Remote Access Setup

Together we can make a difference.™

origin

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.™

origin

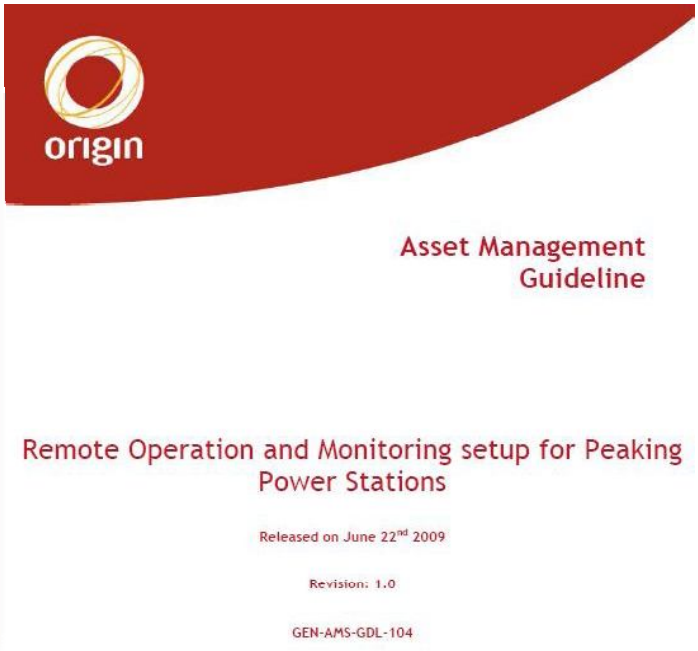
Security measures considered:

- 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



origin

Asset Management Guideline

Remote Operation and Monitoring setup for Peaking Power Stations

Released on June 22nd 2009

Revision: 1.0

GEN-AMS-GDL-104

Network security – Contd.

Together we can make a difference.™

origin

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.™

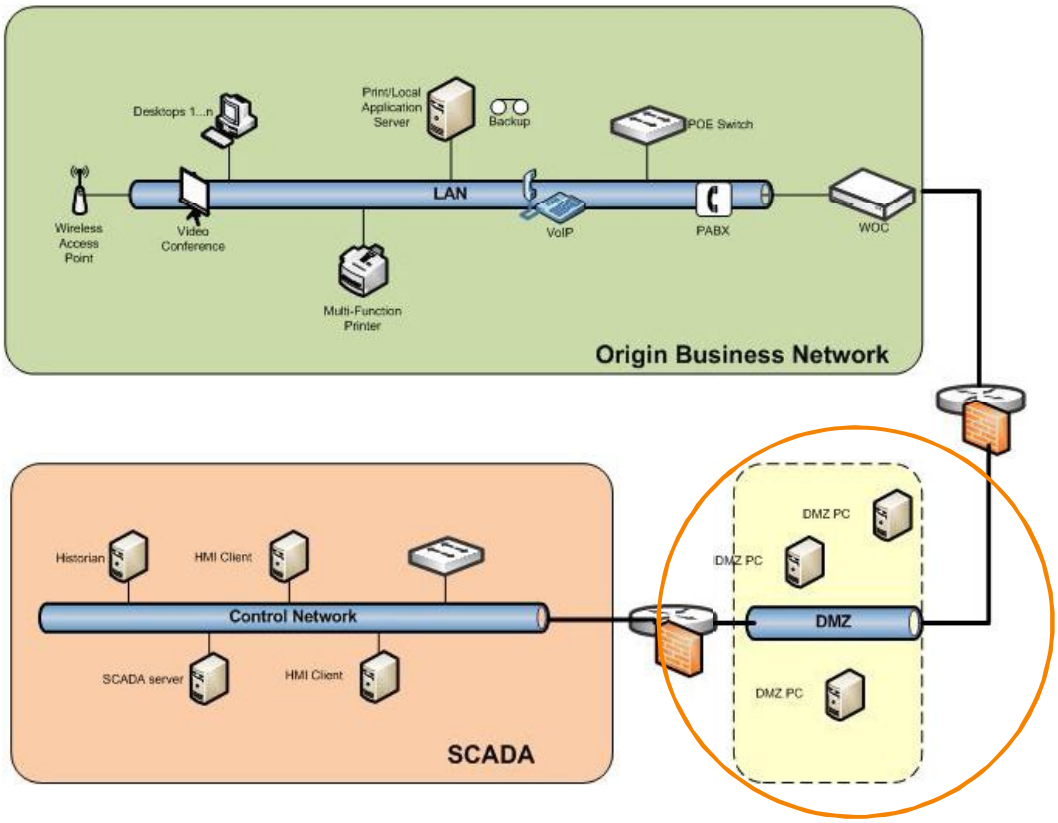
- Standard Architecture with Network security Zones
  - This network is considered a "Restricted" zone in accordance with Origin Enterprise Security Architecture - Logical Network Zone Model.
  - The security of the SCADA DMZ Network shall include a network firewall device that is compliant with Origin 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

Together we can
make a difference.™

Operational Security measures considered:

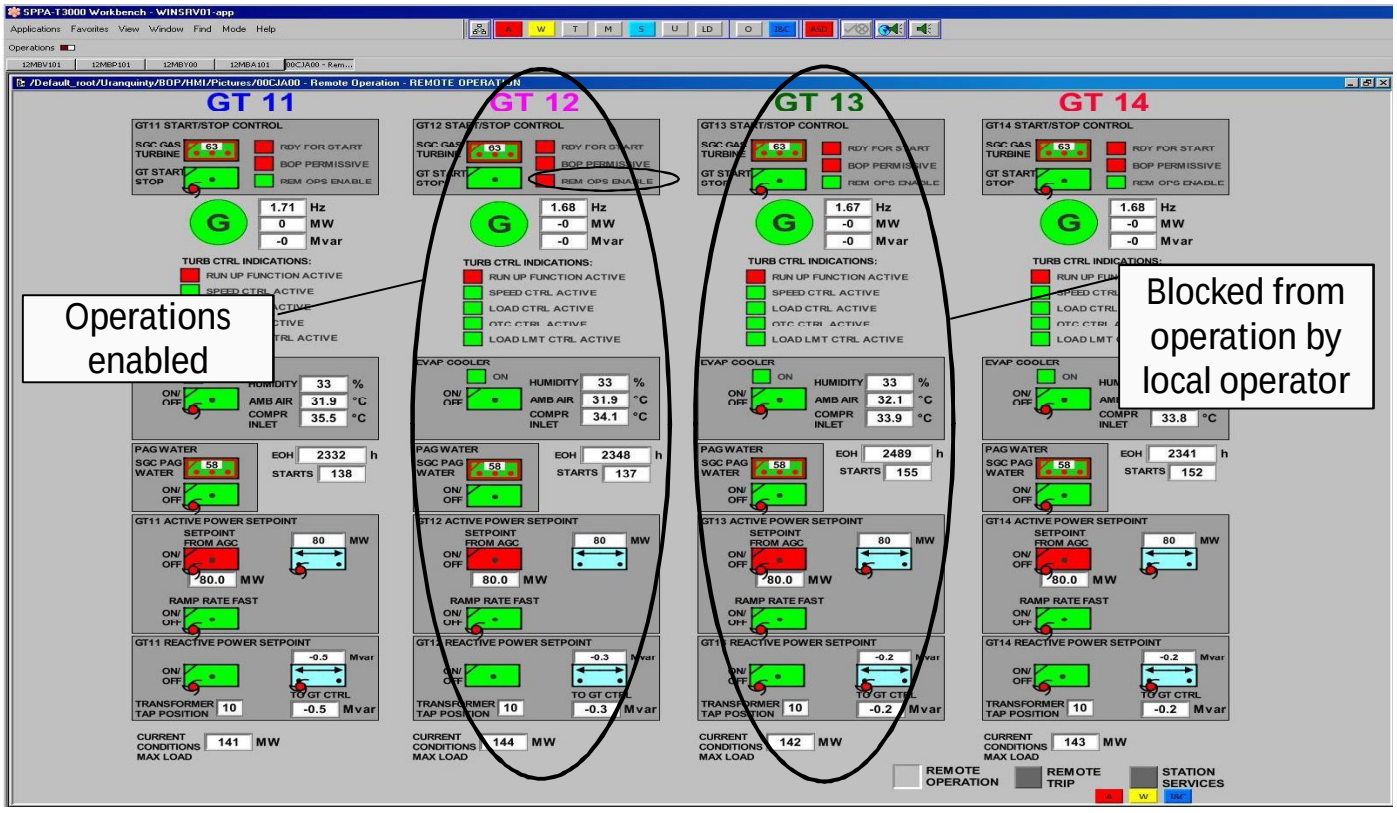
- Enable and Disable remote operation of Gas Turbine to avoid inadvertent operation of GT
- Provide Emergency GT Trip

