SSE - SHET New Transmission Resilience Operation Center Proposal Review Project

Response to Ofgem RIIO ET2 Submission

Final Report, August 12th 2020

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organizations, under contract to the Electric Power Research Institute (EPRI), prepared this report:

EPRI Europe

Principal Investigator
A. Kelly

Together...Shaping the Future of Electricity®

Electric Power Research Institute

3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA

800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

This publication is a corporate document that should be cited in the literature in the following manner:

SSE - SHET New Transmission Resilience Operation Center Proposal Review Project: Response to Ofgem RIIO ET2 Submission. EPRI, Palo Alto, CA: 2020.

EXECUTIVE SUMMARY

In 2020, SSEN submitted a proposal to Ofgem for a new resilience operations center, as part of the RIIO-ET2 process for transmission price control for the period 2021-2026. The proposal was rejected by Ofgem in a draft determination in July 2020, on the basis of a lack of justification of need for the new control center and the proposed solution being disproportionate to the needs identified. EPRI were engaged to assess both the needs and the proportionality of the proposed solution, based on knowledge and experience in the transmission operations industry and with a view to the needs of the control center of the future.

Resilience of both the power system and their control centers refers to the ability to prepare for, operate through and recover from worst-case scenario events. Resilient control center infrastructure is a critical function of transmission operators and transmission owners to ensure that a reliable and continuous electricity supply is maintained to customers. Increasing resilience usually involves investment in infrastructure ahead of time, striking the right cost / benefit and risk balance. It is also essential to plan and continuously train for major events that encompasses all aspects of system operation. This means, not just system monitoring and control, but also operations planning and support teams, so that they can maintain reliability during major incidents. The experience and knowledge of all staff, to operate through and recover from major incidents, is also a key component of a resilient control center.

With resilience in mind, an assessment of the current control center needs, based on specific license and STCP code requirements, was carried out. This needs assessment identified the gaps between effective and optimal operation and the current capabilities. 43 issues were identified, grouped by safety of personnel, system security and cost. The most onerous issues with the current control center were lack of situational awareness overviews, lack of space for coordination and planning, risk of human error due to distraction and inadequate facilities to respond to a major system disturbance.

Following the current needs assessment, an assessment of the potential future system was carried out. 23 possible new technologies or innovations loosely grouped into categories of *new network and technology, interoperability* and *Improved Technology for Monitoring and Control* were identified. All 23 will be incorporated partly or fully into the transmission network of the future in Scotland. All will have to be monitored, controlled, or incorporated into operations-as-usual in the coming years in the SHET control center. As part of the assessment, the future needs based on the current STCP codes were detailed in consultation with SHET engineers. A total of 38 likely needs for the control center to carry out the required STCP tasks in future were identified, and were also grouped by personnel safety, system security and cost.

As well as the issues with the current system and the potential issues with the future system, the risks and threats associated with the “do-nothing” option are also documented in this report. In total, 42 potential risks were identified with continued operation in the current control center. These were grouped by safety, system security and cost.

The 43 issues with the current system, 23 future technologies, 38 future needs and 42 risks associated with “do nothing” can be considered when assessing the need for the new resilience control center.

Quantifiable value of a new facility and reciprocal costs of the “do nothing” option are difficult to define. However, de-risking the system operation facility by upgrading to a new resilience facility, should automatically increase the resilience of the transmission system. Operators will have vastly improved situational awareness and training and the response to emergency events on the system can be clearly planned, trained for, controlled and monitored efficiently. This should increase system operator efficiencies with a consequent increase in system reliability, and reduction in human error. This will untimely benefit the electricity consumer in Great Britain, in the long run.

Situational awareness is the most important aspect of day to day transmission system operation. Control centers are always designed to optimize and maximize situational awareness. For systems with wide spans of control, a large video wall display with the transmission network and key system indicators and trends and alarms is used by the vast majority of system operators around the world. A large Tier 1 display overview of the system improves the operator’s perception, comprehension and orientation of the system. This will be increasingly important in future as the system gets more complex, especially during major system disturbances.

One of the main risks and issues with the current system identified was associated with disruption, distraction and interruption. The level of distraction and interruption, caused by people throughflow near the control desks, may result in human error. Switching and safety coordination are key tasks with lives dependent on concentration and error-free operation. The optimal way to mitigate this is by creating a “no interruption zone” – a dedicated room segregated from normal workers that allows operators to perform safety coordination without distraction. This is not possible in the current facility in Inveralmond House and is an area of potential improvement in resilience in a new facility.

Situational awareness, reduction of human error, are all associated with the highest standards of training. Training for unanticipated events such as blackstart and restoration scenarios can only be carried out with a simulator environment. Most system operators have a training simulator co-located with the control center. This is to streamline on-the-job training for anticipated scenarios and to provide for an efficient training and certification programme.

In the likely future there is likely to be an increase in high impact low frequency events. Control centers must have adequate training facilities to plan and prepare for these events in advance. They must also have optimized situational awareness tools and wide area views of the system to perform the role of system operator. In addition, adequate comfort facilities to cater for operators who are sequestered for long periods working on restoration are important. An optimally designed new resilience operations center should provide for these three important aspects to ensure supply is restored to all customers as quickly as possible after a blackout, given the likely monetary and socio economic costs of any delays to restoration.

Cyber and physical threats are required to be mitigated by SSEN. At present the SHET control center should be categorised as a Critical National Infrastructure (CNI) site by the Centre for the Protection of the National Infrastructure (CPNI). CPNI standards for physical security protections should necessitate physical security upgrades at the facility. SSE has developed a set of Cyber Security Standards that align to the industry best practice NIST (National Institute of Standards and Technology) framework. This is widely acknowledged as the preferred framework for protecting Critical National Infrastructure (CNI).

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
DOCUMENTATION REVIEW

Introduction to Report and Process

In late 2019, Scottish Hydro Electricity Transmission (SHET) made a submission to Ofgem as part of the RIIO-ET2 (Revenue = Incentives+Innovation+Outputs Electric Transmission 2). The submission was for allowed revenue for the subsequent 5 year (2021-2026) period. A total of 49 Engineering Justification Plans (EJPs) were submitted to Ofgem as part of the RIIO-ET2 business plan submission, including the EJP for the proposed new resilience transmission control center - *Engineering Justification Paper - Resilience Operations Centre Engineering Justification Paper T2BP-EJP-0003* [1]. The aim of the EJP was to develop the needs and justification for a new control center. In advance of the EJP development, SHET conducted a stakeholder workshop, documented in: *SHE Transmission Operations Stakeholder Workshop* [2] where stakeholders, when polled on options, opted for the "Responsible Operator" option for the design and build of one new control center.

The SHET EJPs were reviewed by Atkins/SNC Lavalin, on behalf of Ofgem, and a report (*RIIO-T2 TO Submission Review Summary Report*) [3] was developed and released publicly in July 2020 as part of the package of technical annexes to the draft determination report.

Draft Determination for Operations Resilience Center

Ofgem responded with a draft determination in July 2020, the document: *Consultation RIIO-2 Draft Determinations – Scottish Hydro Electric Transmission* [4] details the rationale for the rejection and the decision-making process behind the determination. This is a draft determination and is given to allow SHET to respond to the issues highlighted in more detail, before a final determination is released at the end of 2020.

In the draft determination report, of particular interest for this report, Table 24 on the proposed allowances for SHET's property costs within the non-operational capex section, detail the proposed spend and response.

The proposal for a new resilience operations center was not granted funding in the draft determination, with the rationale:

> *"In our view, SHET has not provided sufficient justification for the preferred option of a new control room and associated building. The corresponding EJP does not provide a clear and unambiguous needs case or demonstrate value for money or efficiency."*

The assessment approach is included in Chapter 3 of an associated report *RIIO-2 Draft Determinations - Electricity Transmission Annex* [5], completed by Atkins/SNC Lavalin. For the property elements of the non-operational capex framework, in which the proposed new control center was allocated the following, more detailed justification for the rejection was given:

"For both Property and STEPM costs, we examined the historical run-rates for spend over the RIIO-ET1 period and performed ratio analysis against Modern Equivalent Asset Value (MEAV) and capex to establish baseline requirements. This was supplemented by a review of specific non-operational property funding requests where these were separately presented by the TOs within their EJPs."

Chapter 3 of the Atkins/SNC Lavalin report details the analysis of each SHET EJP, categorizing them by Load Cost, or a Non-Load Cost and giving each a risk classification coloured by Green, Amber or Red.

Observations and comments about each the EJPs are detailed in Appendix A of the Atkins/SNC Lavalin Submission Review Summary Report [3]. SHET confirmed that no supplementary questions were asked or answered as part of the Resilience Operations Center EJP review process. The notes and risk assessment were compiled by the Atkins/SNC Lavalin authors and submitted to Ofgem.

The Resilience Operations Center (EJP-003) was classified as **a red risk** by Atkins/SNC Lavalin. A red risk is classified in the report as meeting one or more of the risks identified in Table 1-1.

Table 1-1 Risk assessment criteria associated with a red risk judgement

Risk 1	There is a high risk that most of the investment (>50% of the total value of the paper) will not be required in RIIO-T2 period
Risk 2	Needs case is not clear
Risk 3	Significant delay is likely
Risk 4	Solution is significantly disproportionate to the needs case
Risk 5	Scope has significantly expanded beyond the requirements
Risk 6	Significant uncertainty in the scope of work

The risk assessment methodology is further detailed in Appendix D of the Atkins/SNC Lavalin Submission Review Summary Report [3]. The EJPs were scored 1 or 0 depending on whether they did or did not meet the criteria listed in Table 1-2. The EJP for the Resilience Operations Center failed to meet four of the five criteria, only passing on the completed documentation criteria.

Table 1-2 Criteria assessment used by Atkins/SNC-Lavalin in the development of the decision on the resilience operations control center.

Criteria Number	EJP Criteria Assessment	Description	Operations Center (EJP-003) Score Determination in Report
Criteria 1	Paper complete with	That the licensee has followed the suggested format and guidance of what each EJP should contain as requested by Ofgem for the specific	1

	all references available	EJP being assessed, and that all other referenced documents within the EJP are available. Please note that EJPs have only been marked down where missing documents/references are considered to materially detract from the robustness of the submission.	
Criteria 2	Clear and unambiguous needs case identified	That a clear and unambiguous needs case has been presented for the investment. This could be provided through evidence such as: asset condition data; boundary power flow assessment; references to the outputs of other assessment methodologies	0
Criteria 3	Validity of the options considered	That the options being considered and taken forward in the optioneering assessment are reasonable for the needs case identified, and that the reasons given for the rejection of options are acceptable and there are no clear options omitted from the assessment.	0
Criteria 4	Chosen solution proportionate to the needs case	That the chosen/preferred option is a proportionate solution to the identified needs case and that the scope of the solution has not expanded into something far wider with little or no justification	0
Criteria 5	Value for money and efficiency	That the licensee has demonstrated value for money for their chosen/preferred solution. This could be demonstrated via a CBA which should be broad enough in scale for the size of the proposal. Options which re-utilise existing assets or amalgamate works where possible will be viewed favourably. Scope and cost risks are identified in these criteria but do not affect the criteria score unless considered material. An individual assessment summary sheet was produced for each EJP to give a detailed narrative of Atkins assessment on whether that EJP was adequate with respect to the above criteria. SQs were raised to seek clarification on any areas where there was a lack of evidence or clarity in the submission to ensure that there was no ambiguity in the assessment.	0
		Total	**1/5**

Further comments were added in relation to the EJP in the Atkins/SNC Lavalin review report in bullet point format in *Table 3-5 Issues for SHET*. These are summarised in Table 1-3 below, with two additional columns on the right, added by EPRI which attempt to link each of the comments (reasons for rejection) in the review, with the likely risk (from Table 1-1) and the likely criteria (from Table 1-2) associated with each comment. This is a subjective assessment of the issues, given by EPRI.

Table 1-3 Comment log as detailed in the Atkins/SNC Lavalin EJP review report [3]. The two columns on the right link the comments with the likely risk and pass/fail criteria documented above.

