Legal notice

The following presentation contains forward-looking statements concerning BG Group plc’s strategy, operations, financial performance or condition, outlook, growth opportunities or circumstances in the countries, sectors or markets in which BG Group plc operates, or the recommended cash and share offer by Royal Dutch Shell plc for BG Group plc announced on 8 April 2015. By their nature, forward-looking statements involve uncertainty because they depend on future circumstances, and relate to events, not all of which can be controlled or predicted. Although the Company believes that the expectations reflected in such forward-looking statements are reasonable, no assurance can be given that such expectations will prove to have been correct. Actual results could differ materially from the guidance given in this presentation for a number of reasons. For a detailed analysis of the factors that may affect our business, financial performance or results of operations, we urge you to look at the “Principal risks and uncertainties” included in the BG Group plc Annual Report & Accounts 2014. Nothing in this presentation should be construed as a profit forecast and no part of this presentation constitutes, or shall be taken to constitute, an invitation or inducement to invest in BG Group plc or any other entity, and must not be relied upon in any way in connection with any investment decision. BG Group plc undertakes no obligation to update any forward-looking statements.

No representation or warranty, express or implied, is or will be made in relation to the accuracy or completeness of the information in this presentation and no responsibility or liability is or will be accepted by BG Group plc or any of its respective subsidiaries, affiliates and associated companies (or by any of their respective officers, employees or agents) in relation to it.
BG Group at a Glance

We are an international exploration and production and LNG company.
Facility Types

On and offshore production, LNG liquefaction, Coal Seam Gas …
Engineering Support & GTAs

• Asset Centric Operations
  – Asset Technical Authorities

• Central Engineering Resource
  – **LEAD - SERVE – ASSURE**
    – Discipline Leaders
      – Group Technical Authorities

• Central IT with outsourced services
The Journey
2006: The Journey begins …

- Operations provide Process Data to the business
  - Firewall - but not appropriately configured
  - Data provision is the emphasis (no remote access)
- 2007: PDMS core solution for industrial firewall (minimum security)
- 2010: Automation Framework Guideline introduces 3-tier architecture; mandated in 2013 Standard
Standards and Accountability Map

L4 - Corporate network

L3- Central Admin PIN

L3 – Facility Admin PIN
L3 – Facility Management PIN
L3 – Facility Application PIN

L3 – Utility

L2- ICSS

PHD

Controller Firewall

L1 Control Network

3rd party systems
Early Days: Engineering and ICS Cyber Security

- Systems deployed, but limited engagement with Engineering Community
- Engineering and IT in isolation
- Engineering not understanding Operations need for real time data
- BUT – they make the most of the remote access channels now (unofficially) open!
- No realisation of the cyber security risks introduced
2013: The Awakening

Group Audit – P1 Action
- We do not understand our ICS cyber security risk

Assets: Talk to the hand
- Security is IT’s business
- Our systems are air-gaped
- We are busy with real work

IT: It’s Technology!
- It’s an IT infrastructure programme

Automation:
- The list of audit actions seems like an impossible task,
- I cannot articulate the risk
- Oh dear, there is no funding
- How did this land on us?
The message to assets...

- People
- Processes
- Technology

enable PCE Security to facilitate Integrated Operations
Up a Gear
Three Levers for a Shift Change

A. Understanding our environment- **Basis of our strategy**

B. A Vision and a 3 year Roadmap- **Direction for structured and sustainable change**

C. Focus on people: **Drive security through change in attitudes, culture and behaviour**
Three Levers for a Shift Change

A. Understanding our environment—Basis of our strategy

B. A Vision and a 3 year Roadmap—Direction for structured and sustainable change

C. Focus on people: Drive security through change in attitudes, culture and behaviour
A: Understanding our Environment

• Group Audit P1 finding (June 2013) – we do not understand our risk

• Assessments completed at all Operated assets (2014)
  – Key risks highlighted
  – PCE Network topology and inventories produced
  – Quick wins identified

• We broadly understand our risk

• 3 year programme developed to address this risk
  – Integrated IT and C&I programme
  – Managing PCE Security to be BAU
Risk Assessment: The Basis of our Strategy

- Created a common awareness of the process control environment
- Articulated the business risks, and enabled a risk based remediation
- Identified the most effective immediate controls are in **people and process**
- Basis for the integrated IT-Engineering programme (Technology controls)

### PCE Security Area

<table>
<thead>
<tr>
<th>Topic</th>
<th>Platform XYZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1.6 Process Control Remote Access</td>
<td>43%</td>
</tr>
<tr>
<td>10.3.1 Security Management and SPA</td>
<td>24%</td>
</tr>
<tr>
<td>10.3.2 Segregated Architecture</td>
<td>100%</td>
</tr>
<tr>
<td>10.3.3 Data Communications</td>
<td>100%</td>
</tr>
<tr>
<td>10.3.4 Connectivity of Machines to networks</td>
<td>82%</td>
</tr>
<tr>
<td>10.3.5 Connection of Engineering Machines</td>
<td>33%</td>
</tr>
<tr>
<td>10.3.6 Microsoft Domains</td>
<td>100%</td>
</tr>
<tr>
<td>10.3.7 Physical Extension of PCE</td>
<td>N/A</td>
</tr>
<tr>
<td>10.3.8 Malware Protection</td>
<td>40%</td>
</tr>
<tr>
<td>10.3.9 Security Patching</td>
<td>7%</td>
</tr>
<tr>
<td>10.3.10 System Hardening</td>
<td>84%</td>
</tr>
<tr>
<td>10.3.11 Passwords and Accounts</td>
<td>33%</td>
</tr>
<tr>
<td><strong>Overall Compliance</strong></td>
<td>45%</td>
</tr>
<tr>
<td><strong>Estimated Risk from an Incident</strong></td>
<td><strong>2C</strong></td>
</tr>
</tbody>
</table>
Common (Group) Risk