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



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.

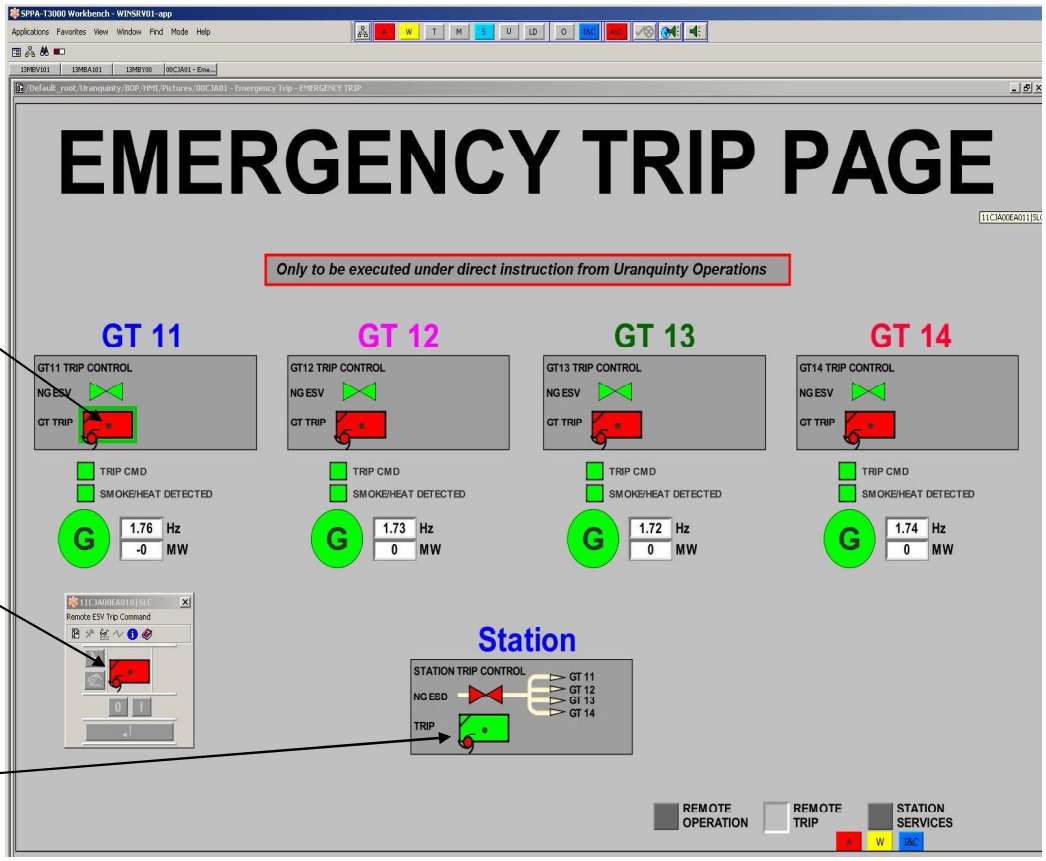
Only under extreme circumstances will the Duty Trader need to use this page.

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.



Physical Security

Together we can
make a difference.™

Power Stations and Control Rooms

- Physical Lockout and Swipe Card Access
- Operator Alarm

Together we can
make a difference.™

origin

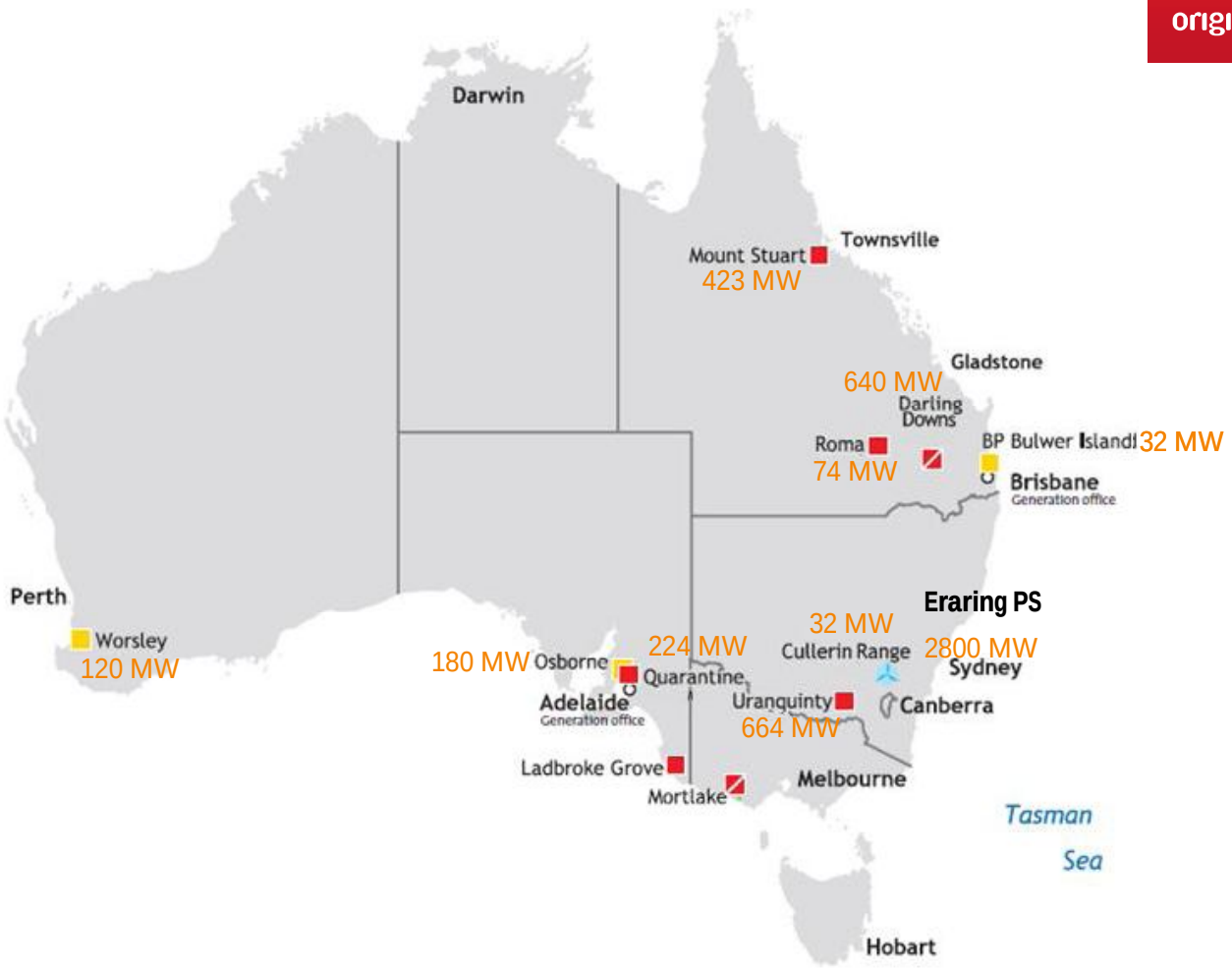
Centralised Remote Operations – Tangiblle Benefits and security threats