Atkins Report Issue Number	Comment	EPRI Assessed Risks Associated with Risk Register Judgement	EPRI EJP Assessment Criteria Judgement
Issue 1	The chosen solution is not proportionate to the needs case. The scope of work as presented (regarding the new building rather than the expansion of the existing facility) is not well justified.	Risk 2, Risk 4	Criteria 2
Issue 2	The EJP proposes the development of an independent and new control room building to accommodate the resource requirements and improve access control. SHET state the additional requirements, namely the need for control desks and support team desks by the end of RIIO-T2, compared to control room desks and support team desks currently. However, the majority of the paper cost is associated with establishing a new building not the control room fit out.	Risk 2	Criteria 2
Issue 3	Furthermore, in establishing the need SHET do not establish how much space the control room needs, and although SHET have considered expanding the current facility, the arguments against an expanded control room in the current facility are weak and are not sufficient for the dismissal of this option. It is also not clear how the issues surrounding tailgating could not be mitigated at the existing site.	Risk 5	Criteria 4
Discussion Issue 4	The primary investment driver for several of the EJPs submitted by SHET was resilience. Most of these documents made a weak case for these projects to be funded as part of RIIO-T2, having presented a needs case based on improvements rather than asset condition	Risk 1, Risk 2	Criteria 5

	There is a high risk that T2BP-EJP-0003 will not be required in the RIIO-T2 period, as they have not presented enough information to justify the proposed scope of works.		
Discussion Issue 5	The options considered in the optioneering assessment were reasonable for the needs case identified, with the majority of EJPs scoring favourably in this area. However, the chosen / preferred option was often not deemed a proportionate solution to the identified needs case, and the majority of schemes did not demonstrate value for money.	Risk 4	Criteria 4

Summary

The SHET proposal to Ofgem as part of the RIIO ET2 submission for a new Resilience Operations Center was rejected following an analysis of the EJP. Following a review, and parsing the information from the review documents, the proposed resilience operations center project was most likely rejected primarily due to:

- **A lack of justification of needs**
- **The proposed solution being disproportionate to the needs identified.**

For the next draft submittal, these points will need to be addressed in detail, with clear needs identified and a justification for the proposed solution of a new Resilience Operations Center.

It is proposed to address the issues in detail in this report, with reference to internal and external and documentation and internationally recognised standards and documentation and international best practices or other experience.

2 THE NEED FOR A NEW RESILIENCE OPERATIONS CENTER

To address the comments and issues from the evaluation of the EJP [3] as discussed in Chapter 1 and to improve the business case and engineering justification, the following questions need to be answered with evidence-based elaboration, where possible:

- What are the current control center needs?
- What are the needs for the future control center to manage the system of the future?
- Why is the current solution, the current control center, not fit-for-purpose?
- What are the risks with maintaining operations from the current control center?
- What value will the new control center bring to the customers and stakeholders?
- What are examples of other control centers for similarly sized transmission owner/operators?

These questions will be addressed in Chapters 2 and 3. **One of the key components to when discussing a new Resilience Operations Center is to define reliability and resilience** – two key concepts in power system operations and control. These will be referred to frequently in the remainder of the report.

Reliability

Reliability, in the context of transmission system operation, refers to the probability that a power system can perform a required function under given conditions over a given time interval. Reliability quantifies the ability of an electric power system to supply adequate electricity on a nearly continuous basis with few interruptions over an extended period of time. It is the overall objective in power system planning and operations, to ensure the system is operational for the loss of any element. It can be monitored and measured in real time.

Effective reliability management ensures the probability of acceptable operation is very high and the system is prepared to withstand selected highly-probable events such as the loss of lines, generation or load.

Resilience

Resilience is a harder concept to define and there is no standard approach or measures (unlike the N-1 criterion for reliability). It is directly related to reliability in that the system cannot be resilient if it is not reliable and it cannot be reliable if it is not resilient. Essentially resilience means that the system is prepared to *fail gracefully and recover under selected worst-case events.* Effective resilience management ensures that the impact of unacceptable operation (for example from a reliability breakdown) will be low [6]. The concept of resilience encompasses:

- Preparing for
- Operating through and
- Recovering from

very significant disruptions to the system, regardless of the cause [7]. Systems with complex threats, that might evolve quickly, such as storms on the power system must designed to be resilient.

Resilient Power Systems and Control Centers

The concept of resilience does not just apply to power systems and can apply to all aspects of transmission system operation, including control centers, IT and EMS infrastructure, staff management etc. Due to its criticality, control centers must be able to deal with very serious threats to buildings and facilities, IT, EMS and SCADA application, and staff. While there is no set standard or metric for resilience, increasing resilience usually involves:

- Investment in infrastructure ahead of time, striking the right cost / benefit and risk assessment balance.
- Detailed planning for major events that encompasses all aspects of system operation, not just system control and monitoring, but also operations planning and support teams, facilities, IT, management, communications.
- Continuous training of staff on the plans, so that they can maintain reliability during major incidents.
- Experience and knowledge of all involved staff to operate through and recover from major incidents.

Grid operators like SHET can anticipate and prepare for certain well defined threats, but cannot possibly foresee every threat, risk and impact. This is true now and will be true in the next decade, as the GB system becomes more interconnected and different threats emerge. **That is why the grid must not only be reliable - but also resilient.**

Having resilient control center infrastructure and plans in place is a critical function of transmission system operators and owners to ensure a reliable control center and continuous supply to customers.

EJP Current Control Center Needs

The question of needs was a key area of focus of the EJP evaluation and the business plan submittal. It seemed that part of the reason the proposal was rejected was that a sufficiently convincing case was not made to justify the need for a new facility. From the EJP, in the needs section EJP, the following six needs were documented and identified:

1. Physical Security
2. Blackstart Re-Powering
3. Dynamic Network Growth
4. System monitoring
5. Business Separation
6. Contingency

Each of these will be addressed in the report with other additions to add more details where necessary.

Legislative / Regulatory Obligations of SHET Control Center

SHET's operating license is issued by Ofgem [8], specifically Section D on the transmission owner standard conditions. It clearly states that the Transmission Owner (TOs) provide services in accordance with the System Operator Transmission Owner Codes (STC).

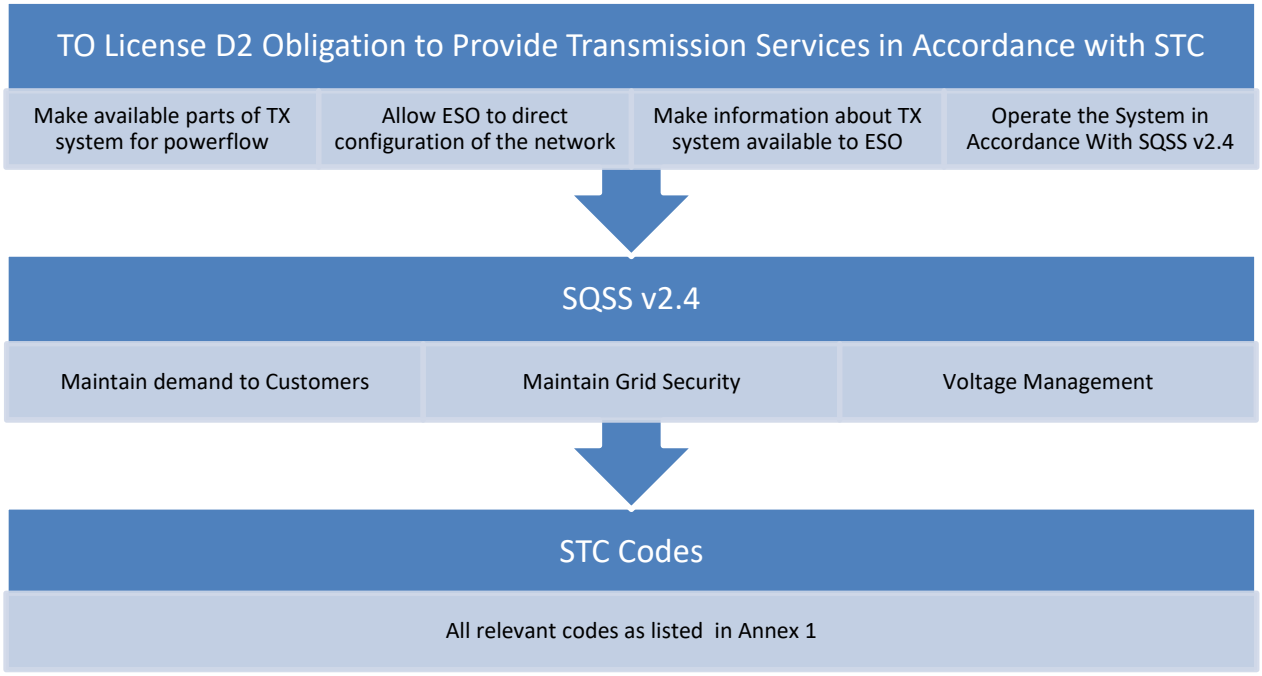

Figure 2-1 Graphic illustration of document and information flow and structure for SHET when owning and operating the transmission system

Key Needs and Indicators of Success for a TO Control Center

SHET developed a list of what it considers the key needs for the control center, to operate the transmission system in accordance with the license, standards and codes as detailed in Figure 2-1.

The performance of the control center is critical for the success in maintaining a safe, secure, reliable, resilient supply to all customers and stakeholders. The key needs and the key performance indicators are summarized in Table 2-1 below.

Table 2-1 Summary table of key operational needs for the SHET control center and associated KPI or output

Key Need for Operational Control Center	Key Performance Indicators / Output
Keeping ENS to a minimum in each event – requires high degree of awareness and capability	ENS allowance 102MWhrs (was 120MWHrs)

ESO liaison – meet the expectation of the ESO with increased operational complexity	As per STCP codes
Exceptional service expectations by stakeholders, with a no FAIL belief. Minimal interruptions and fast as possible restorations	No failures, rapid restoration (dependent on failure)
Physically secure substations and control centers	No security breaches
Boundary flow management with likely increases in coming years due to added connections and other parameters.	Managed boundary flows as per SQSS at all times
Compliance and increased contribution from SHET for MVAr support which is operated by TCC.	300MVAr of equipment at least, plus other services, no failures, optimal voltage control.
Enhanced transparency by increased TCC capabilities in information management and service provision	High degrees of transparency
Preparedness for change to future blackstart strategy – higher degree of communication and awareness	Practiced in restoration to meet target of 60% demand back in 24hrs and 100% in 72hrs.
Need to facilitate innovation	Embrace new technology by providing space to work with developers, house and familiarize our team by parallel running, before live implementation.
Training facility - Having people to do the job - Lead times to prepare our teams for future operations	Training times for our team members require 6 – 12mths to achieve a first level authorisation. Senior roles require 2 – 3yrs on top of this. Refresh training and offline rehearsal of new methods in a safe environment offline

Once the key operational needs (some of which will have discrete KPI / Outputs values for tracking) are established, the next step in the process is to establish the normal tasks and duties of the SHET operators in the control center.

A summary of the roles and obligations are laid out in the STCP codes was developed by SHET and expanded upon by EPRI and are collated in Annex 1. The table in Annex 1 also assesses the consequences of failure, for any particular need or obligation and a rating for how critical the task is to overall system operation in the SHET control center.

Summary of the Issues with Current Control Room in Inveralmond House

Below is a summary of the most important issues with the current control center when operators are carrying out the tasks associated with STCP codes.

Safety and Security Issues

Field Staff Safety

1. Distractions, disruptions and increased stress often occur as people traverse along the accessways next to them.
2. Safety coordination needs are increasing in volume as there are more interfaces with offshore, new users and interconnector builds.
3. There is a lack of space to coordinate safety activities with other team members
4. Working on the live system and following instructions from the control engineers, there is higher risk of operation switching errors.
5. Malicious switching can be carried out with inadequate security.

Control Room Operations Staff Safety

6. The NCI requirements for Inveralmond are lacking due to the open nature of the site, building and floor area. A secure perimeter is needed for blackstart/restoration scenarios. There is no secure area outside of the building to protect staff or equipment.
7. No nominated area for a transmission incident room close to the control room exists.
8. For a storm or major incident that also involves SHEPD, one shared room is not enough to manage the incident. It would be unsuitable as SHEPD are likely to use it. It also is not large enough for an effective s*ilver* command room.
9. For the backup facility at Buroughmuir, the same grid supply point is used for both locations, which has potential redundancy issues.