Accidental or Intentional Impact on Production* caused by:

• Malware introduced by removable media or remote network connection;
  • 2 incidents late 2014

• Malware on maintenance laptops;
  • 1 incident 2014 (infection via vendor laptop)

• Misuse of external access to the PCE
  • E.g. remote connections enabling the exploitation of unpatched vulnerabilities or system access via default passwords;

• Inability to repair/restore systems in a timely manner;

• Systems compromised due to obsolete (unpatched) software.

Notes:
• *Safety risks were also considered however loss of production dominates.
Three Levers for a Shift Change

A. Understanding our environment - Basis of our strategy

B. A Vision and a 3 year Roadmap - Direction for structured and sustainable change

C. Focus on people: Drive security through change in attitudes, culture and behaviour
B: The PCE Security Vision

• **PCE Security enables secure Integrated Operations.**

• **For all the assets in which BG Group has an interest PCE Security management (protection and detection) is commensurate with the perceived risk**, which is well understood and measured via selected KPIs.

• **PCE Security is led and sustained by BG Group Assets**, with support and direction from the centre.

• **Relevant personnel have sufficient awareness to do their part in securing the PCE.**

• **Security incidents, if they do occur, are expediently detected, contained, eradicated and the situation recovered.**
Three Levers for a Shift Change

A. Understanding our environment- Basis of our strategy

B. A Vision and a 3 year Roadmap- Direction for structured and sustainable change

C. Focus on people: Drive security through change in attitudes, culture and behaviour
Safety Moment: Use of Engineering Laptops
C: Focus on People: Culture and Competence

Management Visibility
- Corporate Governance
- The Security Barrier Model

Company wide Awareness
- Front Line Staff Training (E-Learning module)
- Security Videos and Posters
- ICS Security procedures

On-Site Ambassadors
- Facility Champions
- Self assessment

Technical Leadership
- Technical Training
- Engaging SPAs* in Design Decisions
- GICSP Certifications

*Single point of accountability
KPIs - Barrier Model

- Network segregation
- End point protection
- Training and competency
- Detection systems

Reduced attack surface
Access control
Portable device / media control
Supervision and communications

Incident response
Cyber risk
PCE Security Procedures

- Use of Removable Media
- Temporary Engineering Machines
- Password and Account Management
- AV and Patching
- PCE Security Incident Management
- Backup and Recovery
- PCE Security Documentation
The Facility Champion

- **Responsible for implementing secure working practices in the process control environment to mitigate the risk of ‘loss of control’ due to a cyber-security incident**
  - Tailoring the Procedures for the facility, and implementing them
  - Improve procedures adoption; report against non-compliance.
  - Ensure vendors and service providers are aligned to BG security requirements
    - Ensuring facility visitors follow the BG security requirements
  - Culture change – mindsets and work practices of the Facility staff
  - Production and maintenance of a facility implementation plan;
    - Report progress to the Asset PCE SPA and BG PCE Security Engineer
    - Escalating any issues within the implementation plan
  - Assist with technical remediation, lead on facility
# Security Procedures - Calibration

<table>
<thead>
<tr>
<th>Procedure</th>
<th>0% Nothing in Place</th>
<th>25% of Procedural Requirements in Place</th>
<th>50% of Procedural Requirements in Place</th>
<th>75% of Procedural Requirements in Place</th>
<th>100% Already Operating in Line with Procedural Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Use of Temporary Engineering Machines</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>2. Use of Removable Media</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>3. Use of USB Locks</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>4. Anti-virus and Patching</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>5. Password and Account Management</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>6. PCE Security Documentation</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>7. PCE Security Incident Management</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>8. Backup &amp; Recovery</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
</tbody>
</table>
In Summary ...

DONT'T FORGET THE PEOPLE
## The 2 year turnaround

### 2013

- **Awareness**
  - IT led
  - Changes pushed to the Assets
  - Focused on Level 3 (L3) Infrastructure only.

- **Leadership**
  - Security is only for the corporate IT.
  - Process control does not require security

- **Attitude**
  - We think there is a risk, but
    - we cannot articulate
    - and anyway we have bigger things to worry about

### 2015

- **Awareness**
  - We understand our ICS cyber security risks;

- **Leadership**
  - Requirements and Strategy led by Engineering
  - Pull from Asset C&I community for improving security (L3-L0)

- **Attitude**
  - Security is like Safety, part of everything we do
Our Experience

• Technology matters, but

• **People and process matter more**
  
  — First and last line of defence

  — Security can only be sustained if the culture is aligned to this objective

  — Ongoing support, maintenance and development of the technology can only occur if the people and process are competent and engaged.

• **ICS Security is underpinned and sustained by the knowledge, awareness and competence of our people, and the processes they follow.**