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

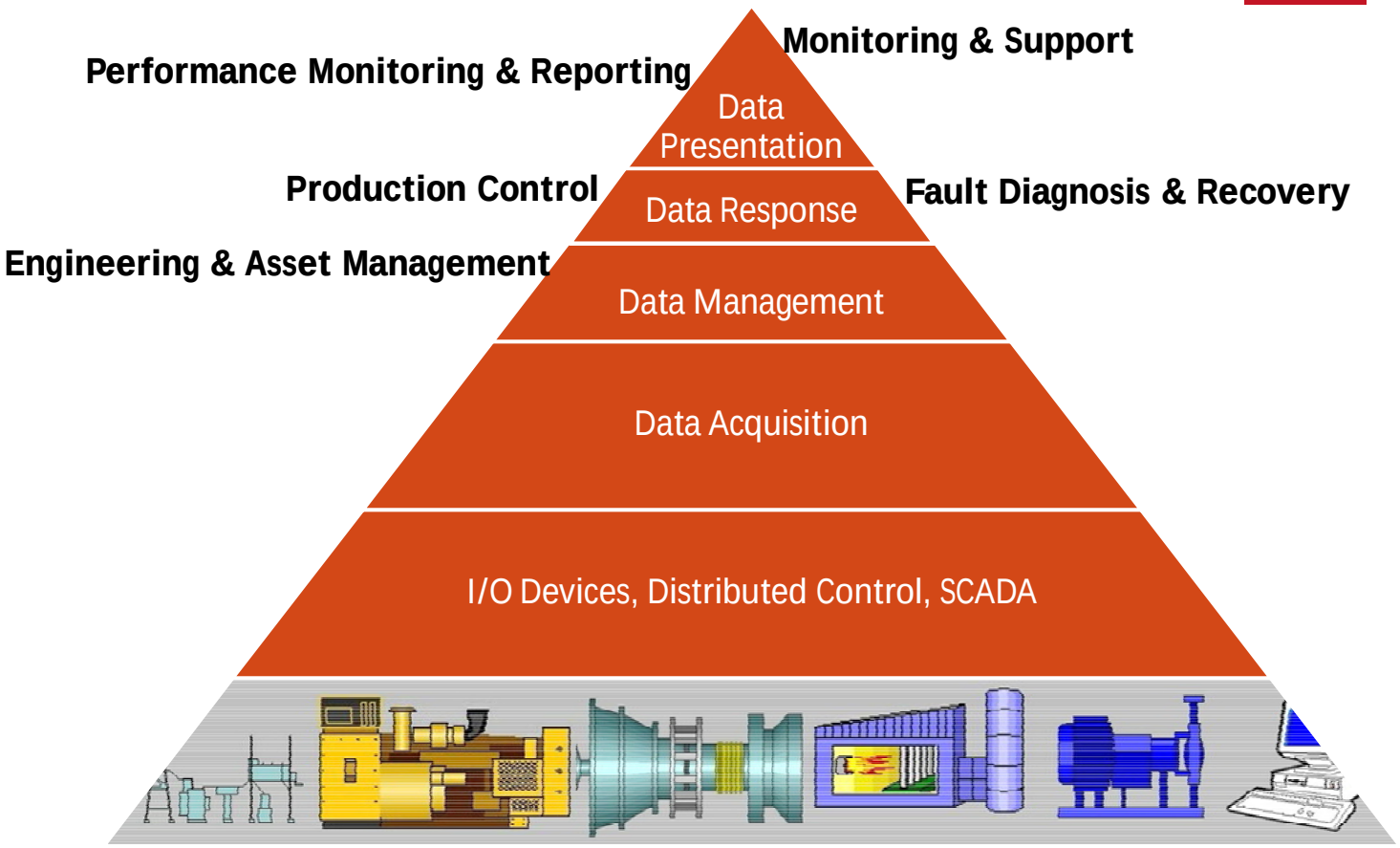
Centralised Remote Operations and Monitoring