System Security Issues

Displays and Overviews

10. Inadequate system overview due to the lack of space and positions of the desks means reduced situational awareness and lack of visibility of key information.
11. Lack of overviews limits wide area view of the system and alarm screens if a test goes wrong.
12. Critical alarms are not displayed on wall overview displays, only on small monitors. No room to add alarms because of capacity limits.
13. Engineers have to search or interpret alarms before seeing the full picture and may alarms not be seen, unless the operators are viewing the correct screens constantly.
14. Small additional screens have been added to assist the engineers, but this obscures some other information.
15. No room to display datalink status on overviews, difficult to monitor the status of datalink.

16. Active Network Management - The optimal way to monitor is to have a status indication or alarms visible on an overview for one look awareness of the status. The lack of overview screens makes this difficult.
17. Adding performance monitoring equipment to monitor the system will, by necessity, increase the screens and overviews needed to view visualizations and / or status of the monitoring equipment. This is not possible given lack of display capability

Desk Space

18. Desk space is limited, giving a small footprint for the operators to use as workspace and inability to install new facilities such as more advanced telephone management systems.
19. Collaboration space is limited. Team discussions are difficult in relation to disturbances.
20. Limited number of restoration desks limits the pace at which SHET can restore the system.
21. The open office has no option for creating a suitable communication hub during events.
22. During a major event, a silver command room would be set up elsewhere in the building but a significant advantage of keeping the TCC teams close would limit communications effectiveness.
23. Lack of capacity and space for protection, operational, user or commissioning testing, relies on using existing monitoring screens for testing while also monitoring the system.
24. For outage planning coordination - dislocation reduces communication and ideas sharing between the year ahead team and the current year team and the manager's awareness is reduced for half of the group.
25. This dislocation can result in miscoordination and suboptimal planning of outages and creates barriers to general awareness of activities within the team.

Data Management and System Monitoring

26. Some systems such as the disturbance recorder servers are not housed at the control center and do not have the 24 hour support that a control center would be able to offer.
27. Risk of mistakes in data preparation and management and data security is of concern.
28. Inefficiencies in data exchange methods may exist due to disperse nature of the group.
29. The data preparation, management and commissioning are carried out in the control room with open access by other staff on the floor.
30. Resources to keep asset nomenclature current have been lacking. Draft documents and publication are often behind on review.
31. No easily accessed centralised database for tracking information and updates

Training

32. For islanding scenarios: Staff are Ill-prepared due to lack of experience and relevant displays. It often relies on the island generation team to manage the island groups.
33. Re-synchronizing is often an issue due to lack of practice and inadequate displays. This results in a lack of situational awareness if island is desynchronized
34. Training is required on all of the ANM devices, given their complexity. New devices will likely be added requiring new training programs.
35. No integrated training facilities exist in the current facility. Classroom and simulator based training and coordination with other entities is non-existent.

Cost Issues

Desk Space

36. Space to house more equipment does not exist at IHP for future needs.
37. There is little or no capacity to increase the number of commissioning desks.
38. Additional staff needed for widespread event management would most likely be distant from the TCC team, with further reduced effectiveness.

Third Party Contractors

39. SHET rely on third party contractors to monitor comms datalinks.
40. SHET are susceptible to third party system providers availability at present.

Facilities

41. The shared facilities at IHP are not suitable for managing a blackstart, due to limitations in the space available to coordinate freely between the Incident Management Centre, Planning Team and Control rooms.
42. The joint kitchen has 2 small domestic fridges that serve all staff on the floor (160) with no room to expand without encroaching into office space, which is already limited.
43. Private space for confidential discussion is not available near the control room.

What the Future needs are for the new control center? - Identifying New Needs

To identify the needs for the SHET system of the future, it is necessary to consider both the current state and potential future state. The future control center can be assessed by using scenario planning, and the future control center needs can be identified with a gap analysis.

Figure 2-2 Graphic illustration of gap analysis

Control Center of the Future Initiative

In 2020, EPRI developed an initiative, entitled *The Control Center of the Future*. The initiative involved webcasts, workshops, surveys and the development of reports and tools that may be required in the control center of the future. Part of this initiative is detailing a framework for forecasting what the future grid or power system will look like, since the future is unknowable, and the power systems is evolving at an unprecedented rate. To plan for the uncertain future, the initiative aimed to focus utilities on the need for a joined up and strategic approach to:

- Data management and network model management
- Software tools including EMS, SCADA, synchrophasors and visualization
- Human performance innovation including training for the future system
- Buildings, ergonomics and hardware in the control center

All four are closely interlinked. Building and facility design are a key component of ensuring operators have an adequate toolkit to manage and operate the future control center.

In the context of Scotland and the Great Britain, the future energy scenario framework, as developed by National Grid Electricity System Operator for 2050 [9], is a useful way to analyse the potential future system operation scenarios. This sets out four possible energy scenarios that that the systems might track in the years and decades ahead. These four scenarios are:

1. Steady Progression (SP)
2. Consumer Transformation (CT)
3. System Transformation (ST)
4. Leading the Way (LW)

At least 40 GW of new capacity will be connected to the system in 10 years. This is approximately 80 % of system peak as of 2019 of additional capacity. Much of this will be offshore wind, much of which is based in Scotland.

	2019	2030			
Emissions		CT	ST	LW	SP
Annual average carbon intensity of electricity (g CO_2e/kWh)	167	41	66	-6	89
Electricity					
Annual demand (TWh)[9]	308	322	304	305	328
Peak demand (GW)[10]	59	67	59	61	62
Total installed capacity (GW)[11]	112	170	147	178	145
Low carbon and renewable capacity (GW)[12]	54	106	93	117	82
Interconnector capacity (GW)	5	19	18	22	16
Total storage capacity (GW)	4	13	7	16	6
Total vehicle-to-grid capacity (GW)[13]	0	2	0	3	0

Figure 2-3 Graphical illustration of the likely scenarios based on the FES for the UK system to 2030, showing wide variance in some operational scenarios, showing the uncertainty of the future system Source NGESO [9]

Looking at the scenarios for 2030 in Figure 2-3, the system that may be under control in 2030, as forecasted by NGESO, has a wide variance on key system parameters and metrics based on projections from the 2019 numbers. The type of system operator and control center that is required for the future system is dependent on the future energy scenario. These projections, and the inherent lack of certainty on exactly what type of system will be required in 2030 and beyond has a major knock-on impact on the transmission system owner / operators in GB, such as SHET.

If one looks out from 2020 to 2030, the transmission grid will, in all future energy scenarios, likely behave in a different way or be composed of different components. This is summarised in Table 2-2. All of the aspects covered in Table 2-2 will have to be considered, in some form for real time transmission system operations for SHET; some are not currently implemented or implemented in a limited fashion and some will not be relevant.

Table 2-2 Table of likely new areas of focus for 2030 grid and control center of the future.

Category	Short Description	Description	Relevant to SHET
	More Connections	Vastly increased renewable generation capacity primarily wind and solar	Yes
	Offshore Wind	Offshore wind will be a key aspect of the future Scottish grid.	Yes

New Network and Technology	Offshore grids	Increase in DC or hybrid AC / DC offshore grids integrating other systems or with large windfarms	Yes
	BESS	More battery energy storage devices and services	Yes
	New Markets	More integrated energy and system service markets.	Partly
	Self-Dispatch	Self-dispatch of generation based on availability and market signals	Partly
	HVDC	More HVDC interconnection to other systems or neighboring TO footprints.	Yes
	New Transmission	More HVAC interconnection to neighboring TO footprints.	Yes
	Active Network Devices	More flexible AC transmission devices (FACTS), more complex power electronic equipment and dynamic line rating.	Yes
	Demand Response	Demand response, active homes, smart metering and less predictable load patterns	Yes
	Weaker Grids	The transmission system will get progressively weaker due to increased renewables and the changing nature of the grid and lower inertia.	Yes
	Ramping	Faster ramping of generation and load resources	Partly
Interoperability	ESO Coordination	There will very likely be increased coordination with NGESO or equivalent in the future as the system becomes more flexible. New regulations, rules will likely be imposed.	Yes
	Coupling	Utility sector coupling including generation, renewables, gas, hydrogen, water, transport	Yes
	TSO/DSO	More TSO / DSO interactions in real time and the blurring of the operability boundary.	Yes
	Electrification	Increased electrification of sectors of society such as heat, agriculture, commercial, industrial load.	Yes
	E-mobility	Increase in E-mobility electricity for transport	Partly

Improved Technology for Monitoring and Control	Business Intelligence	Better use of business intelligence architecture for data analytics	Yes
	AI	Artificial intelligence, machine learning, reinforcement learning	Yes
	Cloud / Edge	Increased use of cloud computing technology and grid/edge devices.	Yes
	Substation Automation	Increased substation automation technology and intelligent electronic devices (IEDs)	Yes
	PMUs	Full observability and controllability using phasor monitoring units (PMUs)	Partly
	Asset Health	Advanced asset health monitoring systems and databases	Yes

Future Needs Gap Analysis

When analysing the current roles and functions of the SHET CR based on the STCP codes, both the inadequacies of the current solution (as documented above and included in totality in Annex 1) and the likely future needs of the control center, related to each STCP function were outlined. These are summarised below:

Safety and Security Issues

Field Staff Safety

1. An improved environment is needed to ensure operators can concentrate on safety activities. Increased commissioning of new equipment and substations will add to workload.
2. Increasing workload will bring increase in workforce on the ground, necessitating still more robust safety management
3. Increased capacity is required to meet the needs of project teams for delivery. Increase from 4 to 6 desk should increase capability.
4. Due to new builds and maintenance of existing network, outages and, as a result, switching and safety coordination will increase in future. Increased number of tests due to new protection equipment and maintenance of existing equipment. A separate area within controlled work area is needed where RT commissioning can take place as standard practice in other TCCs. Reduction in confusion, distraction by having clear and uncluttered workspace is required.

System Security Issues

Displays, Visualization Situational Awareness

5. Larger transmission footprint, more devices, larger span of control, more frequent outages, weather events. Wall mounted video wall display of system conditions as an overview is needed, such that it can clearly display events and be easily understood from anywhere in the Control Room or TCC office.
6. More complex equipment on the grid and more active systems requires better tools to monitor the system.
7. More substations, technology and important individual systems such as HVDC will have own displays and many alarms.
8. Increased number of alarms and devices with different control system interactions. Variety of alarm types will increase.
9. High Impact Low Frequency (HILF) and unanticipated events likely to increase, due to weather events, weaker grids, fragile complex network new equipment. These will have to be managed in real time.
10. Increase in High Impact low Frequency (HILF) events in future, so more frequent analysis and investigations will be required ex-post.
11. Improved awareness of comms datalink status by shadowing the comms links will be required in future. Need to monitor the datalink status constantly in real time, any drop in service has severe impacts on system operation.
12. Development of a set of suitable displays for the islands is needed to enhance awareness and better manage the situation
13. There will likely be a major increase in ANM systems in the coming years impacting transmission and distribution systems, increasing demands on the team in planning and RT timescales. New ANM displays and overviews will be required.
14. The complexity and interactions of ANM systems with existing power electronic devices will be important to monitor and manage in real time.
15. Dynamic line rating devices will be increased which will requiring active monitoring and control.
16. Devices that are not yet developed but will undoubtedly form part of the future system and may involve increased automation will be deployed.

Desk Space

17. A predefined room for the main incident room and smaller area for sensitive discussion or confidential work. This should be as close as possible to the control room.
18. Suitable wall areas for display of plans and progress.
19. Increase communication facilities such as SMART boards and comms ports for extra equipment and people.

Training

20. Increased need to train operators as the system evolves. Blackstart events are difficult to model and predict on the future system but simulation training helps.

21. Blackstart contracts are annually negotiated, blackstart and restoration plans will change annually and necessitates improved training.
22. Classroom type environment to practice and train operators effectively as part of a team is required for more complex disturbances.
23. For islands, training and more suitable displays are needed. Off-line training would benefit the operator teams greatly.
24. All new ANM devices will require training in relation their operation and interactions.

