NEPTUNE ENERGY

Cyber Security Risk Assessments from an Operator Perspective

AGENDA.

NEPTUNE ENERGY

1 Bring cyber expertise to the ICS.

2 Cyber Assessment Framework from an Operators perspective.

3 IT Learnings from the CAF Process.

Presenters

Duncan Hutton
Lead Instrument Engineer

Ben Ramduny
Head of Digital Security

NEPTUNE ENERGY

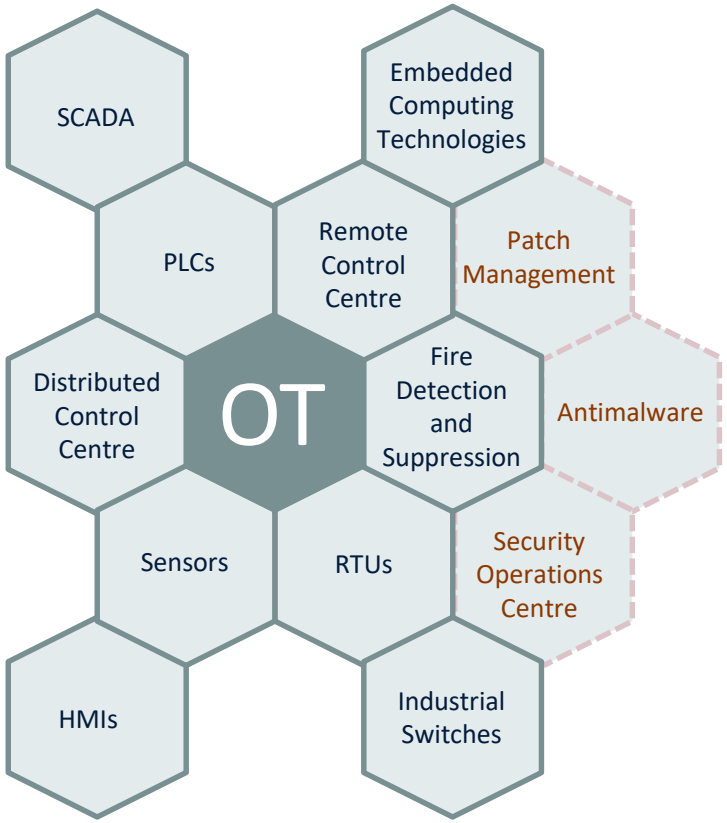
1

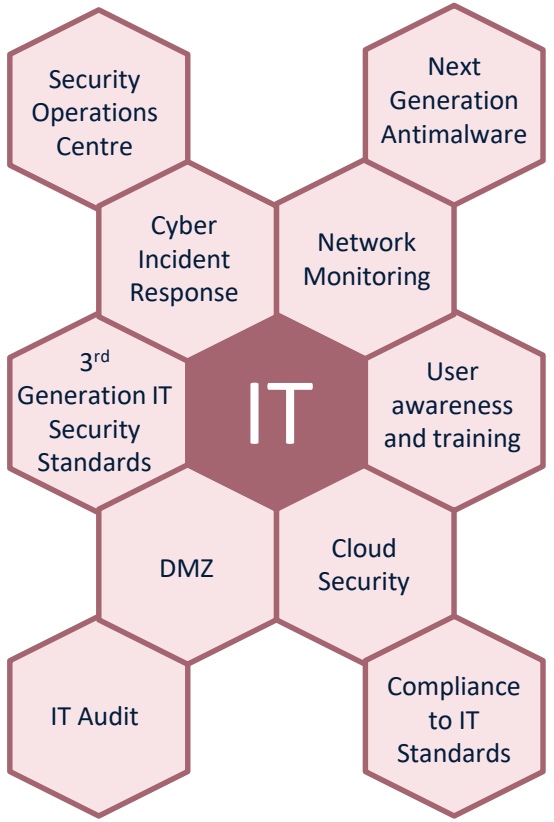
Bring cyber expertise to the ICS

HOW TO BUILD CYBER SECURITY SKILLS IN YOUR INDUSTRIAL CONTROL SYSTEM TEAMS

TRAIN AND UPSKILL YOUR ICS TEAMS?