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.™

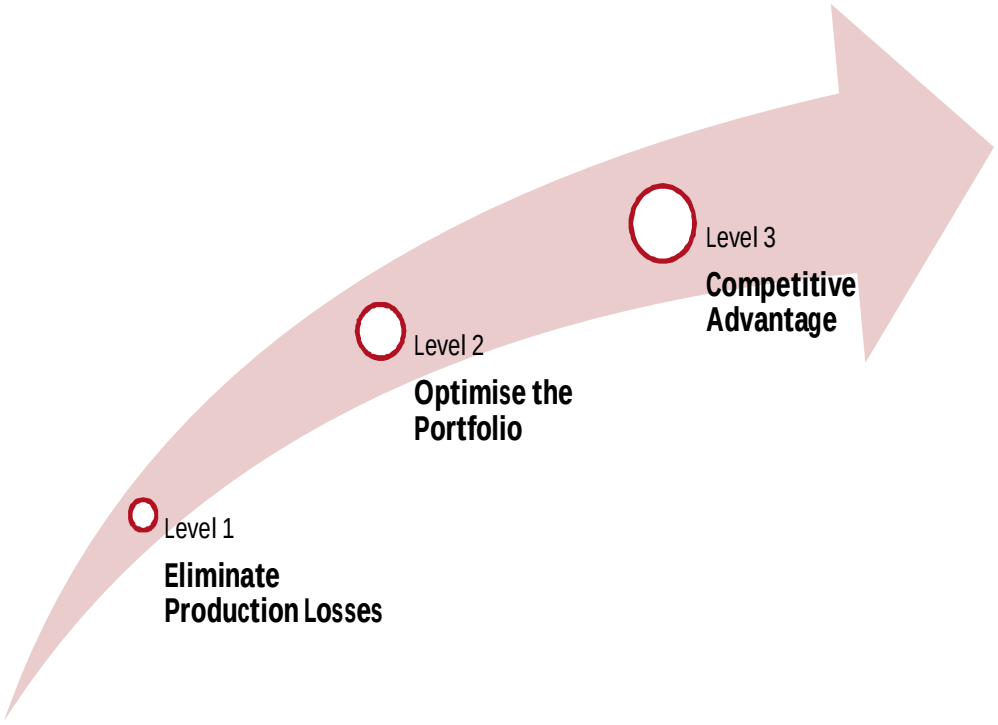
origin

- 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



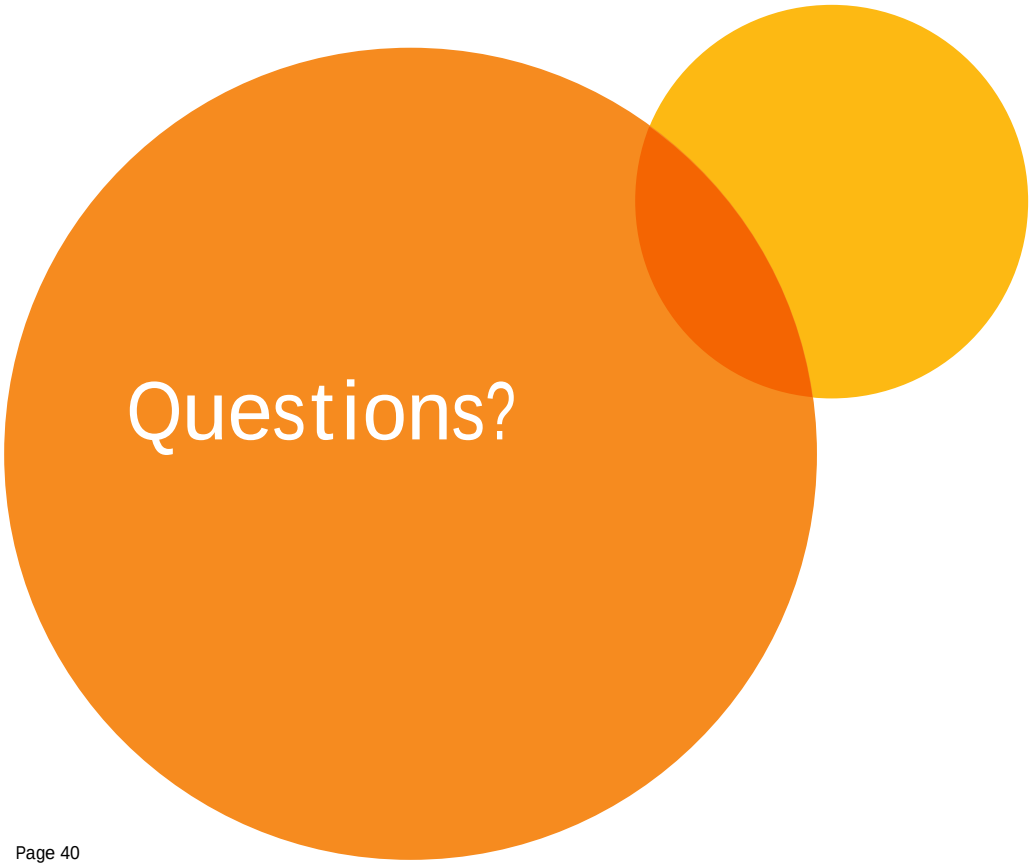
SCADA/DCS installed at Origin Generation sites

Together we can make a difference.™

origin

Generation Site	
Mt Stuart Power Station	Mitsubishi Netmation & GE Mark VIes
Roma Power Station	Citect/Triconex
Darling Downs Power Station	GE Mark VIes
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 Vies
Cullerin Range Wind Farm	Citect/Foxboro

origin


Questions?

ISA Delhi Section

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 : 13-14th Jan. 2012

Together we can make a difference.™

Overview

Together we can make a difference.™

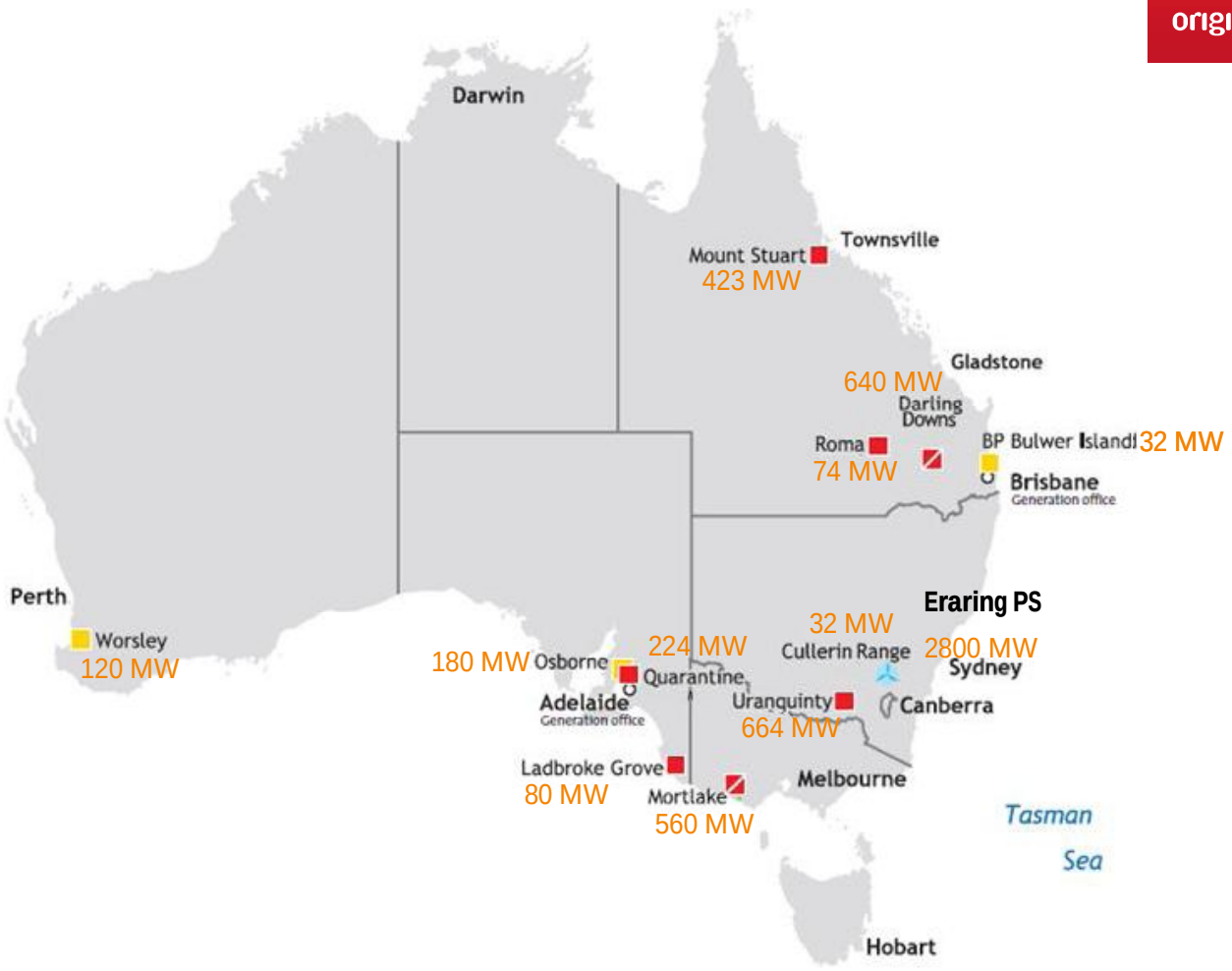
- Origin – Generation portfolio
- Remote operational capability at Origin Power Stations
- Establish remote operation for Peaking Power Station
- Security measures considered and implemented
- Centralised Remote Operations – Tangible Benefits and security threats.

