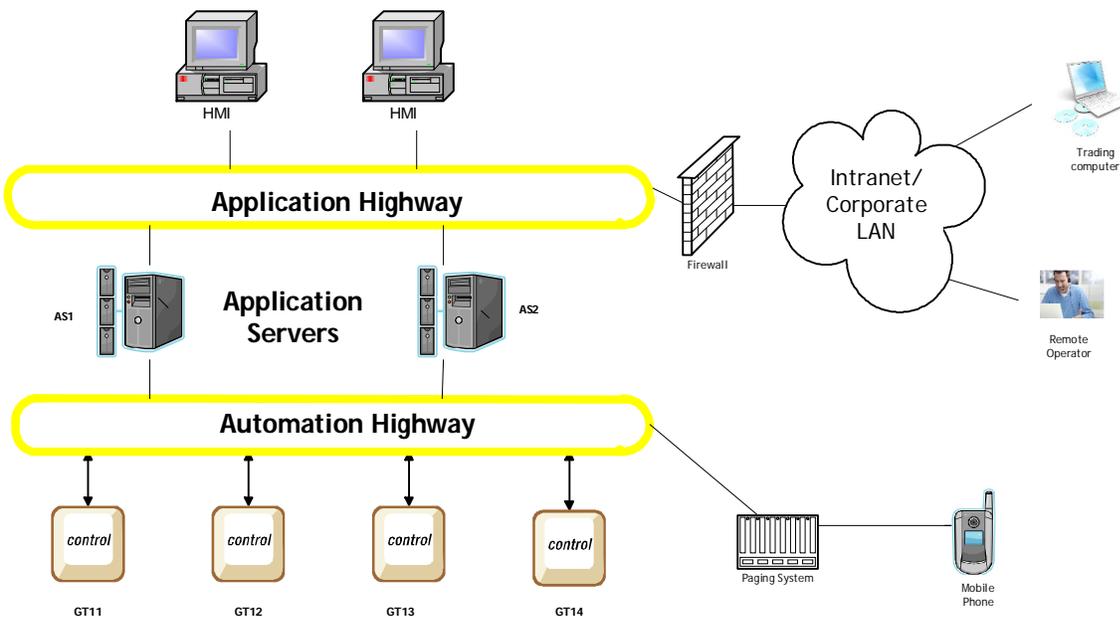
**Green = Not Available, OFF, Closed.**

# DCS Network Architecture

Together we can  
make a difference.™

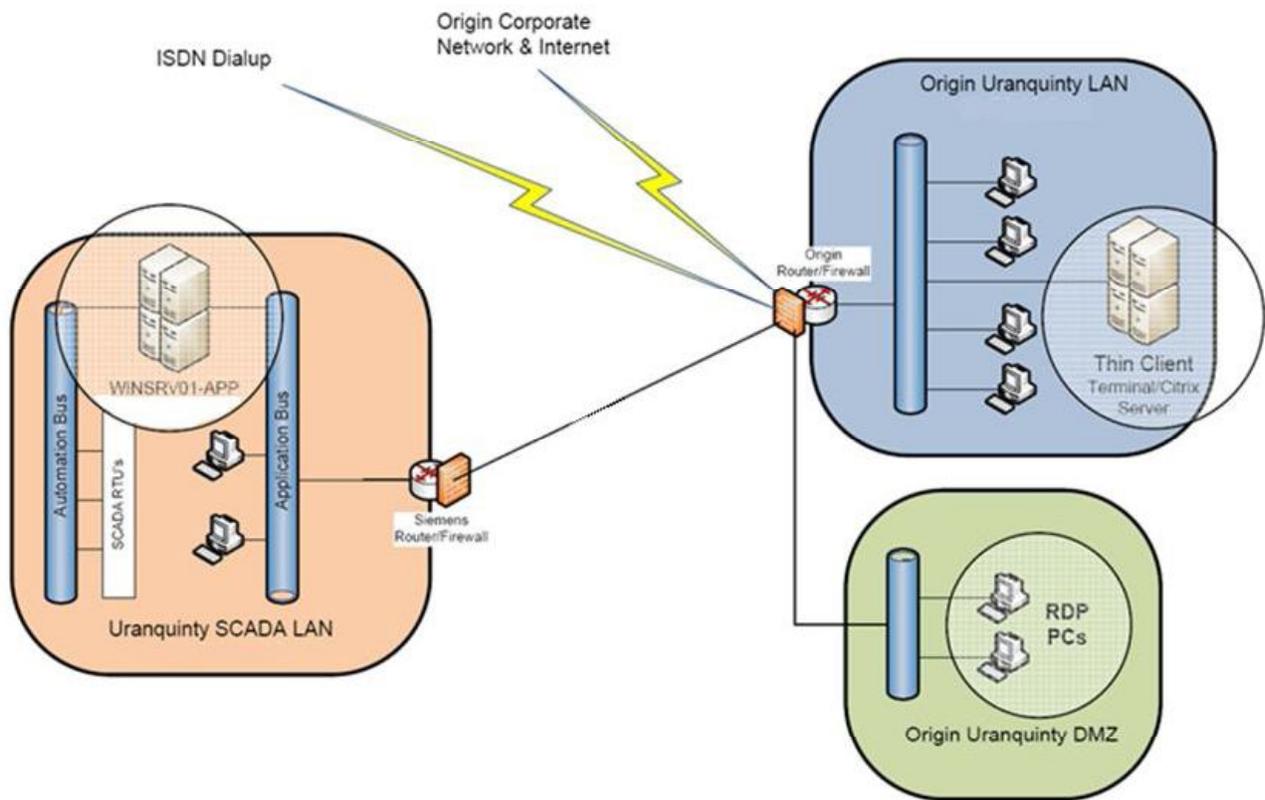
origin

## Remote Operation & Monitoring



# Remote Access Setup

Together we can make a difference.™





### **High Availability and Reliability**

- Triple Redundancy of PCs in DMZ
- Assigned PCs for Operations and Traders
- Additional T3000 Licences
- Monitoring of user login limits
- Limited Access to key users
- Network Redundancy

Together we can  
make a difference.™

origin

Security  
measures  
considered &  
implemented



## Security measures considered and implemented

Together we can  
make a difference.™



### **Security measures considered:**

- Network security
- Operational security
- Physical Security

## Network security

Together we can  
make a difference.™



- OEM Advice: Siemens White paper - T3000 Security
- IT Vulnerability Assessment
  - Application security
  - Intrusion detection
  - Regulation of physical access to the SCADA network
- I&C Guideline - Remote operation of peaking power station



### Asset Management Guideline

### Remote Operation and Monitoring setup for Peaking Power Stations

Released on June 22<sup>nd</sup> 2009

Revision: 1.0

GEN-AMS-GDL-104

## Network security - Contd.

Together we can  
make a difference.™



### Password Authentication Model:

- **Authentication** is the software process of identifying a user who is authorized to access the SCADA system.
- **Authorisation** is the process of defining access permissions on the SCADA system and allowing users with permissions to access respective areas of the system

### Password Compliancy:

- User name specific instead of common practice of Generic usernames.
- Passwords changes periodically.
- Logins disabled immediately for anyone leaves company or moves from within functional area.

### Network Topology:

- Simple networks are at less risk than more complex, interconnected networks. Keep the network simple and, more importantly, well documented from the beginning.
- A key factor in ensuring a secure network is the number of contact points. These should be limited as far as possible.