Data Management and System Monitoring

25. Major increase in new assets connected in future will require increased resource for administration and data management. This is likely to be needed within the period of T2. One extra desk plus storage system will be required to manage this role
26. There will be an increase in outages in the future as a result of new build plans and maintenance work on the existing network. This will result in more outages and more resources in planning and optimizing outages.
27. Exponential rise in planning activity due to the needs of the ESO to have more flexibility in the system.
28. The outage team should work very closely with the system operators and control room team on the outage plan, benefiting from the knowledge transfer from close proximity to experienced staff
29. Increased uncertainty due to flexible plans will require more contingency planning and alternative solutions to be planned.
30. Advanced study and analysis tools such as weather forecasting systems, system stability, HVDC and protection and automation will need to be deployed in the control center with consequent data needs.
31. All ANM systems will have to be modelled in the SHET system, monitored, studied and controlled as necessary by operators
32. Many more performance monitoring devices will be installed on the SHET system in the coming years.
33. It is likely that all new generation connections and any new equipment will have an associated monitoring equipment, the status and data will be monitored from the control room and fed to ESO.

Cost Issues

34. Additional space to house future systems and bring existing equipment under the umbrella of the TCC building for resilience.
35. Using data network or controlled telephony is part of a planned future project.
36. Increased risk of pandemic related issues requiring use of parallel facilities and regular changeovers and cleaning.
37. Increased degradation in main and backup facilities over time may cause more frequent building issues.
38. Diverse location and improved physical security for the separate servers and communications is required.

Projected UK and Scottish Power Growth Rates

The report by the Scottish Government on Scottish Energy Strategy to 2050 [10] details six key paradigms that the Sottish system of 2050 will be built on:

- Consumer engagement and protection
- Energy efficiency
- System security and flexibility
- Innovative local energy systems
- Renewable and low carbon solutions
- Oil and gas industry strengths

The system security and flexibility paradigm are of most importance to SHET in the context of a future resilience control center. It notes *"Scotland should have the capacity, the connections, the flexibility and resilience necessary to maintain secure and reliable supplies of energy to all of our homes and businesses as our energy transition takes place."*

The report aims to ensure the Scottish electricity system operators can *"Continue to work in partnership with National Grid, network owners and other key partners on electricity security and system issues in Scotland",* including:

- Ahead of the relevant regulatory price control reviews, develop:
  - Scotland Electricity Network Vision statement, and
  - Scotland Gas Network Vision statement.
- Collaborate with UK Government, Ofgem and others to deliver the goals in the UK Smart Systems and Flexibility Plan.
- Continue to closely engage with SGN in their 100% Hydrogen pilot project.

These goals and aspirations for Scottish system operators will necessarily require best practice facilities for transmission system control, including a main backup control centers.

Summary – System Operation Needs Gaps Between Best Practice for a Future Control Center and the Current Control Center

When assessing the response to the EJP, it was clear that a more detailed justification of the needs for a new control center was required. This chapter assessed the actual requirements for a control room to operate effectively in the GB system. It assessed the current control room environment and facilities, in consultation with SHET engineers and also the future needs of a control center to manage and operate the likely system of the future. This allows a gap analysis to be conducted, comparing actual needs to operate effectively, limitations of the current facility and the likely future needs.

The gaps in resilience of the current facility are detailed in the chapter, the most important of which are:

- Lack of space and lack of overview display capability, reducing the situational awareness of operators and ability to effectively monitor and control the grid.
- Access by external parties and workers is a security risk. Distraction, disruption, noise may lead to an increased safety risk while switching and/or performing the safety coordination role.

- Lack of an integrated approach to training and lack of facilities to conduct effective training.
- Lack of office space or meeting rooms to accommodate planning, coordination with outage planning team and silver team management in the event of a crisis.
- Rapidly evolving nature of the system means the degraded ability to monitor and control the system may lead to an increased quantity of disturbances or prolonged response due to inability to identify root cause of issues.
- Facilities are inadequate to accommodate a blackstart situation, both from the point of view of system control and restoration as well as prolonged periods within the facility to manage a prolonged emergency.
- Redundant backup facility is inadequate for monitoring and control of the system and for use in an emergency situation.
- Need to adapt to a more flexible space to accommodate the needs of a more complex future system

In total 43 issues were identified with the current control room in Inveralmond House to manage the existing system. 23 future system technologies or changes to current system operation that will impact SHET and 38 needs in the control room to manage the system of the future were identified that can form the basis for considering the development of a new resilience operations center.

3 WHY IDENTIFIED PROPOSAL IS NECESSARY - THE RISKS WITH DO-NOTHING CASE

To address the comments and issues from the evaluation of the EJP [3] (as discussed in Chapter 1) around the disproportionality of the proposed "responsible operator" option, and to improve the business case and engineering justification, the following questions need to be answered with evidence-based elaboration:

- What are the risks with maintaining operations from the current control center?
- What are the cost efficiencies associated with the new control center?
- What value will the new control center bring to the customer?
- What are examples of other control centers for similarly sized transmission owner/operators?

What are the risks with maintaining operations from the current control center?

The "Do-Nothing" case is the option to maintain the current control center facility in the Inveralmond house, and continue to operate the system from there indefinitely, with Buroughmuir as a backup facility. From a high level analysis: There are multiple risks that currently exist that degrade resiliency of operations which are associated with this approach, including:

- Cyber or physical intrusion by hostile actors.
- Reduced or non-existent situational awareness due to lack of Tier 1 displays (discussed in chapter 4) which will increase issues with system control and monitoring as the system gets increasingly complex.
- Difficulty with blackstart and restoration (SHET must act as the system operator), with potentially increased times for restoration as a significant extra cost to the consumer. This is an issue for three reasons:
    - Managing the blackstart from a system point of view with inadequate situational awareness
    - Adequately trained operators on blackstart simulations, process and plans
    - Inadequate physical facilities for a prolonged period of time in the control center to restore the system
- Issues with the adequacy of the redundant backup facility at Buroughmuir in the event a business continuity issue such as a pandemic or building failure, which degrades resiliency.
- More frequent human errors and mistakes as a result of distraction, interruption due to suboptimal control room and office layout and facilities and lack of no-interruption zones.
- Degradation in training standards and practices of operators, especially for a complex evolving system which will require an increased focus on training to effectively monitor and control the grid.

- Lack of joined up approach to system control (i.e. not interlinking outage management and asset health monitoring function) will lead to inefficiencies in transmission operation and maintenance.

As part of the needs assessment and gap analysis undertaken as part of a review of the roles and tasks that SHET must perform in the control room (detailed in Chapter 2), the risks of failure of the function were assessed and documented. These are collated in a table in Annex 1. The risks are summarised below:

Safety and Security Issues

Field Staff Safety

1. Errors or mistakes in operation can have safety risks for staff working on live equipment. Risk of serious injury or death.
2. Danger to the public or workers may result from failures of equipment as result of errors or mistakes.
3. Serious injury or death of field staff as a result of a mistake in commissioning from grid operators.
4. Failure of telephony: Lose ability to dispatch, potentially lose the ability to control system. Safety checks unable to be carried out.
5. Drastic risks to health and safety of working field personnel if safety coordination is mismanaged by the control room operators.

Control Room Operations Staff Safety

6. Increase in cyber/physical security risk at main and backup site
7. Risk of business facilities failure requiring transfer to backup facility due to weather, external threats.

System Security Issues

Situational Awareness

8. Wrong operational decisions or operational switching issues leading to failure of the network due to reduced situational awareness or mistakes or errors.
9. Operational Switching Failure: Brownout or blackout conditions may develop if switching cannot be carried out or if there is a gap in situational awareness.
10. Delays to restoration of customers if there is an outage both for normal outages and more severe HILF events.
11. Grid voltage or dynamic instability can occur with consequent damage to transmission and generation system equipment and assets.
12. Risk of disconnection of customers as a result of a mistake or error during commissioning.
13. System reliability failures, by not understanding what's happening – e.g. protection failure, or inability to diagnose root cause of events
14. Failure to investigate and resolve system issues may result in a repeat occurrence of issues e.g. increased time of disturbed voltage.

15. If a protection, operation, user test goes wrong or is improperly managed, there may be impacts on safety of personnel, customer load, and / or equipment. Equipment without protection for any period is a risk that must be managed by system operators.
16. Failure of Active Network Management devices can result in security standard violations and system impacts.
17. Human error in failing to correctly monitor ANM devices could exacerbate poor system conditions.

Blackstart / Emergencies

18. Blackstart related issues are very important to address. Slow response, of restoration has major socioeconomic impacts. Ernst Young estimate a 913 million GBP per day loss to Scotland for a blackout, with major socio-economic impacts.
19. Backup facility failure: Increasingly complex transmission system is more difficult to monitor and control from the backup site.
20. Compromised space requirements and cleanliness of facilities for sterilization and pandemic related pathogens.

Training

21. Deficiency in training operators for unanticipated events will result in delays in restoration or inadequate response.
22. Inability to adapt to new blackstart routes as they can change more often than previously was the case.
23. Lack of awareness, knowledge as a result of degraded training can pose a system risk.
24. Lack of training on ANM devices poses a risk to understanding of the risks to the system.

Data Management and Monitoring

25. Incorrect data within the EMS and data to ESO market or transmission operator systems could have major economic implications
26. If datalink goes down: Loss of situational awareness, no monitoring or control ability in SHET. Loss of data possible to market and transmission operation systems.
27. If datalink goes down: ESO are blind to major portion of GB system if link goes down and undetected.
28. Confusion in switching plans and orders because of mislabeled nomenclature may result in mistakes in switching or operation.
29. Increase in alternative planning and network access strategy adds to team workload, to maintain efficiency and reduce errors.
30. Risks to ESO operations and market processes if data is not cleanly exchanged or if there is a breakdown in the processes for any reason.
31. A failure in performance monitoring equipment will lead to degraded situational awareness for a period.

32. In a system that is weaker and more complex, a degraded system for any period may cause system issues to go undiagnosed or may exacerbate already bad system conditions.

Cost Issues

33. Unsolved issues on the system will be active for longer than necessary.
34. Failure to comply with STCP (with consequent license issues) and risk of continued issues due to lack of resolution from failure to investigate.
35. Costs of maintaining islands is high if the timeframe is long for restoration
36. Lack of opportunity for gens to return to market has cost implications for them.
37. Overuse of diesel generation when islands are de-synchronized.
38. Risk of damage to equipment and assets with cost implications.
39. Incorrect data or naming can have cost implications for asset management.
40. Sub-optimal outage planning can have major impacts on delivery of extremely capital intensive works projects.
41. Cancellations, deferrals can have major implications on cost and resource adequacy planning for the asset owners and generators.
42. Delays in delivery of this information are difficult to recover from and can delay the delivery of a project.

What Value will a New Control Center Bring to Customers and Stakeholders?

Improved Resiliency

Operating from a safe, secure facility, which dramatically lowers the risk of intrusion or nefarious activity will build on the excellent resiliency record of SHET. Field crew staff, grid operations staff will have more security and peace of mind and there will be less risk of commercially sensitive information being stolen and used for nefarious ends. Overall resiliency will be improved with a new control center. There will be a reduced risk of building failure, necessitating emergency operations from the backup control center.

Having a clear redundancy plan and adequate redundant facilities also allows a dedicated backup facility in case of major incidents in the building or in the event of a future pandemic. At present the backup facility is not fit for purpose, so if a major incident occurred in the building, there would be a risk to the reliability of the system during changeover and operation at the backup.

Improved Efficiency

Having a larger facility will allow improved capability to monitor the system under control. This will lead to improved operator situational awareness at all times when monitoring and controlling the system. For load loss incidents - when they do occur – the response of the operators is critical. With a new facility - with better system monitoring - the response will be more efficient and faster so that supply can be restored in the minimum time frame. More space and a custom designed control center layout facility will allow operators to more efficiently manage the system.

As the system evolves with new network technology, increased sector coupling and improved software and data for monitoring the system, operators will have the facilities and tools to exploit the increased flexibility and ensure the network is run in the most optimized fashion.

Having more space for office and team collaboration spaces will allow outages to be planned more effectively and plans to adjust the system can be optimized. This efficiency will lead to cost reductions for outage delays or overruns.

Reduced Human Error

Having a modern, integrated, training facility in the main control center will be instrumental to more complete and efficient on-the-job training, classroom based training and simulator based training for grid operators. This is a critical aspect of future system operation as the system is evolving so rapidly that training needs to keep pace with the rapidly changing system as documented in Chapter 6.