Together we can
make a difference.™

origin

Origin – Generation Portfolio

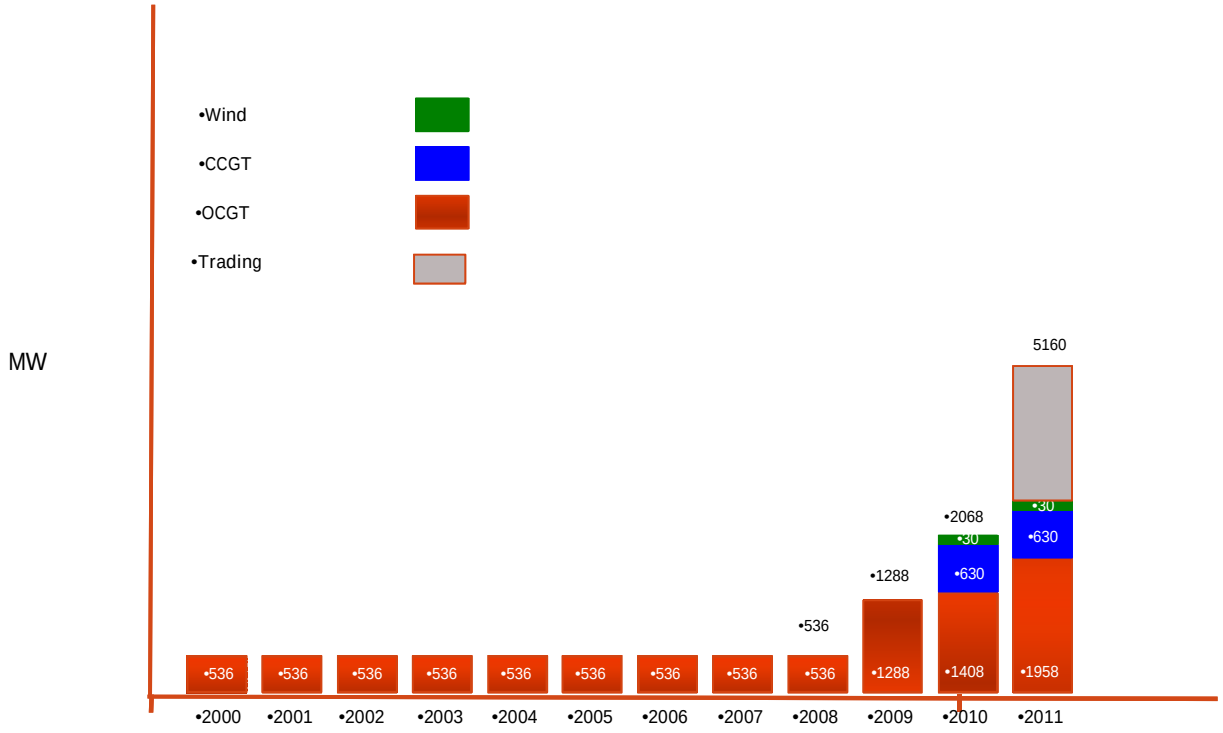
Generation Portfolio



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.™

origin

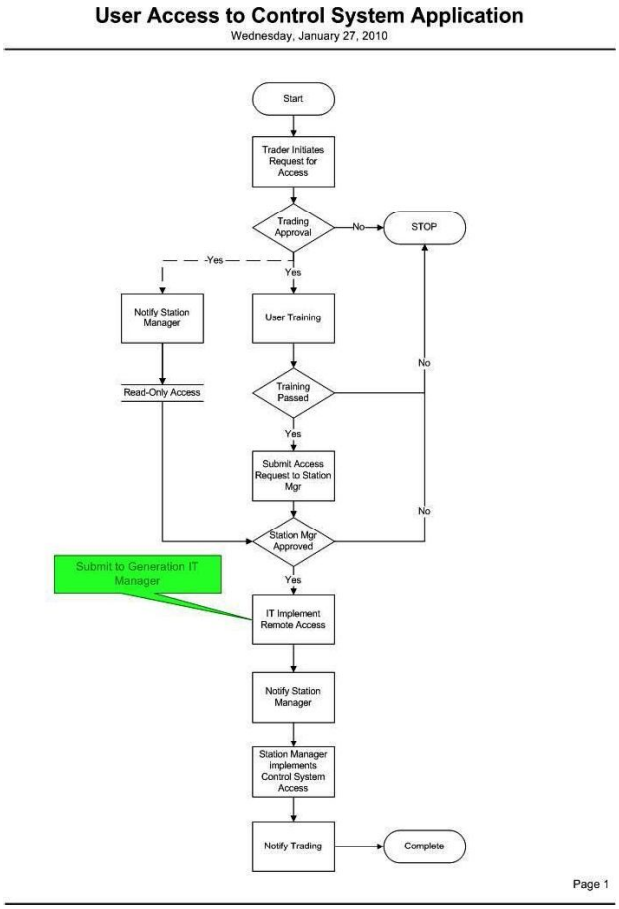
- Train Commercial traders to operate power plant:
  Plant Operational Competency Model which includes:

  - 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

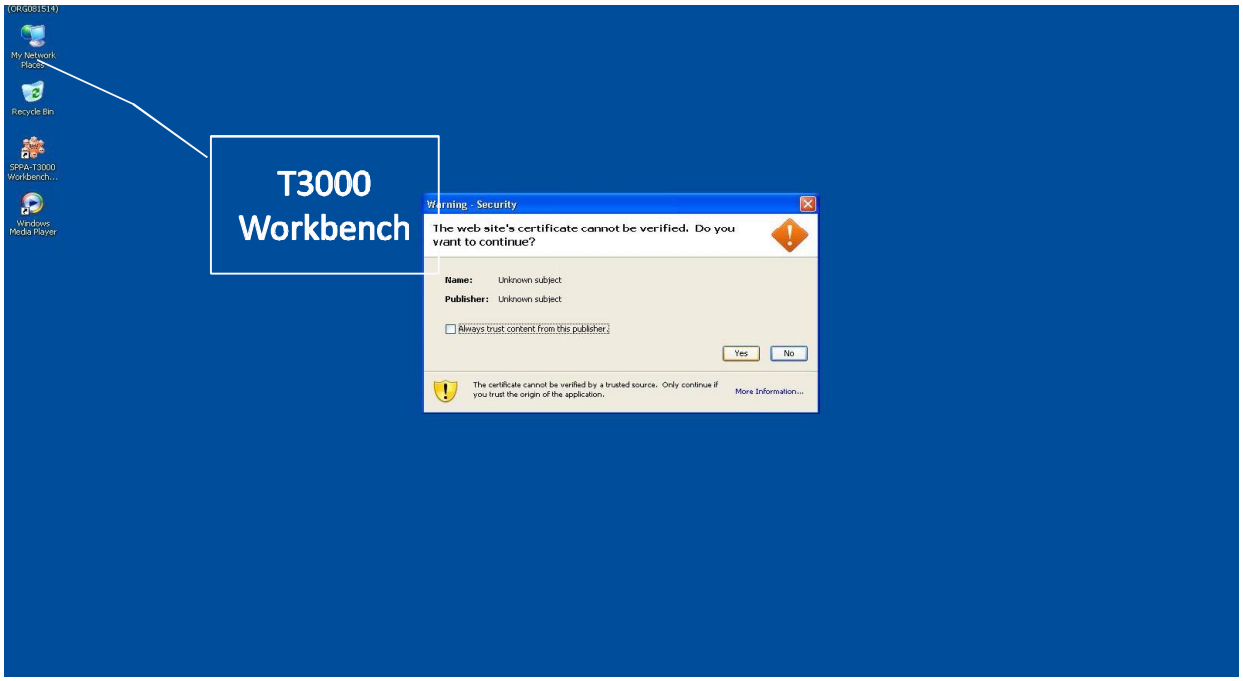


Connecting to Plant Control System (SPPA T3000) - Overview

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.