## Network security - Contd.

Together we can  
make a difference.™



- Standard Architecture with Network security Zones

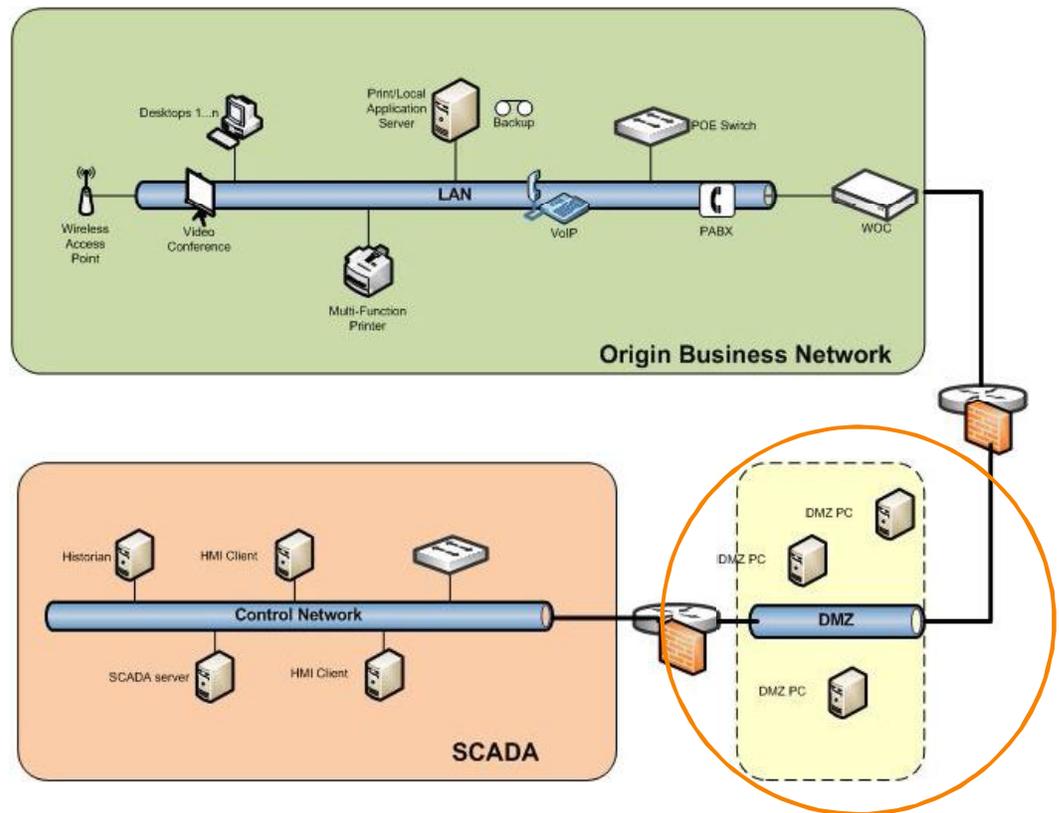
- This network is considered a "Restricted" zone in accordance with Origin Enterprise Security Architecture - Logical Network Zone Model.
- The security of the SCADA DMZ Network shall include a network firewall device that is compliant with Origin architecture
- Restrict access to the SCADA DMZ Network and Applications to only authenticated users and specified network communication protocols required for the applications running on the host computers
- SCADA DMZ Network communication shall be given priority over general Origin Business Network communications
- The SCADA DMZ consists of 2 network security zones; the SCADA DMZ being restricted and the Control System being secured

# Network security - Contd. Standard Architecture

Together we can  
make a difference.™

origin

- Firewalls
- RDP access to DMZ PCs.





### Operational Security measures considered:

- Enable and Disable remote operation of Gas Turbine to avoid inadvertent operation of GT
- Provide Emergency GT Trip

# Operational Security - Contd.

- Below are examples of different operational access rights.
- Remote Operations may be blocked by the Uranquinty Duty Operator.

Together we can make a difference.™

origin

The screenshot displays four turbine control panels (GT 11, GT 12, GT 13, GT 14) with various operational parameters and controls. The panels are arranged in a grid. Each panel includes a 'START/STOP CONTROL' section with 'SQC GAS TURBINE' and 'GT START/STOP' buttons, a 'TURB CTRL INDICATIONS' section with 'RUN UP FUNCTION ACTIVE', 'SPEED CTRL ACTIVE', 'LOAD CTRL ACTIVE', 'OTC CTRL ACTIVE', and 'LOAD LMT CTRL ACTIVE' indicators, and an 'ACTIVE POWER SETPOINT' section with 'SETPOINT FROM AGC' and 'RAMP RATE FAST' controls. The 'CURRENT CONDITIONS MAX LOAD' is also displayed for each turbine.

GT 11: 1.71 Hz, 0 MW, -0 Mvar. Current conditions: 141 MW. Legend: REMOTE OPERATION (white), REMOTE TRIP (grey), STATION SERVICES (red, yellow, blue).

GT 12: 1.68 Hz, -0 MW, -0 Mvar. Current conditions: 144 MW. Legend: REMOTE OPERATION (white), REMOTE TRIP (grey), STATION SERVICES (red, yellow, blue).

GT 13: 1.67 Hz, -0 MW, -0 Mvar. Current conditions: 142 MW. Legend: REMOTE OPERATION (white), REMOTE TRIP (grey), STATION SERVICES (red, yellow, blue).

GT 14: 1.68 Hz, -0 MW, -0 Mvar. Current conditions: 143 MW. Legend: REMOTE OPERATION (white), REMOTE TRIP (grey), STATION SERVICES (red, yellow, blue).

Operations enabled

Blocked from operation by local operator

RED = OK, ON, Run, Open, Active.

Green = Not Available, OFF, Closed.