NEPTUNE ENERGY

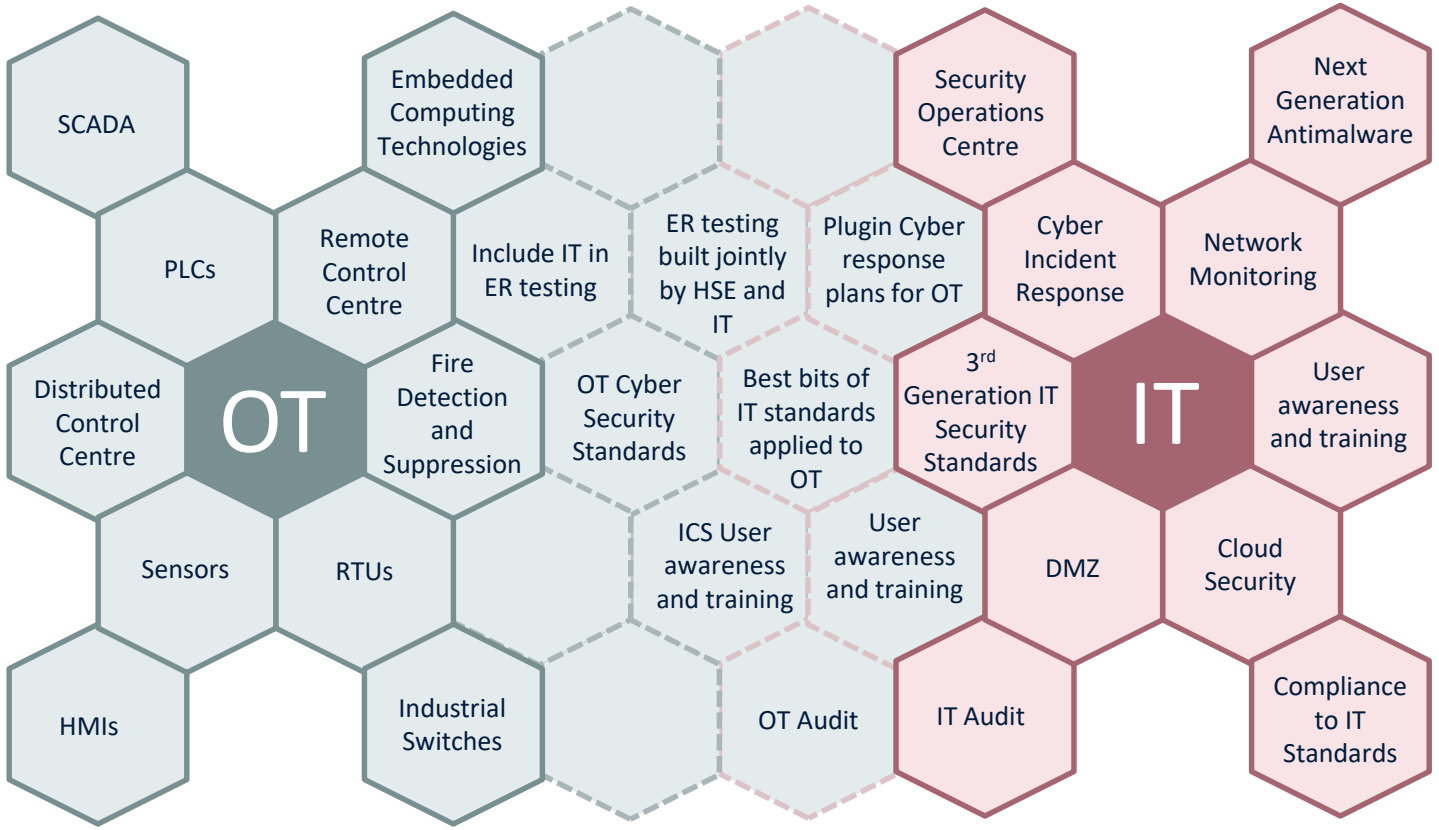




HOW TO BUILD CYBER SECURITY SKILLS IN YOUR INDUSTRIAL CONTROL SYSTEM TEAMS

YOU DON'T, YOU BRING BOTH TEAMS TOGETHER AND LEVERAGE THE EXPERTISE

NEPTUNE ENERGY

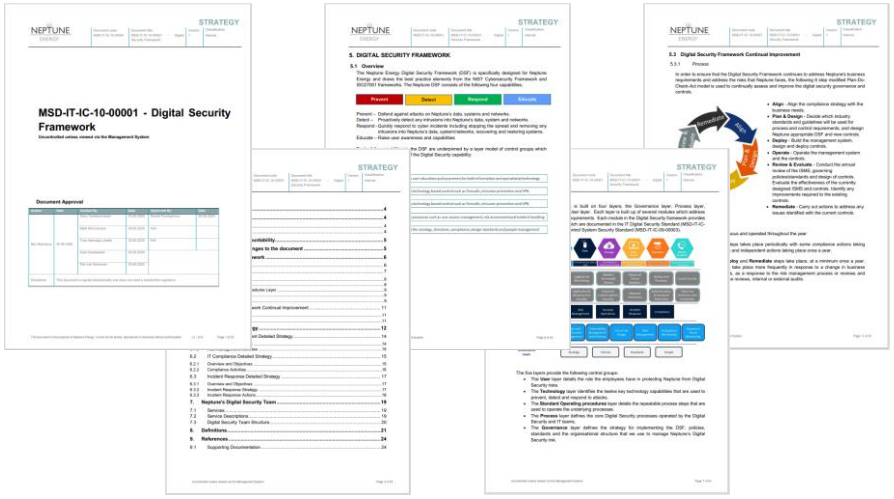


INTEGRATED APPROACH TO CYBER SECURITY

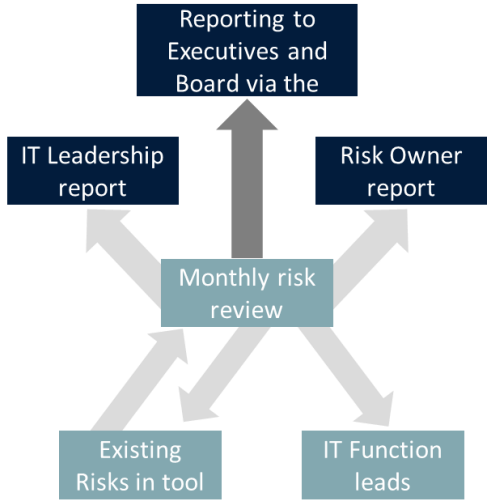
STRUCTURED, STANDARDS BASED, RIGHT TOOLS, MANGING OUR RISKS AND REMAINING COMPLIANT

NEPTUNE ENERGY

1. Define a target, a framework and strategy



2. Build a robust Risk Management process



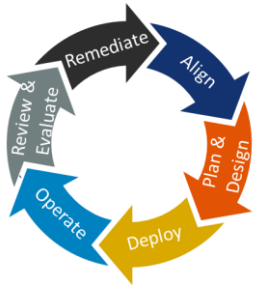
Top Risks:

- Cyber ICS
- Cyber IT
- Outage of IT Systems or Network
- Compliance
- Software Licencing

3. Deploy the right technology and processes

Remote and Cloud Access	Logging and Monitoring	Mobile / Removable Devices	Advanced Threat Analytics	Backup and Recovery	Email Security
Network Security	Application & Infrastructure Security	Industrial Control System Security	Malware Protection	Authentication & Password Protection	Data Loss Detection and Prevention

4. Build 1st line compliance function to monitor controls



INTEGRATED APPROACH TO CYBER SECURITY

STRUCTURED, STANDARDS BASED, RIGHT TOOLS, MANGING OUR RISKS AND REMAINING COMPLIANT

NEPTUNE ENERGY

1. Define a target, a framework and strategy

2. Build a robust Risk Management process

Top Risks:

- Cyber ICS
- Cyber IT
- Outage of IT Systems or Network
- Compliance
- Software Licencing

3. Deploy the right technology and processes

Remote and Cloud Access	Logging and Monitoring	Mobile / Removable Devices	Advanced Threat Analytics	Backup and Recovery	Email Security
Network Security	Application & Infrastructure Security	Industrial Control System Security	Malware Protection	Authentication & Password Protection	Data Loss Detection and Prevention

4. Build 1st line compliance function to monitor controls

2

Cyber Assessment Framework

NEPTUNE ENERGY

- What risk assessment method approach to apply?
- HSE Mandatory completion of Basic Cyber Security Inspection Pack – responses reviewed against OG86
- BCSIP extracted from Cyber Assessment Framework^{v3} for CAT2 installations – is it enough?
- CAF Major Accident Hazard (or loss of essential service) focused:
    - **Review against good practice**
    - **Does not reveal business risk or financial consequence**
    - **Output feeds improvement plan**
- HSE OG86 (MAH Focused) aligned with IEC 62443