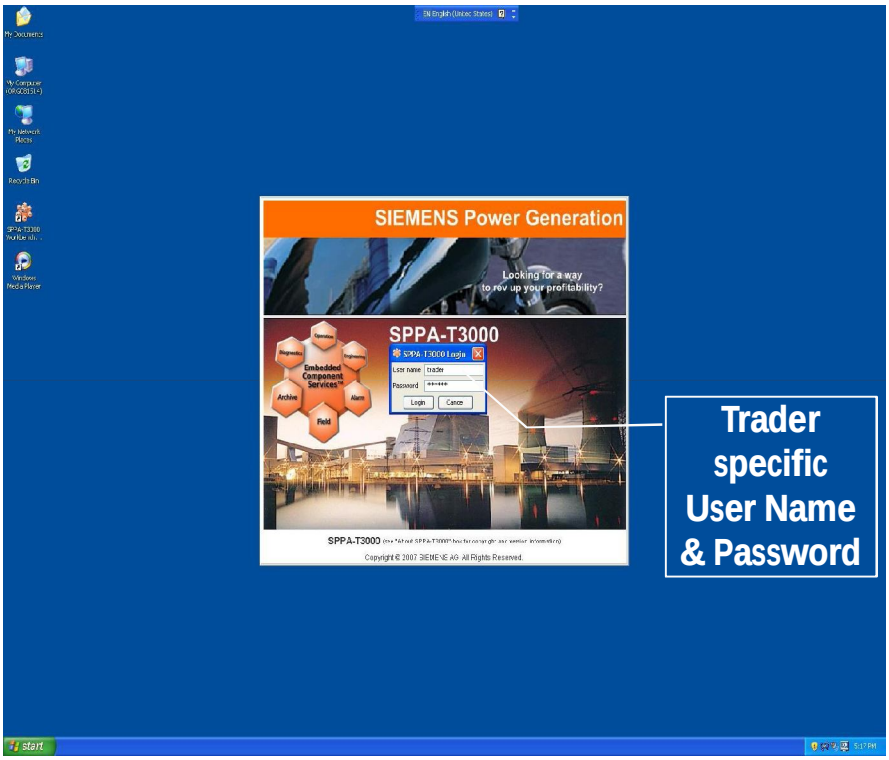


Uranquinty Control System Access

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

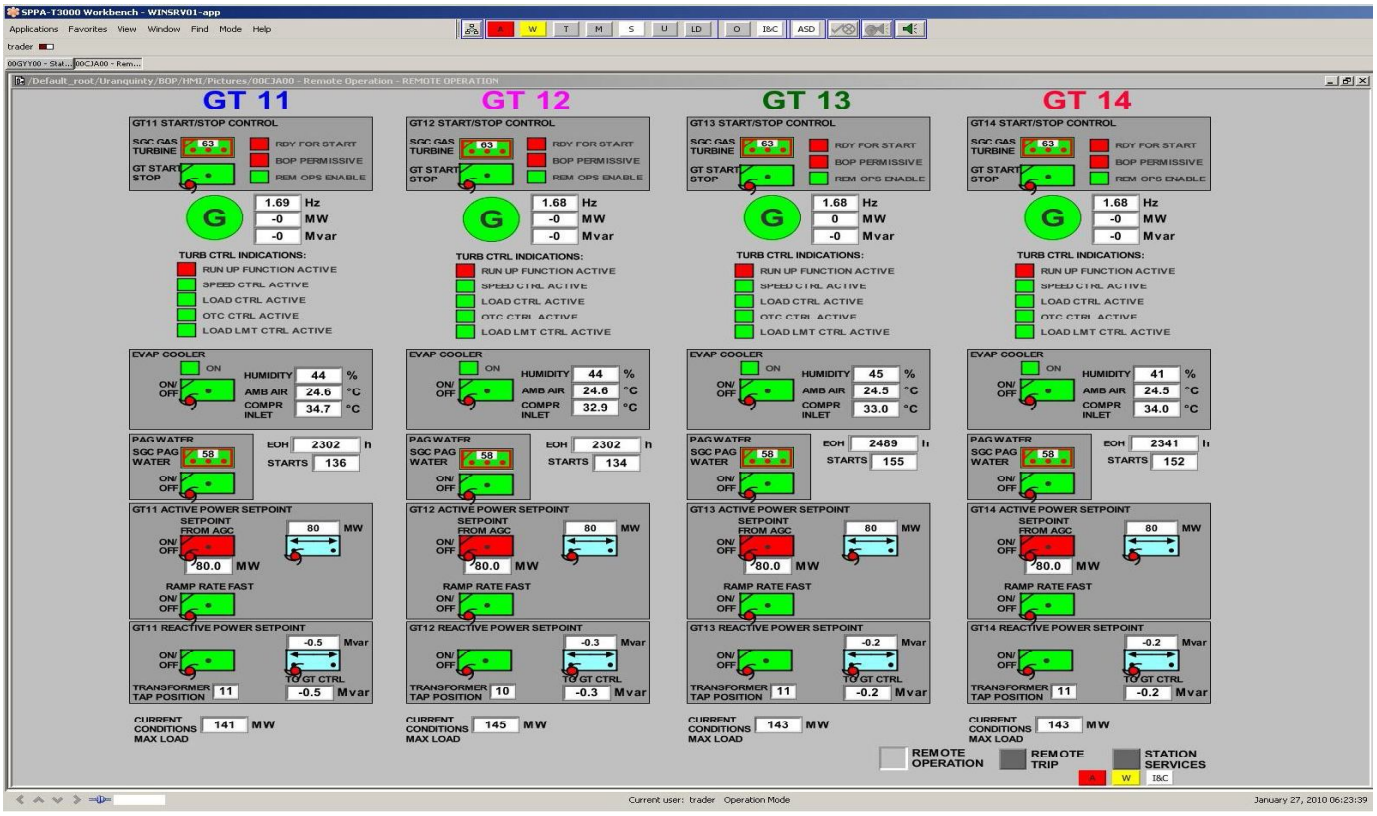


Customised HMI for Traders

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

Together we can make a difference.™

origin

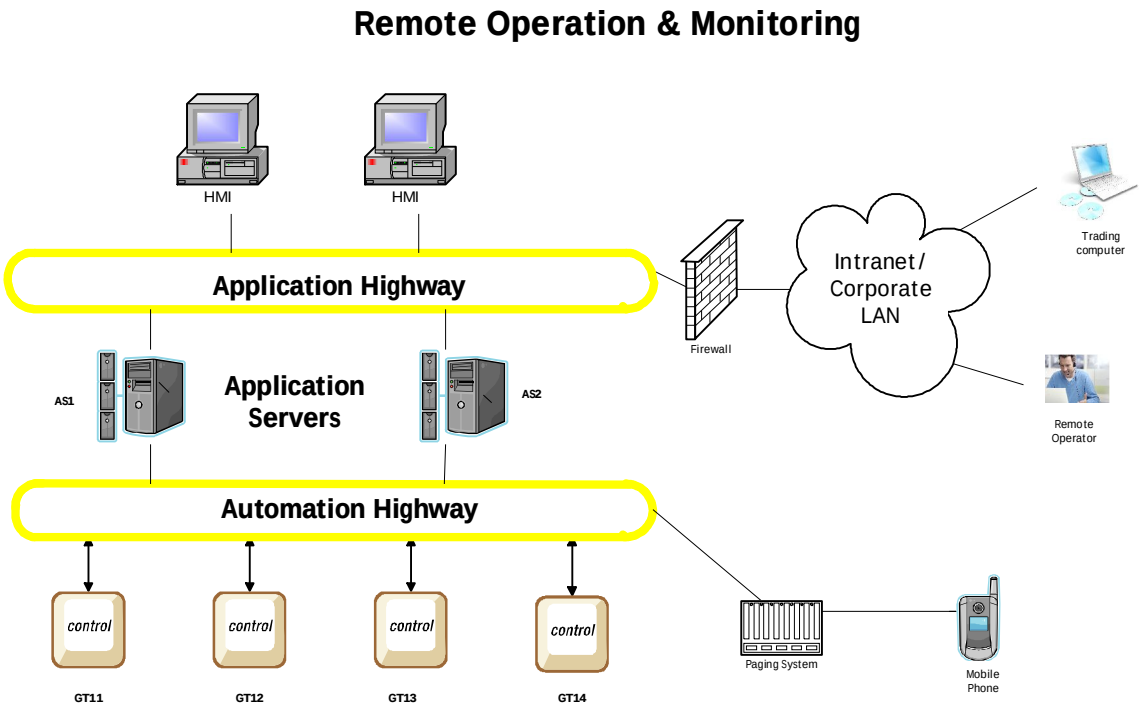


RED = OK, ON , Run , Open, Active. **Green = Not Available, OFF, Closed.**

DCS Network Architecture

Together we can make a difference.™

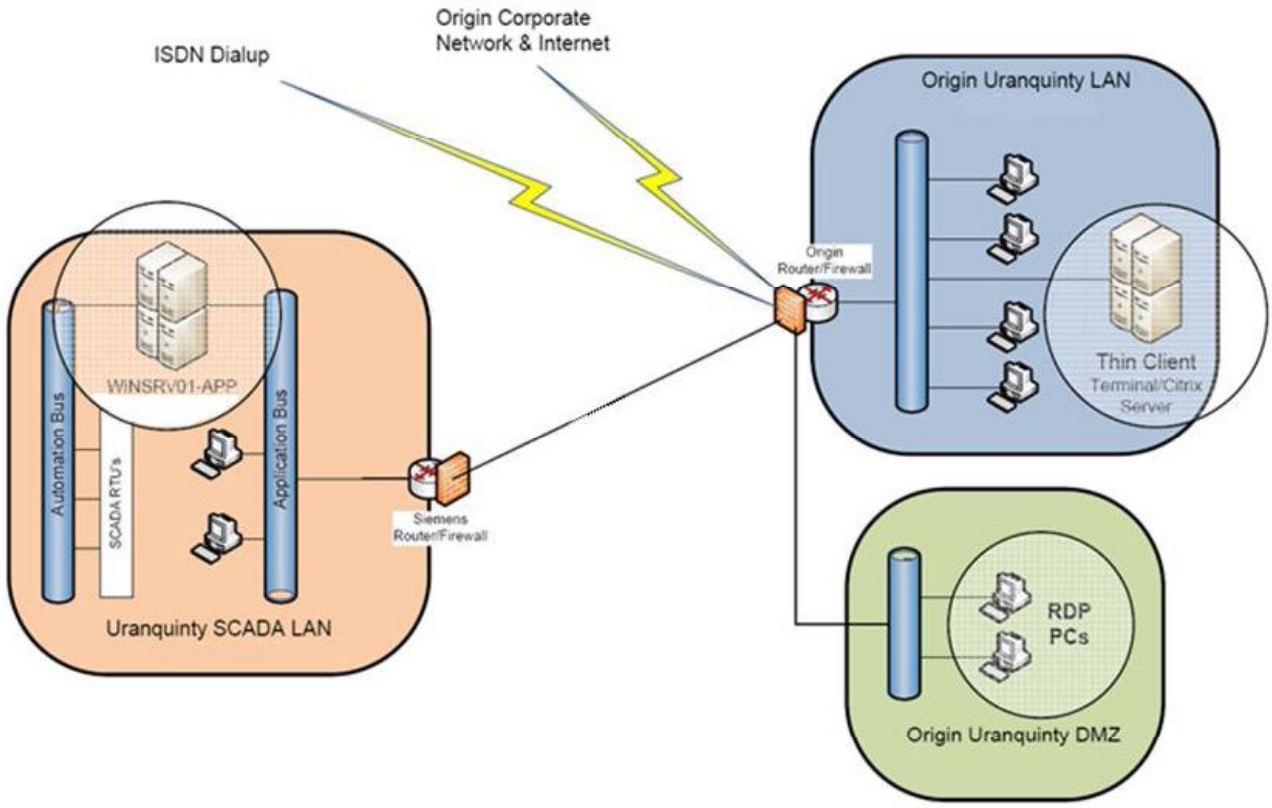