The impact of the 2020 global pandemic has meant that on the job training (OJT) involving close contact with a shift operator will be very difficult in the future. Operators who are consistently trained in an environment integrated with the main control center will be less likely to make mistakes in real time, meaning less human error-related incidents related to switching on the system. This may result in less inadvertent load disconnections, lower ENS, and reduced safety switching incidents. This will be in the context of a massive increase in network upgrade and addition projects in the coming years. Improved training will also lead to faster response to loss of load events when they occur as operators will be able to detect and mitigate the issues more efficiently.

Improved Reliability

The improved efficiency and reduced potential for human error of operators and the operations team more generally will lead to improved reliability of the system, reduced ENS and faster response to emerging system issues. New facilities will bring new and improved IT infrastructure, which will be designed with resiliency in mind. The key functional tasks of operators in the control center such as switching, and voltage control will be carried out efficiently and proactively instead of reactively. Improved situational awareness should ensure system monitoring and security and alarm management is carried out to the highest standard.

Future Ready

The system is changing very rapidly and forecasting in the 5-10 year time horizon is about as difficult as it has been in any period in the history of electricity grid operation. Having a facility and staff that are capable of adapting to whatever future grid emerges will be critical. Some control centers in Europe have recently been adapted to cater for the changing system. For example, in Spain Red Eléctrica de España - the Spanish TSO - have installed a renewables control desk in their main control center. Having this adaptability to meet whatever the future system needs might be is a powerful incentive in the need develop a new facility. Some functions of the STCP or future regulations may require dedicated resources, operators or desks to be set up. Some examples of potential dedicated future roles might be renewables management, offshore grid management, HVDC management, coordination with ESO, DSO or other sectors, cyber/physical security, testing and commissioning, system stability or security management, power system monitoring

Figure 3-1 CECRE renewables control desk as an add-on to the main transmission control center in RE. [Source: Red Eléctrica website]

Change in Regulations in Future

The rapidly changing network is causing rapidly changing regulations, new market rules and services and other functional changes that SHET must adapt to once imposed by Ofgem or National Grid ESO. These changes in regulation are unknowable now, but the future operations teams and control center staff will have to adapt to meet the requirements if/when they are imposed. There will be closer collaboration with the ESO as the system will be operated more flexibly. Having a control center that has facilities that are capable of being adapted quickly, efficiently and linked with training will add value to SHET in future and potentially reduce costs associated with retrofits.

Opportunity Cost

The present solution for the SHET control room or Buroughmuir are not adequate or adaptable for the needs of the future system and are likely not CNI compliant for physical security at present. Upgrading one, or more likely, both of these facilities will be required in the coming years to mitigate the security risks. The incurred opportunity cost of investing in upgrades of facilities that are substandard relative to developing a new facility on a green field site may be significant, There is also a risk of investing in an upgrade or retro-fit project while the system changes in such a radical fashion as to render the retro fit inadequate for future system control.

Summary

When assessing the needs and justification as well as the proportionality of the solution, it is essential to assess the risks of maintaining operations from the current facilities. This would be

essentially be the “Do Nothing” case. This chapter highlighted 42 of the key risks to maintaining operations at current main and backup facilities as they are today around the broad topics of safety and security, system security and cost. The key risks identified were:

- Safety issues associated with switching, testing, voltage control and safety coordination as a result of distraction, disruption and noise.
- Risks to field crew of human error from reduced situational awareness and distraction.
- Risk to system operation integrity as a result of inadequate displays and lack of space to plan and coordinate.
- Potential risks of slow response to blackstart and restoration due to inability to co-locate silver team command centers near the control centers.
- Cyber physical security risks as a result of co-location and sharing office space and inadequate backup facilities.

There are many other risks identified in this report which reinforce the point.

It is necessary also to identify value for money for the consumer in developing a new facility. In this case, defining clear metrics and monetary value is difficult, however value can also be achieved by reduced costs. By de-risking the system operation facility by upgrading to a new facility, the resilience of the transmission system is automatically increased. Operators will have vastly improved situational awareness and training and the response to emergency events on the system can be clearly planned and executed. This should increase system operator efficiencies with consequent increase in system reliability, which will untimely benefit the end consumer.

4 THE NEED FOR A NEW CONTROL CENTER

The main advantages of upgrading to a new control center facility for SHET will be some or all of the following:

- Large videowall for
  - improved situational awareness,
  - improved decision making
- Structured, segregated environment
- Reduced disruption, interruption and distraction
- Allows for operational team collaborations within control center during:
  - normal operations for planning
  - emergencies, blackstart events, silver team events

Situational Awareness – Endsley's Model

Situational awareness is a nebulous term but its importance to reliable and resilient system operation cannot be understated. The most widely accepted definition and model of situational comes from Mica Endsley [11] is shown in Figure 4-1.

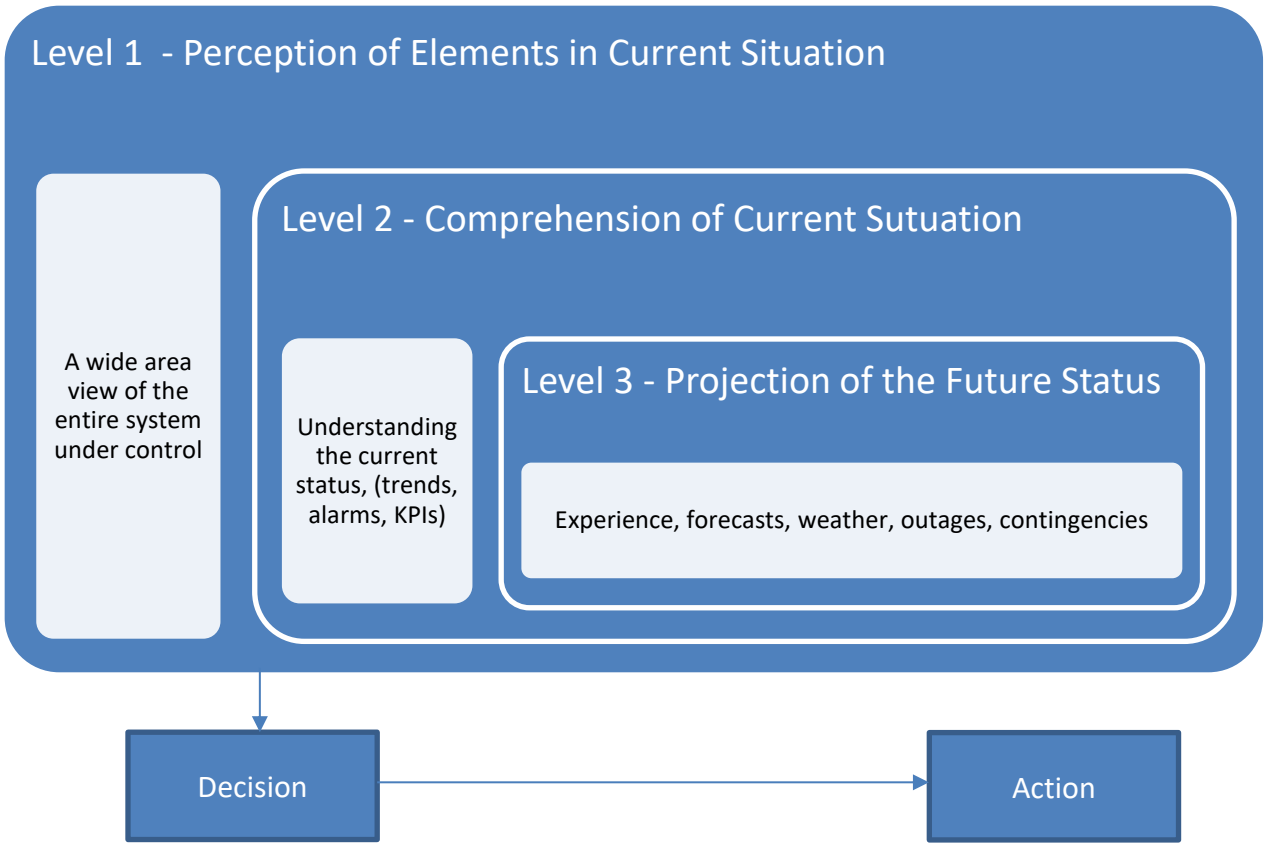

Figure 4-1: Mica Endsley's model is the most widely used model of situational awareness for control center or system critical operators [11]

In the context of transmission system operation, The level 1 and level 2 of the situational awareness model **require a wide area view of the system under control**. It is not possible to perceive and comprehend the elements of the system without an image or model of the system in its current state as well as key performance indicators for the transmission system under control and its alarms.

Situational Awareness and Structured Decision Making – Boyd's OODA Cycle Model

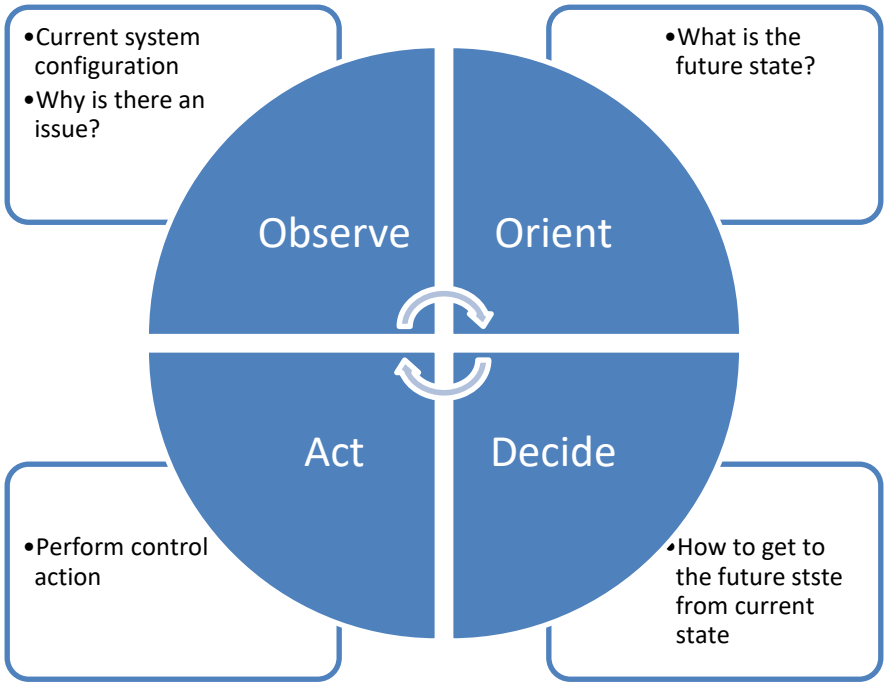

Figure 4-2 Boyd's Observe Orient Decide Act (OODA) loop model of decision making and situational awareness

John Boyd's OODA model [12] is commonly used model for decision making in both real time operations and in everyday business operations. A simplified version of the loop and explanation is shown in Figure 4-2. It encompasses four states that are in a loop or cycle:

- **Observe**
  - Observing the system as it currently is and if an alarm or issue appear on the system
- **Orient**
  - Based on the current observed state and alarms, identify what the future state should be, based on forward projection and other available information
- **Decide**
  - Make a decision based on best available information
- **Act**
  - Perform action

Both Endsley's Level 1 *perception* state and Boyd's o*bserve* state are critical first steps in decision making and control in a real time, system critical scenarios, such as transmission system operation.

In the context of transmission system control, having a wide view of the system under control is essential to this process.

Best Practice Display Design – Linking Displays to Situational Awareness

The frameworks situational awareness for decision making described above have in recent years permeated into visualization techniques and design best practices for human machine interfaces (HMI) in control centers. This change has led to the adoption of the ISA 101 standard on HMI design and best practices [13] and design books such as the High Performance HMI Handbook [14]. These emphasize a hierarchical approach to display designs, with each display tier in the hierarchy, progressively showing more detail.

The Tier 1 display is the initial entry point of interacting with the system via the model. This should be as complete as possible display of the system under control or an all-encompassing dashboard, showing the key system parameters and whether they are within limits or not.

Tier 2 displays more information about a specific task – voltage control, outages, alarms, substations

Tier 3 displays more detailed information for switching, usually control displays in substations.

Tier 4 are support displays, substation tabulars or backend displays.