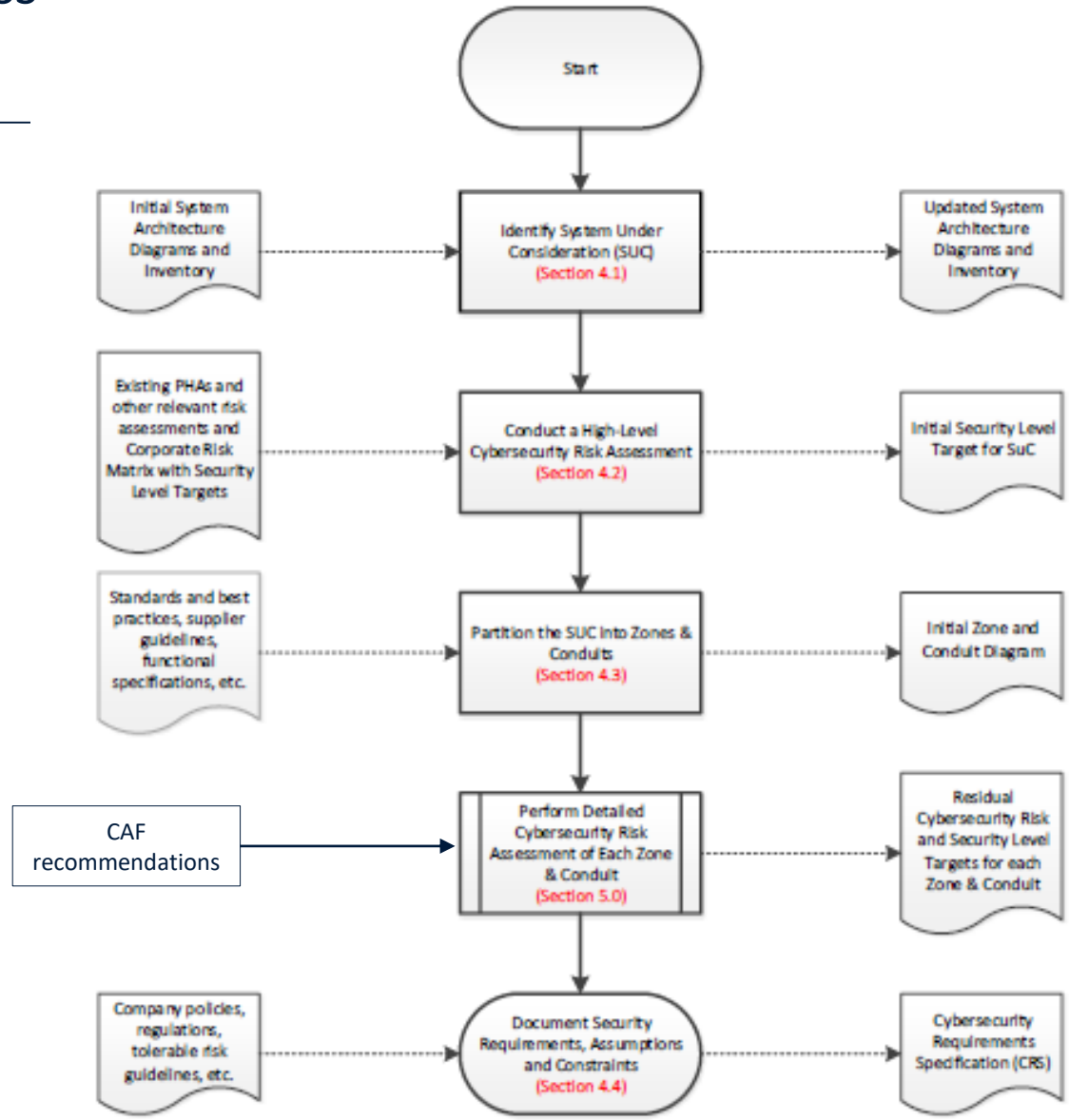
- Neptune ICS Corporate Standard based on NIST 800-82 r2 (annual risk assessment)

- Concluded IEC 62443 compatible with NIST 800-82 r2 and complements CAF

- IEC 62443 risk assessment process identifies:
    - Safety Risk
    - Environmental Risk
    - Business Risk
    - Reputation Risk

CAF & IEC 62443 RISK ASSESSMENT PROCESS

1. **CAF**
2. High Level Risk Assessment
3. Zone & Conduit Analysis
4. Detailed Risk Assessment
5. Cyber Security Improvement Plan
6. Cyber Security Management Plan



See Figure 1 in
IEC 62443-3-2 2015

Why?

- Cygnus is ‘Category 2’ installation.
- HSE expect DH to complete CAF self-assessment and produce improvement plan
- HSE onshore inspection:
  - BCSIP/CAF response & improvement plan against OG 86
- HSE offshore inspection:
  - Cyber Security Barriers breached by a hypothetical Cyber event (compromised engineering workstation)

When?

RA meetings July/August 2020 via MS Teams.

Who?

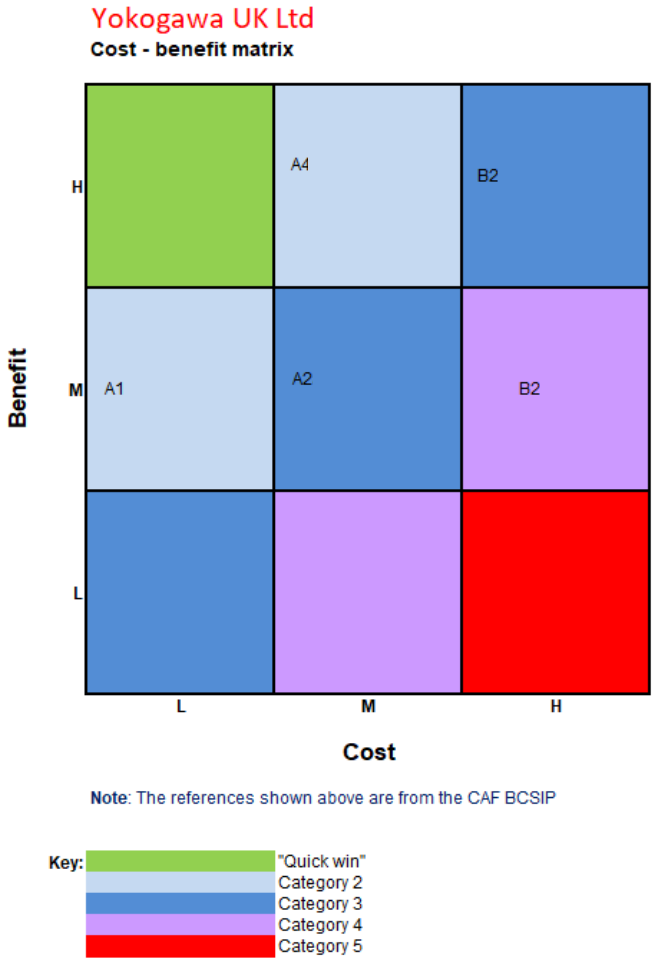
Duncan Hutton – Lead Instrument Engineer
Muhammad Tariq – Instrument Engineer
Rob Turner (Yokogawa – Facilitator and SME)
Tracy Guthrie – Procurement
Sam Smith – Industrial IT
Tony Duncan – Cyber Lead
Ben Ramduny – Head of Digital Security & Risk Management