origin



Remote Access Setup

Together we can
make a difference.™

origin



Remote Access Setup

Together we can
make a difference.™

origin

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.™

origin

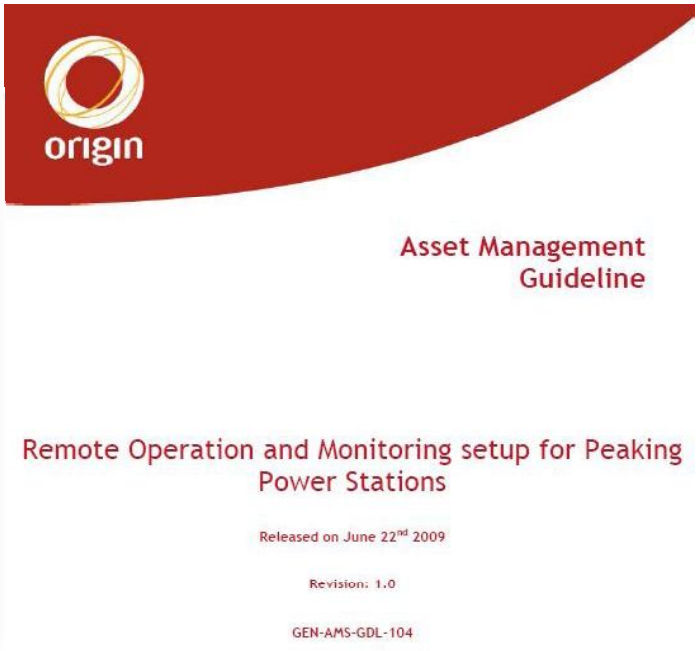
Security measures considered:

- 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



origin

Asset Management Guideline

Remote Operation and Monitoring setup for Peaking Power Stations

Released on June 22nd 2009

Revision: 1.0

GEN-AMS-GDL-104

Network security – Contd.