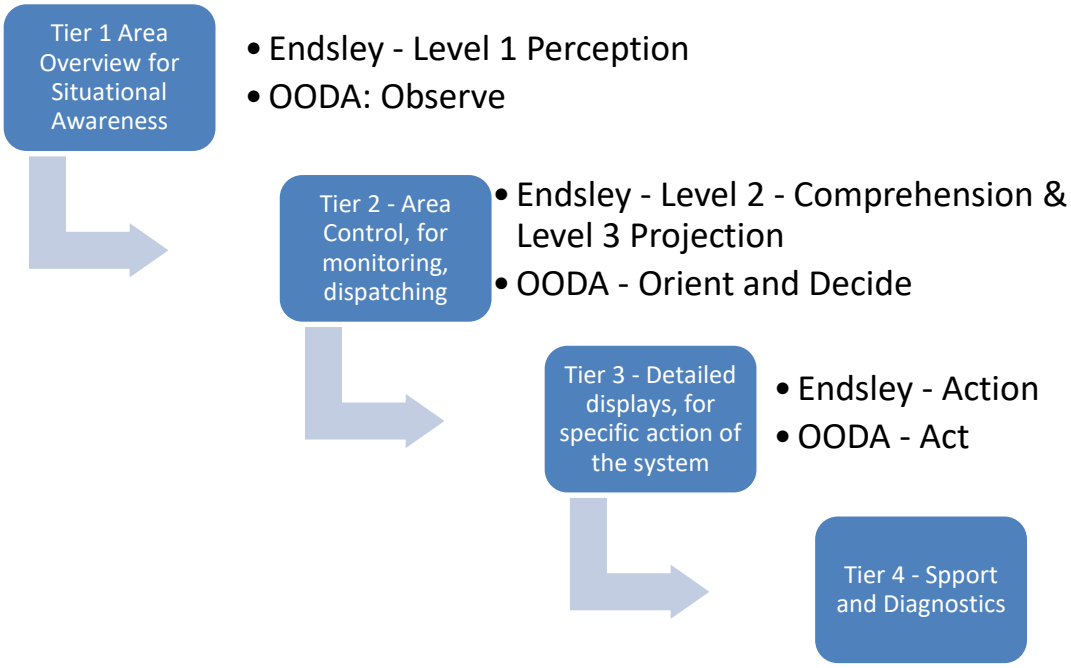

Figure 4-3 High Performance HMI Handbook [14] 4-Tier framework for effective HMI design and the crossover to situational awareness models of Endsley & Boyd.

Large Videowalls

The vast majority of transmission operation companies around the world have a large video wall display in their control centers. This is irrespective of the precise function or role of the control center (balancing, transmission operations, transmission ownership, reliability coordinator). The

videowalls give a wide overview of the entire system under control. The videowalls in use in transmission control centers today evolved from a static map board display which gave a one line overview of the transmission system under control. As transmission systems expanded, it was difficult to represent the grid in a static configuration, so a more dynamic solution was required. With the advent of modern Energy Management System (EMS) and software and visualization technologies, there is now a wide range of possibilities for the display of a wide variety of information on videowalls. The information on a videowall is used to guide and inform the operator in their decision making processes, alert them to issues on the system and to observe and perceive the current state and project or orient to the future state.

In recent years the large videowalls in control centers have adapted to show, not just the grid but also key indicators, trends, alarm statuses of the system's status, related to the operator's role.

The Current SHET Control Center

At the current SHET control room, there are two displays on the wall, which currently act as the "Tier 1" type displays of the system (see Figure 4-3). These screens display the transmission system overview, and a small number of trends. The displays are 42 inch monitors, and the resolution quality is low.

Even if the resolution quality was high the amount of information that can be comfortably displayed on the screens, while still being visible to operators at the desks in the control room is very constrained. In the future, as the system expands, the other elements of the system will have to be prominently displayed. Refer to Chapter 2 on what elements of the future system will be incorporated into a future control room.

The system will undoubtedly become more complex, HILF and unanticipated events will become more frequent, requiring better methods of observing the system under control and to give the operators in the control room optimal situational awareness. This can be achieved by

- Large, full transmission system overview being displayed prominently
- Streamlined and effective dashboards, displaying key information prominently and linking the information to other relevant information.

Double Screens and Double Height Spaces

A proposed solution might be to add (bank) more screens to the control room console desks. In other transmission control centers and in other industries requiring real time monitoring and control (aviation, space, transport, finance) double screens are common. They are also used in the existing SHET facility which can be seen in Figure 4-4. This solution is useful for improving visualizations of the system but are usually used to display different elements or parameter displays rather than overviews of the system.

However due to the limitations of the control room, and because there is no double height space – if screens are banked, they will take away visibility of the overview screens on the wall. Without standing, it will be difficult to see the overview displays on the wall over the banked desk monitors.

Figure 4-4 Existing SHET facility control center desks

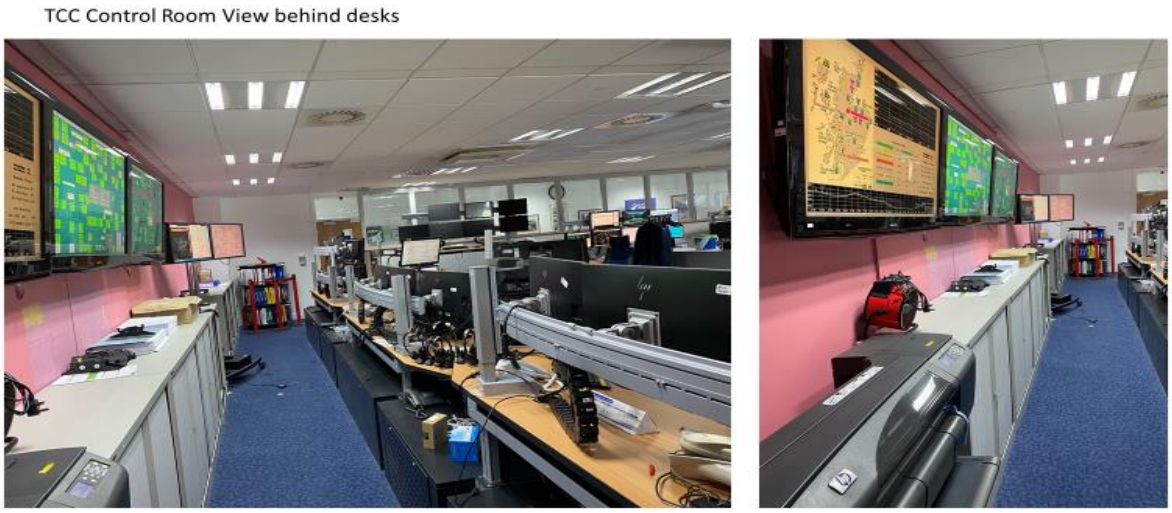

Figure 4-5 Existing SHET control center wall displays

Display Screen Equipment (DSE) Regulations – Ergonomics

People who constantly work with display screen equipment such as computer monitors in a control room are likely to develop health issues such as back, shoulder and neck pain as well as eye strain

issues [15]. Unless the equipment is ergonomically aligned these issues can exacerbate over long time periods resulting in poor health outcomes for staff.

One of the best practices for an ergonomic setup of DSE equipment is to regularly stand up and sit down and to take regular breaks. This is only possible in a control room if there are stand up desks. The SHET control room desks could be re-purposed with stand-up desks but due to the height restrictions in the control room, the wall displays would be obscured, especially if the monitors are banked. Many control centers around the world allow the use of stand up desks for their operators.

In a new control room facility, with a double height space or higher the Point 1 overview displays or videowalls would not be obscured to any point in the room even with a stand up desk.

Figure 4-6 Control room in Elia the transmission system operator in Belgium [Source Elia Group Website [16]]

Similar Control Center - Scottish Power

An example of a very similar arrangement is Scottish Power Energy Networks Network Control Center in Glasgow. As seen in Figure 4-7, the wall is covered in displays of essential information such as the network overview, trends, alarm list, contingencies, communication status, GB system status and information, weather, phasor monitoring units and others.

This arrangement allows operators to observe the system and perceive any imminent danger and to diagnose network issues via the Point 1 displays with “one-look” - should they get an audible indication or flashing animation notification. It also improves the operator’s ability to serve as an aid to restoration and blackstart if that is required.

This arrangement would not be possible or costly to implement in the current SHET environment. This demonstrates that the operators at SHET, when compared with operators Scottish Power (who perform an almost identical role and function) are at big disadvantage in terms of their ability to perceive and monitor the system. As the system progresses into the future, these limitations will be exacerbated further due to the rapidly evolving nature of the system.

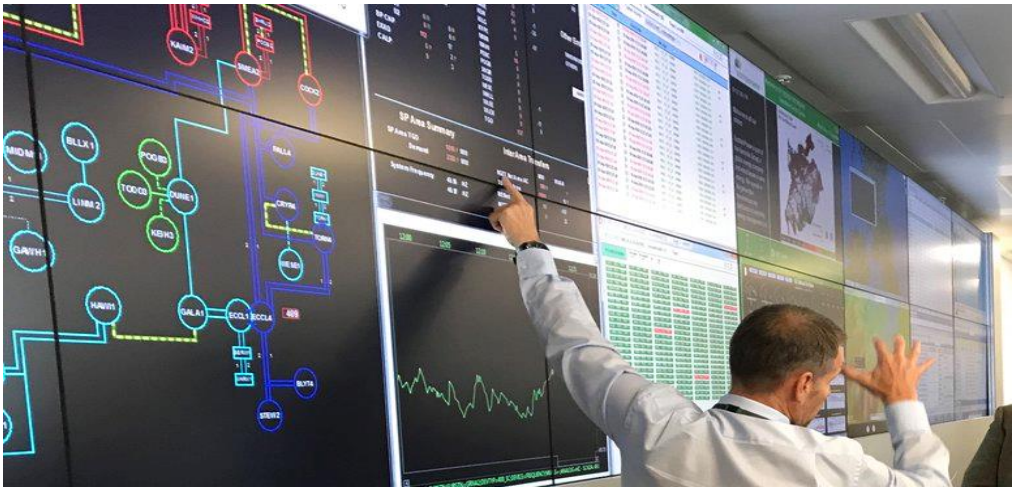

Figure 4-7 Scottish Power Energy Networks - Network Control Center [Source: Twitter]

Extending the Existing Facility

There exists an option to extend the existing control room facilities in Inveralmond house, however the building is at capacity at present, repurposing the existing facility to include all the necessary facility changes would likely be expensive relative to the cost of developing a greenfield site with the facilities designed and built with limited constraints or restrictions.

It should also be stated that Buroughmuir, which currently acts as the backup facility is constrained in a number of ways also including space limitations, single point of failure of the grid supply point, and inadequate physical security arrangements. As per the proposal to Ofgem, the current facility in Inveralmond would be adequate as a backup facility for infrequent, emergency use, with enough space, as well as the existing display screen equipment and hardware to monitor and control the grid, albeit with sub-optimal overviews and limited displays for situational awareness.

Disruption, Interruption and Distraction

Human errors in system control or in safety critical operations can be broadly distinguished in two categories as per Reason [17]:

- Category 1 - A person intends to carry out an action, the action is appropriate, but they carry it out incorrectly, and the desired goal is not achieved. - An execution failure has occurred. Execution errors are called slips and lapses.
- Category 2 - A person intends to carry out an action, does so correctly, the action is inappropriate, and the desired goal is not achieved - A planning failure has occurred. Planning failures are mistakes.