1. **Self-assessment against the Indicators of Good Practice in BCSIP/CAF**
2. Sort ‘not achieved’ items by cost v benefit.
3. Group by Improvement Category (dependency)
4. Assign a priority to each item.
5. Develop a high-level improvement plan based on Improvement **Category** and **Priority**.

- Matrix shows ref from CAF BCSIP

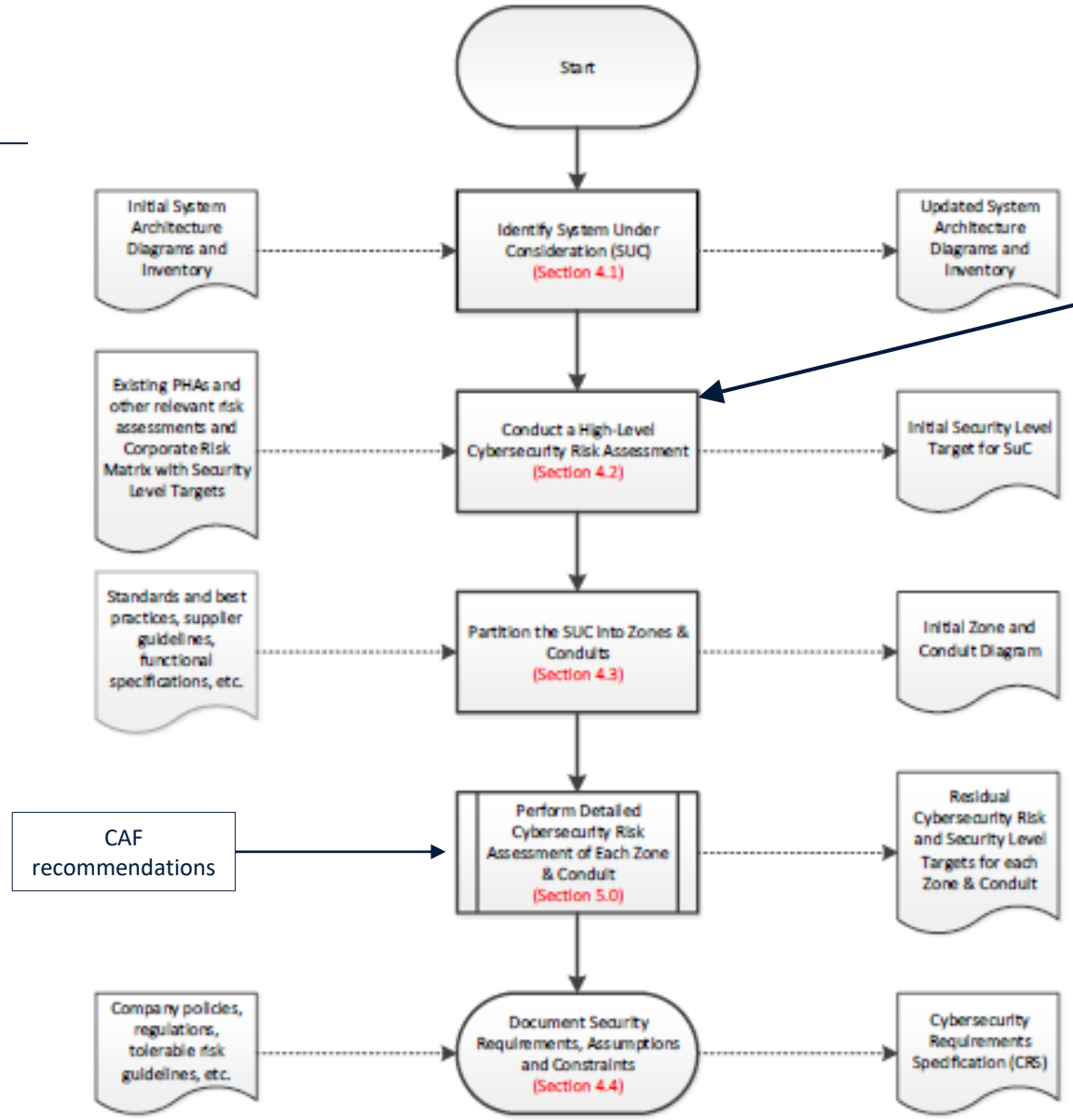
- Cost (resource and/or service/equipment)
  - Low: <1 week OR <£20k
  - Med: 1 week to 1 month OR £20k
  - High: >1 week OR >£100k

