HARNESSING INDUSTRIAL CONTROL SYSTEMS SECURITY IN A GLOBAL ORGANIZATION

SANS European ICS Security Summit
September 2015

Maarten Oosterink
Principal PCD IT Security Engineer
DEFINITIONS AND CAUTIONARY NOTE

The companies in which Royal Dutch Shell plc directly and indirectly owns investments are separate entities. In this document “Shell”, “Shell group” and “Royal Dutch Shell” are sometimes used for convenience where references are made to Royal Dutch Shell plc and its subsidiaries in general. Likewise, the words “we”, “us” and “our” are also used to refer to subsidiaries in general or to those who work for them. These expressions are also used where no useful purpose is served by identifying the particular company or companies. “Subsidiaries”, “Shell subsidiaries” and “Shell companies” as used in this document refer to companies over which Royal Dutch Shell plc either directly or indirectly has control. Companies over which Shell has joint control are generally referred to as “joint ventures” and companies over which Shell has significant influence but neither control nor joint control are referred to as “associates”. The term “Shell interest” is used for convenience to indicate the direct and/or indirect ownership interest held by Shell in a venture, partnership or company, after exclusion of all third-party interest.

This presentation contains forward-looking statements concerning the financial condition, results of operations and businesses of Royal Dutch Shell. All statements other than statements of historical fact are, or may be deemed to be, forward-looking statements. Forward-looking statements are statements of future expectations that are based on management’s current expectations and assumptions and involve known and unknown risks and uncertainties that could cause actual results, performance or events to differ materially from those expressed or implied in these statements. Forward-looking statements include, among other things, statements concerning the potential exposure of Royal Dutch Shell to market risks and statements expressing management’s expectations, beliefs, estimates, forecasts, projections and assumptions. These forward-looking statements are identified by their use of terms and phrases such as “anticipate”, “believe”, “could”, “estimate”, “expect”, “intend”, “may”, “plan”, “objectives”, “outlook”, “probably”, “project”, “will”, “seek”, “target”, “risks”, “goals”, “should” and similar terms and phrases. There are a number of factors that could affect the future operations of Royal Dutch Shell and could cause those results to differ materially from those expressed in the forward-looking statements included in this presentation, including (without limitation): (a) price fluctuations in crude oil and natural gas; (b) changes in demand for Shell’s products; (c) currency fluctuations; (d) drilling and production results; (e) reserves estimates; (f) loss of market share and industry competition; (g) environmental and physical risks; (h) risks associated with the identification of suitable potential acquisition properties and targets, and successful negotiation and completion of such transactions; (i) the risk of doing business in developing countries and countries subject to international sanctions; (j) legislative, fiscal and regulatory developments including potential litigation and regulatory measures as a result of climate changes; (k) economic and financial market conditions in various countries and regions; (l) political risks, including the risks of expropriation and renegotiation of the terms of contracts with governmental entities, delays or advancements in the approval of projects and delays in the reimbursement for shared costs; and (m) changes in trading conditions. All forward-looking statements contained in this presentation are expressly qualified in their entirety by the cautionary statements contained or referred to in this section. Readers should not place undue reliance on forward-looking statements. Additional factors that may affect future results are contained in Royal Dutch Shell’s 20-F for the year ended 31 December, 2014 (available at www.shell.com/investor and www.sec.gov ). These factors also should be considered by the reader. Each forward-looking statement speaks only as of the date of this presentation, 28 September 2015. Neither Royal Dutch Shell nor any of its subsidiaries undertake any obligation to publicly update or revise any forward-looking statement as a result of new information, future events or other information. In light of these risks, results could differ materially from those stated, implied or inferred from the forward-looking statements contained in this presentation. There can be no assurance that dividend payments will match or exceed those set out in this presentation in the future, or that they will be made at all.

We use certain terms in this presentation, such as discovery potential, that the United States Securities and Exchange Commission (SEC) guidelines strictly prohibit Shell from including in filings with the SEC. U.S. Investors are urged to consider closely the disclosure in our Form 20-F, File No. 1-32575, available on the SEC website www.sec.gov. You can also obtain this form from the SEC by calling 1-800-SEC-0330.
This presentation intends to share some experiences, learnings and thoughts for those that are, or will be implementing projects to improve Industrial Control Systems (ICS) Security. This presentation will not discuss technology, but focus is on the following topics:

- Defining a standard
  - IT and Engineer
  - Vernacular
  - Lifecycle
  - Partners and peers
- Assuring your standard
  - Lines of defence
  - Trias politica
  - A journey across cultures
DEFINING A STANDARD
RAISING KIDS IN A MIXED MARRIAGE: IT & ENGINEERING
Linking ICS Security & Barrier Thinking

Making the Mixed Marriage Work: Vernacular

Diagram showing the relationship between hazards, threats, barriers, scenarios, and consequences.
MANAGING THE HOUSEHOLD BUDGET: COST & BENEFIT

<table>
<thead>
<tr>
<th>Agent</th>
<th>Authorization</th>
<th>Motivation</th>
<th>Top Event</th>
<th>Initial Risk</th>
<th>Practice Areas - Control Effectiveness (likelihood)</th>
<th>Practice Areas - Control Effectiveness (impact)</th>
<th>Residual Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>Internal</td>
<td>Non-authorized</td>
<td>Denial of Service</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Indirect</td>
<td>External</td>
<td>Non-authorized</td>
<td>Denial of Process Data</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

Not properly tested Operating System patch update or Antivirus signature file causes a disruption in the operation of a control system.
RAISING KIDS: SETTING ACHIEVABLE GOALS

Process Control Domain IT Security Bow-Tie

- **Prepare**
  - Governance
  - Workforce Development
  - Management of Change
  - Asset Inventory

- **Prevent**
  - Access Control
  - Portable Media
  - Portable Computers
  - Operating System Security Patches

- **Detect**
  - Event Log Management
  - Anti-Virus

- **Respond**
  - Network Architecture
  - Incident Response

- **Recover**
  - Backup and Restore

© Shell Global Solutions International B.V. | September 2015
RAISING KIDS: SETTING ACHIEVABLE GOALS

NIST Cyber Security Framework

Identify
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect
- Access Control
- Awareness and Training
- Data Security
- Information Protection Process and Procedures
- Maintenance
- Protective Technology

Detect
- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

Respond
- Response Planning
- Communications
- Analysis
- Mitigation

Recover
- Recovery Planning
- Improvements
- Communication
**ICS SECURITY LIFECYCLE**

**Buy Secure:** The Supplier assurance process assesses Shell’s major suppliers of industrial automation and control systems to assure ICS Security is embedded into their product lines and practices.

**Deploy Secure:** The Capital Projects assurance process assures that we deploy secure. To do this we perform policy and design reviews to ensure proper design and implementation of ICS Security and to sign-off as part of Shell’s project assurance framework.

**Run Secure:** The Operating Assets assurance process measures Operating Assets adherence to ICS Security requirements in their day-to-day, run and maintain procedures and activities across all their facilities.

© Shell Global Solutions International B.V.

September 2015
### PCD IT Security Domain Competency Guideline

**November 2015**

#### Competency Profiles for PCD IT Security

<table>
<thead>
<tr>
<th>Competency</th>
<th>Shell Resources</th>
<th>Ecosystem Resources</th>
<th>Vendor Resources</th>
<th>Global GICSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Goal: 100</td>
<td>Goal: 50</td>
<td>Goal: 50</td>
<td>Goal: 1000</td>
</tr>
</tbody>
</table>

#### Shell Resources

- [ ] 100
- [ ] 50
- [ ] 0
- [ ] 45
- [ ] +5

#### Ecosystem Resources

- [ ] 50
- [ ] 25
- [ ] 0
- [ ] 20
- [ ] +5

#### Vendor Resources

- [ ] 50
- [ ] 25
- [ ] 0
- [ ] 15
- [ ] +5

#### Global GICSPs

- [ ] 1000
- [ ] 500
- [ ] 0
- [ ] 550
- [ ] +5

© Shell Global Solutions International B.V.

September 2015
Now available for download:
WIB Plant Security standard
ASSURANCE: LINES OF DEFENCE

Regular assurance process

1\textsuperscript{st} Line of Defence
Security Focal Points on site/project

2\textsuperscript{nd} Line of Defence
Central ICS / IT Security team

3\textsuperscript{rd} Line of Defence
External / Shell Internal Audit
KEY TAKEAWAYS

- Leverage industry standards and practices while recognizing your organization's strategy, culture, and ICS Security maturity.
- Recognize the strengths of Engineering as well as IT and land on a common vernacular.
- One dollar spent buying secure is 10 dollars saved in project, potentially 100 dollars in operation.
- Defining a standard is easy, justifying it is key in getting it from the ground, assuring it is key in getting it implemented as intended.