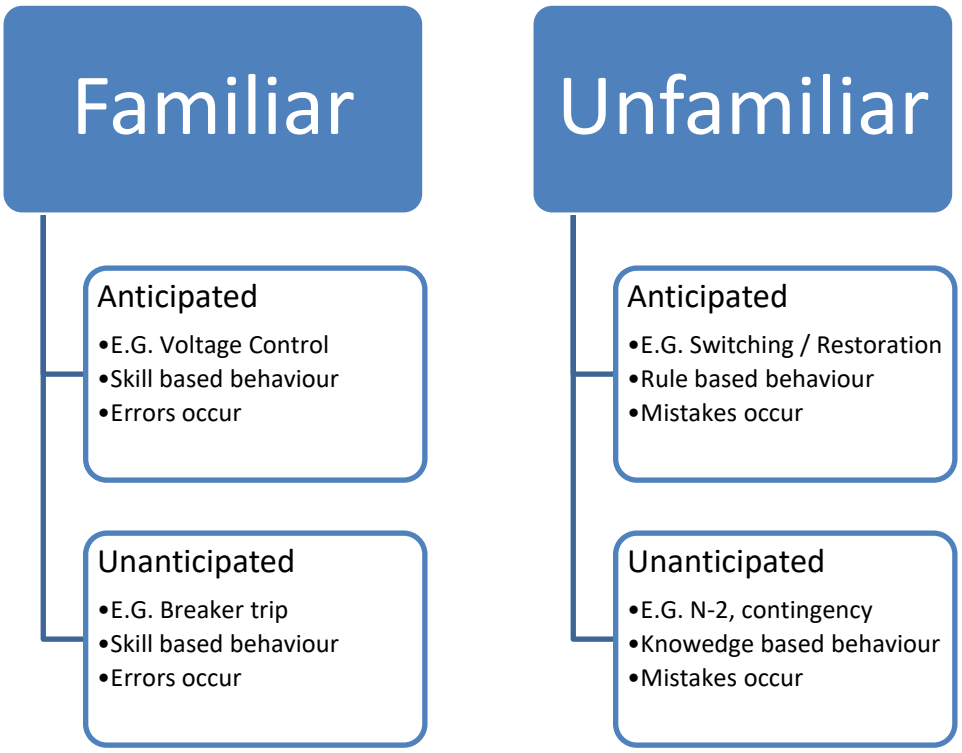

Figure 4-8 EPRI model of familiar and unfamiliar events adapted from Rasmussen [22]

Approximately 61 % of all human errors in complex safety critical environments are skill based, category 1 errors involving slips or lapses during familiar events. Distraction and interruptions are a common cause of category 1 errors.

Effects of Distractions And Interruptions

Distractions and interruptions include anything that draws away, disturbs, or diverts attention from the task at hand, forcing attention on a new task - at least temporarily. Attending to the new task increases the risk of an error with one or both of the tasks because the stress of the distraction or interruption causes cognitive fatigue, which leads to omissions, mental slips or lapses, and mistakes [18]. Distractions can be caused by a variety of sources such as: noise, electronic devices, alarms. Interruptions are caused by people seeking procedural clarifications, requests, calls etc. When these occur during procedural activities (such as switching) return to the procedure can result in slips or lapses.

High reliability organizations (HROs e.g. health care, space, fire crew, transmission system operators) are adopting practices to limit distractions and interruptions, usually from aviation such as:

- No Interruption Zone – a demarcated zone for critical procedures and tasks can be carried out and all staff are aware that no interruptions are allowed. This would be a standard arrangement for a control room, segregated from all non-critical staff.

- Do not disturb signs either worn by operators or signs on the desk or more typically usually a door lock and safety siren in transmission control rooms.
- Better education of other staff of the criticality of the role of operator and the nature of critical switching and safety coordination.
- Designated times for interruptions.
- Checklists – during switching ensuring a plan is maintained and checked off so that if interruptions occur return is straight forward
- Preparation – plan ahead and limit the need to interrupt a procedure by having to retrieve an item
- Reduce noise by muting alarms temporarily or other usual background noise.

SHET Control Center Layout, Human Throughflow

The current SHET control room is in a very disadvantageous position relative to the office layout, which contributes to distractions, interruptions and potentially errors. Some of the issues with room and office layout include

- Human Traffic
    - A constant throughflow of human traffic near the control room desks especially of non-operational personnel is a constant distraction to operators. It also increases the risk of exposure to sensitive documents or information on the displays in the control room.
- There are many meeting rooms in the vicinity
    - Non-operational staff attend meetings near the control room desk operators, this adds to the throughflow of people and leads to interruptions and distractions as meetings start and end
- Conversations
    - Meetings near the desk inevitably lead to loud conversations between meeting participants at or near the desks. These conversations increase the noise levels and lead to distractions
- Background Noise
    - Because the control room is on a floor with numerous other personnel, background noise increases distraction potential during normal system operation tasks.
- Position of the team leader – does not defend switching and operators.
    - In a properly laid out control room, the supervisor would be the first point of contact for potential interruptions, before operators are interrupted. The layout of the existing room does not allow for this.
- Lack of a No Interruption Zone
    - Because the control room is on a floor with numerous non-operational staff, a no interruption zone with switching siren or door lock ability cannot be implemented unless the floor is entirely cleared.

Mistakes in System Operation

As shown in Figure 4-8 mistakes occur during unfamiliar events both anticipated and unanticipated. They are usually due to failures in planning for the events (switching errors or

outage changes). In SHET, effective planning is inhibited by lack of space in the control room and in the dislocation of team members as well as distractions. Suboptimal plans to deal with unfamiliar events are a cause of human error, during all types of events.

Summary

This chapter outlines the key areas and importance of situational awareness, decision making, displays and monitors and the causes of human errors. The key points were made with reference to the SHET control room and included:

- The most commonly used models of situational awareness emphasize the need to **observe the current status of the system or perceive the system** at it currently stands.
    - As it's the first step in the framework, this is arguably the most important aspect of real time operations of system critical grids.
- Observing or perceiving the system with a wide area overview is a key element of best-practice human interface display design which has a hierarchical approach to displaying information. Tier 1 is at the top of the hierarchy. Tier 1 displays should have a wide area overview of the transmission system as well as key indicators of system status.
- All transmission system operators around the world have adopted this framework for visualization and situational awareness since the earliest days of transmission grids, by installing large map board or videowall overviews of the system
- In recent years these large videowalls/map boards have included dashboard type information as well as the system overview
- There is no space for a large videowall in the SHET office, the existing facility is not adequate to display information about the entire system and will not be adequate to display other information in the future, as the system evolves.
- This results in inadequate or degraded situational awareness for the operators in normal and emergency system operation.
- Double banked screens can help but adding these inhibits the view to the Tier 1 displays on the wall of the current control room.
- Setting the display screen equipment up optimally is a key aspect of ergonomic design in a control room. Many control centers around the world are installing stand up desks for operators to allow breaks in continuous sitting. Implementing this in the existing control center would inhibit views of the Tier 1 displays further.
- Scottish Power, a system similar in nature and size to SSEs have a network operation center that has a very effective Tier 1 display overviews and videowalls which enhances operator situational awareness.
- Category 1 errors are the main causes of human error in control rooms. These are errors that occur in familiar circumstances, for example during voltage control or responding to alarms.
- They are caused mainly by slips or lapses, where predefined steps are not followed, missed or skipped. Distraction and interruptions are the main cause of category 1 errors.

- Segregating a non-interruption zone for switching is an effective way to limit distraction and interruptions. This is not possible in SHET control room due to the layout of the office and the human traffic.
- Close meeting rooms, noise, conversations, desk layout are all causes of distraction, and interruptions which may cause human errors during familiar and unfamiliar scenarios.
- Mistakes occur due to failures in planning for unfamiliar events. In SHET, effective planning is inhibited by lack of space in the control room and in the dislocation of team members as well as distraction.

5 CYBER / PHYSICAL SECURITY AND BUILDINGS

To understand the cyber and physical security needs for the future control center, it is necessary to analyse the current security system and any existing physical security standards that must be adhered to. Physical security precautions are essential to ensure the safety of staff in the office and in the field and operators and for the protection of commercially sensitive data and information in relation to the grid and SHET company in general.

Risks of Deficient Cyber / Physical Security

There are numerous important risks to having deficient physical security in the SHET control center building. It is reasonably easy to affect catastrophic damage on the health and safety of field workers and individuals and to cause widespread disruption to society by nefariously switching on the network.

As an example, a line that is out of service for maintenance will typically have maintenance personnel in the vicinity of the outaged plant. If the line is energised unexpectedly (nefariously) from the control center, then serious injury and death could occur. The risks can be summarised by:

- Physical or remote access to the control center by nefarious individuals to:
  - Perform malicious damage by switching dead plant into service
  - Control the grid to disconnect HV equipment and cause blackouts or brownouts.
- Building damage causing an evacuation, to the transmission control center backup facility that at present is sub-optimally designed.
- Vandalism of computers or other equipment which may cause monitoring and controllability of the system to be lost.
- Open access to documents or computers or other systems containing sensitive, confidential or system critical information, that may be used to affect markets or cause other harm.

Current SHET Physical Security Arrangements

At present the SHET control center is/should be categorised as a Critical National Infrastructure (CNI) site by the Centre for the Protection of the National Infrastructure (CPNI) [19]. This means that as a critical site for the control of national infrastructure, the site needs a level of physical security, beyond that of a normal office facility, and requires capital investment to upgrade the physical security provisions and facilities to the heightened standard, governed by the CPNI (the exact standards are not publicly available). Increased operational expenditure is also expected to maintain the hardened cyber/physical security facilities at the control center.

The SHET, and all transmission control centers in the UK, are deemed critically important, given the consequences to wider society of a security breach resulting in a nefarious incident in the control center. In SHET's case the amount of power that is generated within, or flows through the

SHET transmission footprint, makes it integral to the integrity and stability of the wider Great British grid. A major cyber / physical security breach in the SHET control center has the potential to cause catastrophic socio-economic damage on the GB system as a result of loss load or a blackout and/or result in serious injury or death of personnel.

There is always a heightened risk of cyber/physical security breaches at critical national infrastructure sites for well-documented reasons, so rigorous procedures and protocols must be adhered to and facilities must be of the highest standard.

SSE has developed a set of Cyber Security Standards that align to the industry best practice NIST (National Institute of Standards and Technology) framework. This is widely acknowledged as the preferred framework for protecting Critical National Infrastructure (CNI).

Issues Associated with Current SHET Control Center

There are a number of issues associated with physical security of the building housing the current SHET control center that were highlighted in the EJP, namely:

- Mixed use office building
- Excess of non-operational, office staff in the building and control room floor, vigilance difficult due to the mixed nature of personnel visits
- Risk of tail-gating into control room
- Entry exit points not secure
- Lack of clear segregation between business units in SSE

This resulted in a conclusion from SSE Group Security (as documented in the EJP) that there is no acceptable permanent solution to security concerns at the existing location.

CPNI Security Standards / Guidance

The Center for Protection of National Infrastructure is authority on the protection of critical assets and infrastructure in the UK. While no published standards are available for download or publicly accessible for the hardening requirements of critical assets and facilities, the CPNI documents security risks and mitigation on its website [20] in relation to cyber/physical security. The list includes:

Threats

- Terrorism
  - The current terrorism threat is SUBSTANTIAL – meaning a threat is LIKELY
- Espionage
  - Including cyber espionage
- Cyber Intrusion
  - There have been documented cases of cyber intrusion in electricity networks including in Ukraine, ENTSO-E in Belgium, and in Portugal and Denmark.
- Other
  - Weapons of mass destruction
  - Organised crime

Mitigations Gap Analysis

The CPNI documents a number of threat mitigation topics and suggested mitigation measures [20]. These are not part of an official standard or compliance documents for critical infrastructure. The threat mitigations are listed in Table 5-1 along with how each threat mitigation is currently implemented in the SHET control center. This allows a gap analysis to be performed on what is required of a critical infrastructure site and what is currently in use in the existing site. **The current SHET arrangements and the gaps columns should be documented by SHET group security.**

Table 5-1 Threat mitigations as proposed by CPNI and whether they apply to SHET in the current or future control center

Threat Mitigation Topic	**Current SHET**	**CPNI Suggested Measures**	**Gaps**
Doors		Measures to assist in the detection, tracking and monitoring of intruders and other threats, such as unmanned aerial vehicles	
Search and screening		Measures to assist in the detection of threat weapons, including for example explosives, knives, firearms, chemical/biological/radiological material etc.	
Access controls		Access control and locking systems Physical and active barriers to deny or delay the progress of adversaries	
Perimeter physical defenses		Physical and active barriers to deny or delay the progress of adversaries Measures to protect people or assets from the effect of blast or ballistic attack Measures to protect against or limit the spread of chemical, biological or radiological material	
Intruder detection, monitoring		Measures to assist in the detection, tracking and monitoring of intruders and other threats, such as unmanned aerial vehicles. Access control and locking systems	
Windows		Measures to protect people or assets from the effect of blast or ballistic attack	

		Measures to protect against or limit the spread of chemical, biological or radiological material	
Building services		Measures to protect against or limit the spread of chemical, biological or radiological material	
Structural framing, walls and floors		Measures to protect people or assets from the effect of blast or ballistic attack Measures to protect against or limit the spread of chemical, biological or radiological material	
Protection of sensitive information and assets		Measures to protect sensitive (e.g. classified) material or assets	
Security control room		Security personnel (covered within the Personnel and People Security). Command and control. The response to an incident	

Other European Control Centers – Physical Security Arrangements

Based on experience of other transmission operators in Europe and the UK, some or all of the following measures are implemented at the building which houses the transmission control centers.