Together we can make a difference.™

origin

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.™

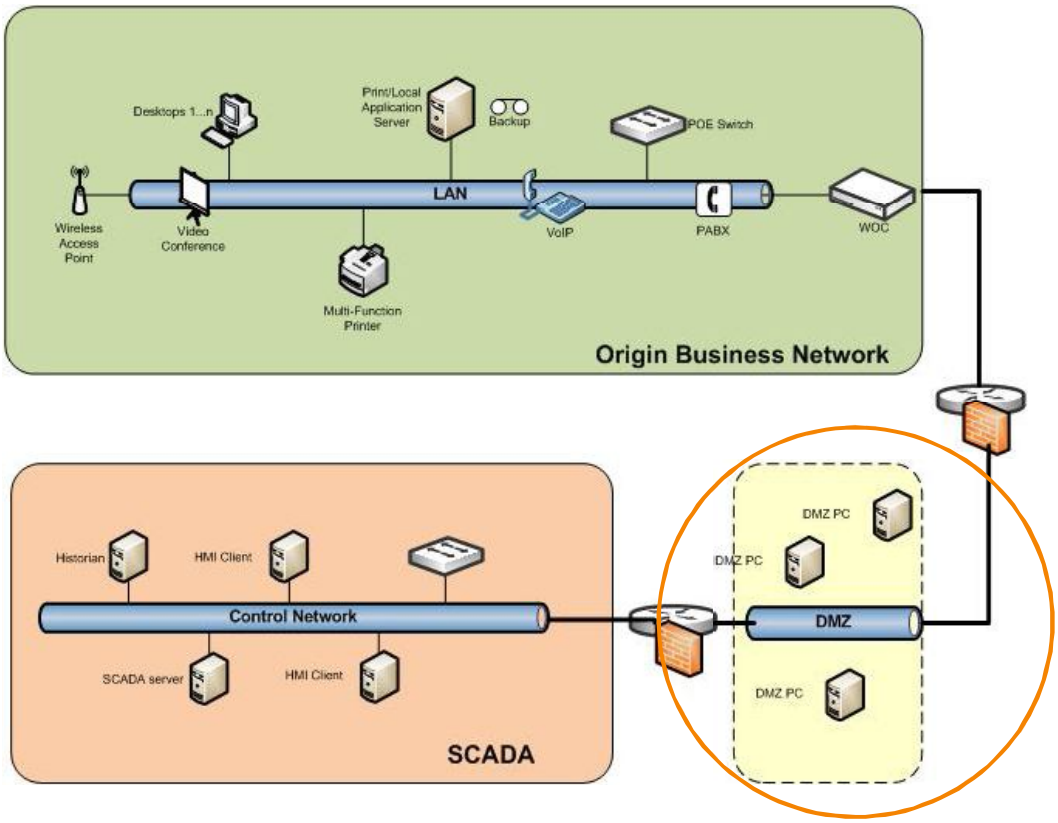
- Standard Architecture with Network security Zones
  - This network is considered a "Restricted" zone in accordance with Origin Enterprise Security Architecture - Logical Network Zone Model.
  - The security of the SCADA DMZ Network shall include a network firewall device that is compliant with Origin 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

Together we can make a difference.™

Operational Security measures considered:

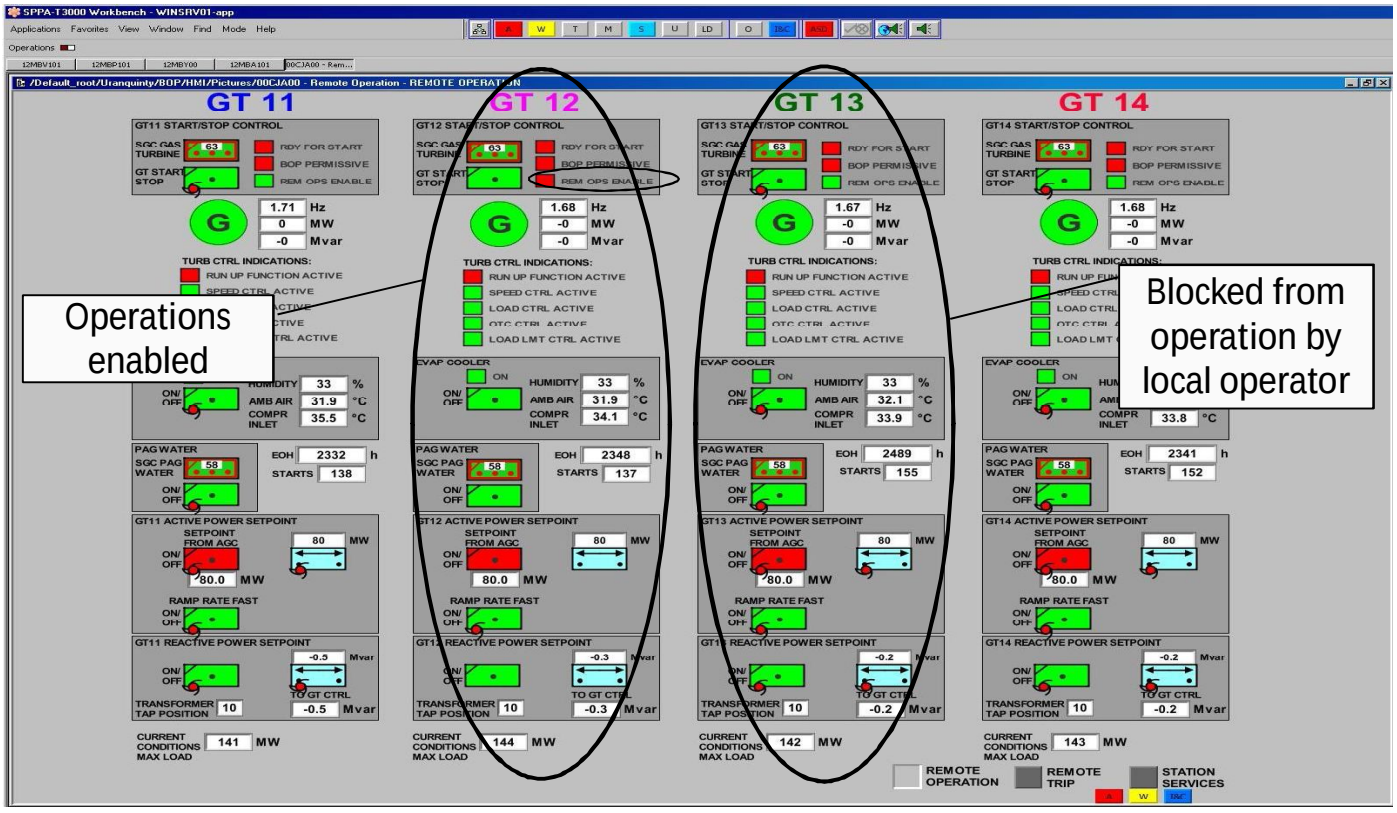
- Enable and Disable remote operation of Gas Turbine to avoid inadvertent operation of GT
- Provide Emergency GT Trip

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



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

Green = Not Available, OFF, Closed.