- Benefit
  - **Low:** Minimal improvement defend / detect / respond capability
  - **Med:** Some improvement defend / detect / respond capability
  - **High:** Significant improvement defend / detect / respond capability
  - **"Quick wins":** Low cost & High benefit



IEC-62443 RISK ASSESSMENT PROCESS

1. CAF
2. **High Level Risk Assessment**
3. Zone & Conduit Analysis
4. Detailed Risk Assessment
5. Cyber Security Improvement Plan
6. Cyber Security Management Plan



See Figure 1 in
IEC 62443-3-2 2015

1. **Terms of Reference** for HLRA: CF00-32-AC-103-00004 "Terms of Reference, Cygnus Cyber Security High-level Risk Assessment"
2. The System under Consideration (SuC)
3. The corporate risk matrix

SuC:

"The industrial control systems located on the Cygnus platforms, including the associated networks, up to and including the Cygnus boundary firewall."

No 'back office' or other IT-related systems on the Cygnus platforms were considered as part of the SuC.

RISK ASSESSMENT MATRIX

SEVERITY	CONSEQUENCE						LIKELIHOOD				
	People	Environment	Assets / Financial			Reputation / CSR	A	B	C	D	E
			Business Interuption & Business value lost	Production Loss	Material Damage/ Cost Impact		UNLIKELY	POSSIBLE	SOMETIMES	REGULARLY	OFTEN
							Never heard of in E&P industry	Heard of in E&P industry	Incident has occured in NE	Happens several times per year in NE	Happens several times per year in the Asset
5	Catastrophic health effect / Multiple Fatalities or multiple PTDs	Sensitive Environment Can be restored to a satisfactory / agreed state in period of YEAR(S)	>6 months	> 500 kboe (>3000 mmscf)	Catastrophic Damage >10M USD	International Public Attention - International Press and TV	High Risk		Intolerable Risk		
4	Major health effect / PTD or Fatality or Multiple LTI with PPD	Sensitive Environment Can be restored to an equivalent capability in a period of MONTHS	1 - 6 months	200 to 500 kboe (1200 to 3000 mmscf)	Major Damage 1M - 10M USD	National public concern - National Press and TV - International echoes					
3	Serious health effect / injury (LTI with PPD/Multiple LTI)	Sensitive Environment Can be restored to an equivalent capability in period of WEEKS	2 weeks - 1 month	50 to 200 kboe (300 to 1200 mmscf)	Serious Damage <1000k USD	Regional public concern - Regional Press and TV - National echoes	Medium Risk				
2	Moderate health effect / injury (Single LTI without PPD)	Non-sensitive Environment Can be restored to an equivalent capability in period of WEEK(S)	1 - 14 days	10 to 50 kboe (60 to 300mmscf)	Moderate Damage <500k USD	Local Public concern - Local Press - Regional echoes					
1	Minor Health effect / injury (first aid/MTC)	Non-sensitive Environment Can be restored to an equivalent capability in period of DAYS	<1 day	<10kboe (<60mmscf)	Minor Damage <50k USD	No public concern - Local echoes	Low Risk				

HIGH LEVEL RISK ASSESSMENT - PROCESS

NEPTUNE ENERGY

For each sub-system:

1) **Allocate to one of the following equipment classes**:
   - BPCS (Basic Process Control System)
   - SIS (Safety Instrumented System)
   - Other control equipment
   - Network equipment
2) Consider the two scenarios of:
   - **Total Loss** of sub-systems functionality
   - **Partial Loss** (I.e. compromise) of the sub-system's functionality
3) For each scenario assess:
   - The <u>most likely</u>, dominant **consequence** and its **likelihood**.
   - Use risk matrix to identify **<u>unmitigated</u>** risk the sub-system presents to the organisation.
   - Identify risk ranking driver: **Safety**, **Environmental**, **Financial** or **Reputational** consequences

Sub-systems:

(derived from the asset inventory)

1) Sub-system A i.e. ICSS - Safety System
2) Sub-system B i.e. Instrument Air Compressor UCP
3) Sub-system C
4) Sub-system D

HIGH LEVEL RISK ASSESSMENT - OUTPUTS

- Attendance register
- The risk assessment worksheet for each sub-system within System under Consideration:
    1. The failure mode (partial or complete loss of the sub-system)
    2. Consequence rating 1 to 5
    3. The most significant consequence category (safety, financial, environmental, etc.)
    4. Likelihood rating A to E
    5. The risk ranking Low, Medium, High or Intolerable Risk
- A register outstanding questions, assumptions or other observations
- Assessment study close out report

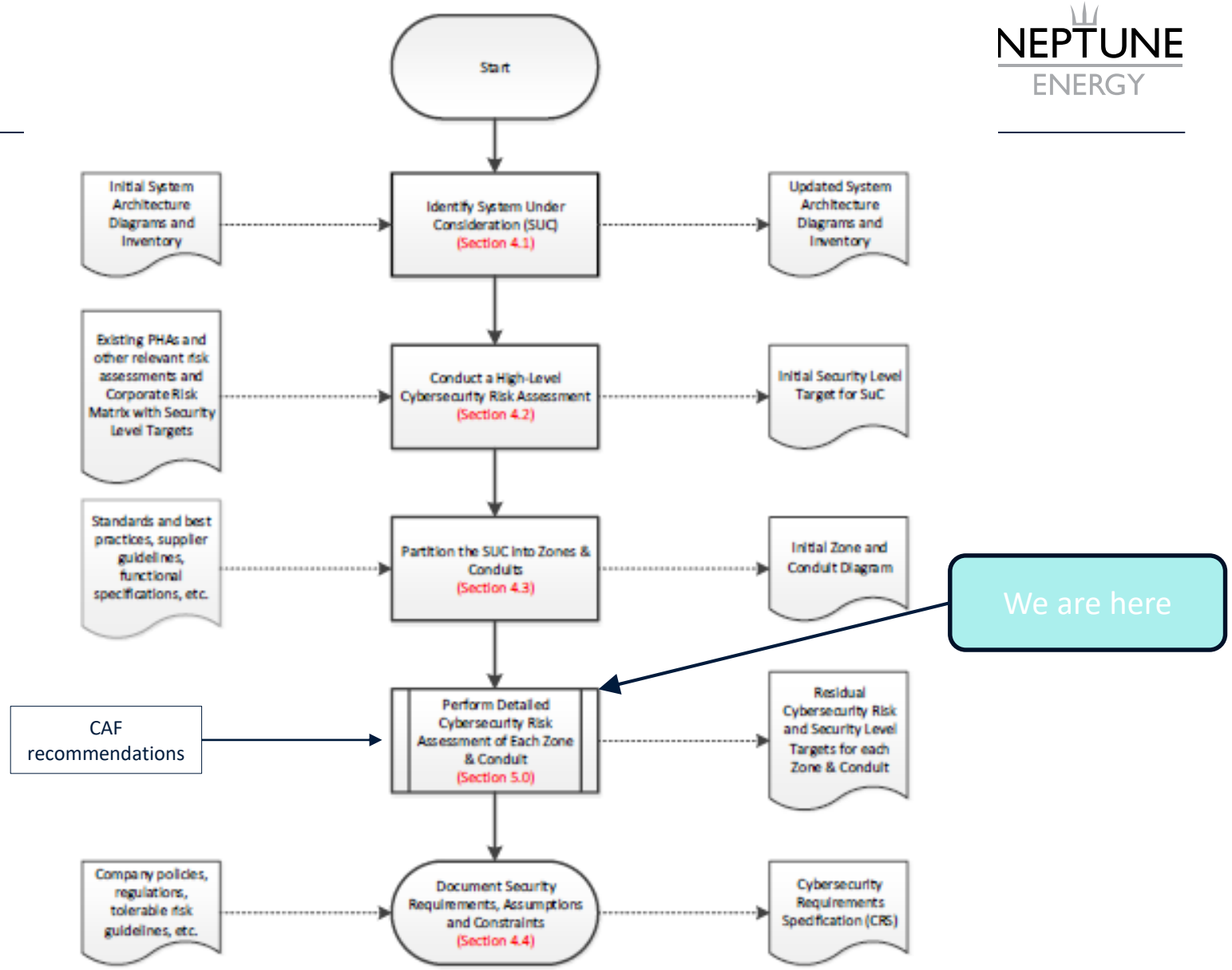
Study conclusion:

Following sub-systems are 'high risk' and shall be put forward for detailed risk assessment:

1) Sub-system A i.e. ICSS - Safety System
2) Sub-system B i.e. Instrument Air Compressor UCP
3) Sub-system C
4) Sub-system D

IEC-62443 RISK ASSESSMENT PROCESS

1. CAF
2. High Level Risk Assessment
3. **Zone & Conduit Analysis**
4. **Detailed Risk Assessment**
5. Cyber Security Improvement Plan
6. Cyber Security Management Plan



See Figure 1 in
IEC 62443-3-2 2015

1. **Terms of Reference** for DRA: CF00-32-AC-103-00005 "Terms of Reference, Cygnus Cyber Security Detailed Risk Assessment"
2. The System under Consideration (SuC)
3. The corporate risk matrix

SuC:

"The industrial control systems located on the Cygnus platforms, including the associated networks, up to and including the Cygnus boundary firewall."

No 'back office' or other IT-related systems on the Cygnus platforms were considered as part of the SuC.

RISK ASSESSMENT MATRIX

SEVERITY	CONSEQUENCE						LIKELIHOOD				
	People	Environment	Assets / Financial			Reputation / CSR	A	B	C	D	E
			Business Interuption & Business value lost	Production Loss	Material Damage/ Cost Impact		UNLIKELY	POSSIBLE	SOMETIMES	REGULARLY	OFTEN
							Never heard of in E&P industry	Heard of in E&P industry	Incident has occured in NE	Happens several times per year in NE	Happens several times per year in the Asset
5	Catastrophic health effect / Multiple Fatalities or multiple PTDs	Sensitive Environment Can be restored to a satisfactory / agreed state in period of YEAR(S)	>6 months	> 500 kboe (>3000 mmscf)	Catastrophic Damage >10M USD	International Public Attention - International Press and TV	High Risk		Intolerable Risk		
4	Major health effect / PTD or Fatality or Multiple LTI with PPD	Sensitive Environment Can be restored to an equivalent capability in a period of MONTHS	1 - 6 months	200 to 500 kboe (1200 to 3000 mmscf)	Major Damage 1M - 10M USD	National public concern - National Press and TV - International echoes					
3	Serious health effect / injury (LTI with PPD/Multiple LTI)	Sensitive Environment Can be restored to an equivalent capability in period of WEEKS	2 weeks - 1 month	50 to 200 kboe (300 to 1200 mmscf)	Serious Damage <1000k USD	Regional public concern - Regional Press and TV - National echoes	Medium Risk				
2	Moderate health effect / injury (Single LTI without PPD)	Non-sensitive Environment Can be restored to an equivalent capability in period of WEEK(S)	1 - 14 days	10 to 50 kboe (60 to 300mmscf)	Moderate Damage <500k USD	Local Public concern - Local Press - Regional echoes					
1	Minor Health effect / injury (first aid/MTC)	Non-sensitive Environment Can be restored to an equivalent capability in period of DAYS	<1 day	<10kboe (<60mmscf)	Minor Damage <50k USD	No public concern - Local echoes	Low Risk				

DETAILED RISK ASSESSMENT - PROCESS

Zones under Consideration:

(Derived from 'High Risks Systems' from HLRA)

1) Sub-system A i.e. ICSS - Safety System
2) Sub-system B i.e. Instrument Air Compressor UCP
3) Sub-system C
4) Sub-system D

For each ZuC:

- Identify potential threat scenarios including threat source, action and vulnerabilities.
- Review threat scenarios and use risk matrix to identify: Consequences, likelihood and the unmitigated risk the threat scenario presents to the organisation – Ref HLRA to assist progress & consistency

- Determine the CRRF and the Security Level Target, SL-T. See the diagram below.
- Consider existing countermeasures for each threat scenario identified and use risk matrix to re-evaluate the residual cyber security risk.
- Evaluate the residual risk and consider additional countermeasures if still above the tolerable risk level.

DETAILED RISK ASSESSMENT - OUTPUTS

- Attendance register
- The risk assessment worksheet for each ZuC:
    1. The name of the ZuC
    2. The threat scenarios
    3. Most significant consequence (safety, environmental, financial, reputation)
    4. Impact rating for most significant consequence 1 to 5
    5. Likelihood rating 1 to 5
    6. Risk rating 1 to 25
    7. Security Level Target, SL-T
    8. Existing countermeasures
    9. Recommendations to reduce assessed risk to a tolerable level
    10. Residual risk
- A register of any outstanding questions, assumptions or other observations
- Assessment study close out report.

Study conclusion:

Most Significant risks in ZuC

- **Assessed Mitigated Risk**
- **Above or Below tolerable risk?**
- **List of additional mitigating defence measures**

NEPTUNE ENERGY

3

IT Learnings from the CAF Process

WHAT DID I LEARN FROM GOING THOUGH THE CAF PROCESS

RIGS ARE COMPLEX, CAF TAKES TIME, YOU NEED SOMEONE WITH EXPERIENCE

NEPTUNE ENERGY

About the Rig

- Lots of ancillary systems need to be considered
- It's not the obvious systems that are the most “at risk”
- Nothing is isolated (anymore)

About the Process

- Get someone who has done it before
- Need the guys who know to participate
- Present the results at management level AND technical level

Going Global…

- Neptune approaches the issue of cyber security differently in each country.
- Building relationships between the teams is hugely important.
- Need the buy-in from senior management.

WHAT DID I LEARN FROM GOING THOUGH THE CAF PROCESS

RIGS ARE COMPLEX, CAF TAKES TIME, YOU NEED SOMEONE WITH EXPERIENCE

NEPTUNE ENERGY

About the Rig

- Neptune approaches the issue of cyber security differently in each country.
- Building relationships between the teams is hugely important.
- Get someone who has done it before

About the Process

- Get someone who has done it before
- Need the guys who know to participate
- Present the results at management level AND technical level

Going Global…

- Neptune approaches the issue of cyber security differently in each country.
- Building relationships between the teams is hugely important.
- Need the buy-in from senior management.

WHAT DID I LEARN FROM GOING THROUGH THE CAF PROCESS

RIGS ARE COMPLEX, CAF TAKES TIME, YOU NEED SOMEONE WITH EXPERIENCE

NEPTUNE ENERGY

About the Rig

- Neptune approaches the issue of cyber security differently in each country.
- Building relationships between the teams is hugely important.
- Get someone who has done it before

About the Process

- Get someone who has done it before
- Need the guys who know to participate
- Present the results at management level AND technical level

Going Global…

- Neptune approaches the issue of cyber security differently in each country.
- Building relationships between the teams is hugely important.
- Need the buy-in from senior management.

QUESTIONS AND ANSWERS