- Human security at the main entry checking entry
- Armed guards at main entry point
- Sign In / Sign Out for all visitors entering the premises
- Pre-approval, validation, ID checking at entry
- Swipe access for staff to building at all entry / exit points
- Swipe access is mandatory for entry and exit at all doors
- Turnstiles linked to security swipe system, electronically logging all entry and exits.
- Tailgate-proof turnstiles for entry of staff
- Cameras at all entry and exit points
- Swipe access to lifts.
- Restricted access from lifts to floor with control center, IT, or EMS personnel or equipment.
- Swipe plus pin code entry to the control center room.
- Fingerprint / biometric access to control center room or control center building.
- Swipe entry and exit access to car park.
- No openable windows in the control center room.
- All deliveries inside the building perimeter accompanied by physical security personnel.
- All deliveries logged in an electronic system.
- Temperature and symptom checking for serious illnesses such as COVID-19.

Control Center Security Standards in North America

The North American Reliability Corporation (NERC) has responsibility for standards and compliance for the key functions of electricity system operators and owners in North America, primarily transmission system owner/operators. Physical security standards are codified in the Critical Infrastructure Protection (CIP) set of standards [21]. CIP standards cover physical and cyber security. Since there is no UK or European wide security standard specific to the transmission system and control centers, the CIP standards represent best practice for transmission operators for standards of cyber physical security that can be used for comparison purposes.

CIP-014-02 Physical Security

The standard for physical security is CIP-014-02 [22]. A full analysis or replication of the standard is not required in this report, however the standard addresses key requirements and measures for transmission facilities (including HV transmission equipment and control centers), including detailing the requirements for:

- Risk assessment (and third party verification of the risk assessment) of transmission facilities and control centers that if rendered inoperable could result in uncontrolled separation or a cascading system incident.
- Evaluation of the potential threats and vulnerabilities including the unique characteristics of the facilities based on prior experience or external threat warning information.
- A documented physical security plan (to be verified by a third party) should be developed and maintained for the transmission facilities to include resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats.
- Law enforcement contact and coordination information.
- A timeline for executing the physical security enhancements and modifications specified in the physical security plan.
- Provisions to evaluate evolving physical threats, and their corresponding security measures, to the transmission station(s), transmission substation(s), or primary control center(s).

CIP 002-05-1a Cyber Security — BES Cyber System Categorization

This standard details the process for classifying and categorizing the cyber system. All equipment can be classified as either Electronic Access Control of Monitoring System (EACMS), Physical Access Control System (PACS) or Protected Cyber Assets (PCA). All assets should be further classified by impact rating based on the functional role of the control center. The impact ratings are High, Medium and Low.

All control centers must categorize their cyber equipment and the impact category, if the equipment gets compromised.

CIP 005-05 – Cyber Security Electronic Security Perimeter

This standard mandates that all applicable cyber assets connected to a network via a routable protocol shall reside within a defined Electronic Security Perimeter (ESP) and all External Routable Connectivity must be through an identified Electronic Access Point (EAP).

CIP 006-06-2 – Physical Security of Cyber Assets

The stated purpose of CIP 006-06-2 is "To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES." Depending on the categorization of equipment in CIP 002-05-1a, for all medium and high impact cyber assets, transmission operators are required to develop a physical security plan with at least the requirements documented in Table 5-2 for all control centers, to ensure safety and to mitigate risks. These are listed not as specific requirements that SHET should implement in the existing or new control centers, but as a guide to best practices and standards on an electricity system that is not quite equivalent, but similar in nature. This table can also be populated by SHET group security, as required.

Table 5-2 CIP 006-06-2 requirements and how they would potentially relate to the SHET control center

Requirement Number	CIP 006-06-2 Requirements	Implemented in Current SHET CC	Plan to implement in new SHET CC
1.1	Define operational or procedural controls to restrict physical access		
1.2	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.		
1.3	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.		
1.4	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.		
1.5	Issue an alarm or alert in response to detected unauthorized access through a physical access point into		

	a Physical Security Perimeter to the appropriate personnel		
1.6	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.		
1.7	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.		
1.8	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry. And retain for at least 90 days.		
1.10	Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.		
2.1	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.		
2.2, 2.3	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances. Retain for at least 90 days		

3.1	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly		

CIP 007-06 — Cyber Security – Systems Security Management

The aim of CIP-007-06 on system security management for cyber security assets in control centers is "to manage system security by specifying select technical, operational, and procedural requirements in support of protecting Bulk Electric System (BES) Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)."

The requirements listed Table 5-3 are for all functional entities with high or medium impact cyber assets, specifically related to transmission owner/operators with a control center. These are listed not as specific requirements that SHET should implement in the existing or new control centers, but as a guide to best practices and standards on an electricity system that is not quite equivalent, but similar in nature. This table can also be populated by SHET group security, as required.

Table 5-3 CIP 007-06 Requirements and how they relate to the proposed new SHET CC.

Req. #	CIP 007-06 Requirements	Implemented in SHET CR	Plan to implement in new SHET CR
1.1	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device, then those ports that are open are deemed needed.		
1.2	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media		
2.1	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.		

2.2	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.		
2.3	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations		
2.4	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate		
3.1, 3.2	Deploy method(s) to deter, detect, or prevent malicious code. Mitigate the threat of detected malicious code.		
3.3	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.		
4.1, 4.3	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code. Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.		
4.2	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum,		

	each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.		
4.4	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.		
5.1	Have a method(s) to enforce authentication of interactive user access, where technically feasible.		
5.2	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).		
5.3	Identify individuals who have authorized access to shared accounts.		
5.4	Change known default passwords, per Cyber Asset capability		
5.5	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, nonalphanumeric) or the maximum complexity supported by the Cyber Asset.		
5.6	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.		
5.7	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.		

Other CIP Standards

The remaining CIP standards are important for the management and ongoing implementation of cyber / physical security in a control center but are less relevant for detailed description in this report. They are listed below for reference and the most up to date version of the standards can be accessed from the NERC website [21].

- CIP-003-8 Cyber Security - Security Management Controls
- CIP-004-6 Cyber Security - Personnel & Training
- CIP-008-5 Cyber Security - Incident Reporting and Response Planning
- CIP-009-6 Cyber Security - Recovery Plans for BES Cyber Systems
- CIP- 010-2 Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-011-2 Cyber Security - Information Protection

ISA/IEC 62443

The most widely used standard for cyber security in Europe is the ISA/IEC 62443 . This was developed with focus on manufacturing and process plants but has broad applicability and adoption by European electricity system operators. The standard provides a widely recognised framework for detecting and mitigating cyber security vulnerabilities. The standard is composed of four main and separate parts. General – (Part 1), policies and procedures (part 2), system (part 3) and components (part 4).

Each part has sub-parts and associated standards documents, that fully describe aspects of cyber security for large scale industrial automation and control systems and control centers. Important standards within the framework are generally considered to be:

- IEC 62443-2-4, which covers the policies and practices for system integration
- IEC 62443-4-1, which covers the secure development lifecycle requirements
- IEC 62443-4-2, which covers the IACS components security specifications
- IEC 62443-3-3, which covers the security requirements and the security levels

There are many vendors who will aim to certify systems to the standard sin ISA/IEC 62443, achieving and maintain certification is a key component of cyber security and protection in control centers.

Environmental Considerations for Building

The control centre building should be built in a location that is safe from natural disasters such as

- Flooding caused by burst riverbanks or excessive rain
- Wind
- Lightning
- Hurricane, tropical storms

The control center and cyber assets should be located so as not to be compromised by any of the above naturally occurring disasters.

Summary

Due to the nature of the facility at Inveralmond house, maintaining cyber / physical security at both the main control room and at the backup at Buroughmuir can be a challenge, and presents risks to the resilience of the system. In this chapter some of the risks as documented by CPNI were highlighted as well as some of the mitigations that can be used to offset the risks. As the facilities are transmission control centers, they will likely have to be upgraded to CPNI security standards since they need a heightened level of security for the protection of critically important system assets in the UK. The evaluation process is ongoing.

The CIP standards for North American TSOs are the best available, publicly available standards specifically for the physical and cyber security of transmission system control centers. The requirements are outlined in the chapter as part of a gap analysis with the current and future control centers to be assessed by SSE group security,

The current threat is classified as substantial by CPNI, all means necessary should be put in place in the control center to mitigate any risks to the cyber physical security of the sites.

6 CONTROL CENTER OPERATOR TRAINING

Best Practice Operator Training Programmes

Best practice operator training programmes for transmission system operators around the world require a programme of training which includes both:

- Initial training
- Continuous training

European System Operator Guideline (SOGL), which in 2020 are binding on transmission operators and owners in the UK [23] mandate that the program be composed of at least:

1. A description of the transmission system elements
2. Operation of the transmission system in all system states including restoration
3. Use of the on-the-job systems and processes
4. Coordination of inter-TSO operations and market arrangements
5. Recognition of, and response to, exceptional operational situations
6. Relevant areas of electrical power engineering
7. Relevant aspects of the (GB) internal electricity market
8. Relevant aspects of the network codes or guidelines
9. Safety and security of persons, nuclear and other equipment in transmission system operation
10. Inter-TSO cooperation and coordination in real-time operation and in operational planning at the level of main control rooms which shall be given in English unless otherwise specified
11. Joint training with transmission-connected DSOs and significant grid users, where appropriate. Including training on interoperability issues and shall include preparation and activation of coordinated remedial actions if applicable.
12. Behavioral skills with particular focus on stress management, humans acting in critical situation, responsibility and motivation skills
13. Operational planning practices and tools, including those used with the relevant regional security coordinators in the operational planning.

Training programmes should be updated at **least annually or following significant system changes or to reflect changing operational circumstances**, market rules network configuration and system characteristics (such as generation, demand patterns and market evolution)

The training programs should award certification to operators on an annual basis for completion of the initial or continuous training program.

SHET Training

At present training times for SHET team members require 6 – 12 months to achieve a first level authorisation. Senior roles within SHET control center require 2 – 3 years on top of this. There is

no dedicated simulator or specific training classroom environment and most training is on the job training.

STCP-006-001

Section 3.6 of the STCP-006 covers Black Start Training, stating that

"NGESO shall carry out and make available appropriate and regular training for TO staff, to allow them to carry out their roles and responsibilities under a Black Start condition. The TO shall make available appropriately skilled personnel to complete the prescribed Black Start training"

The ability to train for a blackstart and restoration scenario would be significantly enhanced by a utilizing a modern DTS facility.

Training Methods

The most common approaches to operator training in transmission control involves:

- On-the-job training (OJT)
- Classroom based training
- Simulation exercises based on realistic scenarios, including blackstart and restoration, contingency events.

On-the-job training means to shadow or sit next to a working, experienced operator as they perform their tasks on the power system in real time. Since this is the most tried and trusted method of training it is considered the most effective for normal, everyday operator tasks.

Skill-based behaviour refers to operations that follow trends or alarms with automatic responses for example responding to a voltage trend or acknowledging an alarm.

Rule based behaviour refers to operations that follow rules or procedures, such as switching plans or test checklists.

Knowledge based behaviour involves cognitively assessing options, predicting consequences and make decisions in real time without an appreciation for the results. It is the most cognitively intensive form of work in a control center and can likely only be trained for with a DTS. Knowledge based behaviour is required for unanticipated, unfamiliar events.

The ultimate aim of training is to ensure they are comfortable with both familiar and unfamiliar events. However, within the familiar and unfamiliar categories, since the vast majority of time is spent on normal operations, it is most likely that OJT covers anticipated events only, such as switching on the system or responding to normal operation events such as a trip-reclose events, or asset health alarms.

Simulator training is more commonly used to test operator's response to **unanticipated** events

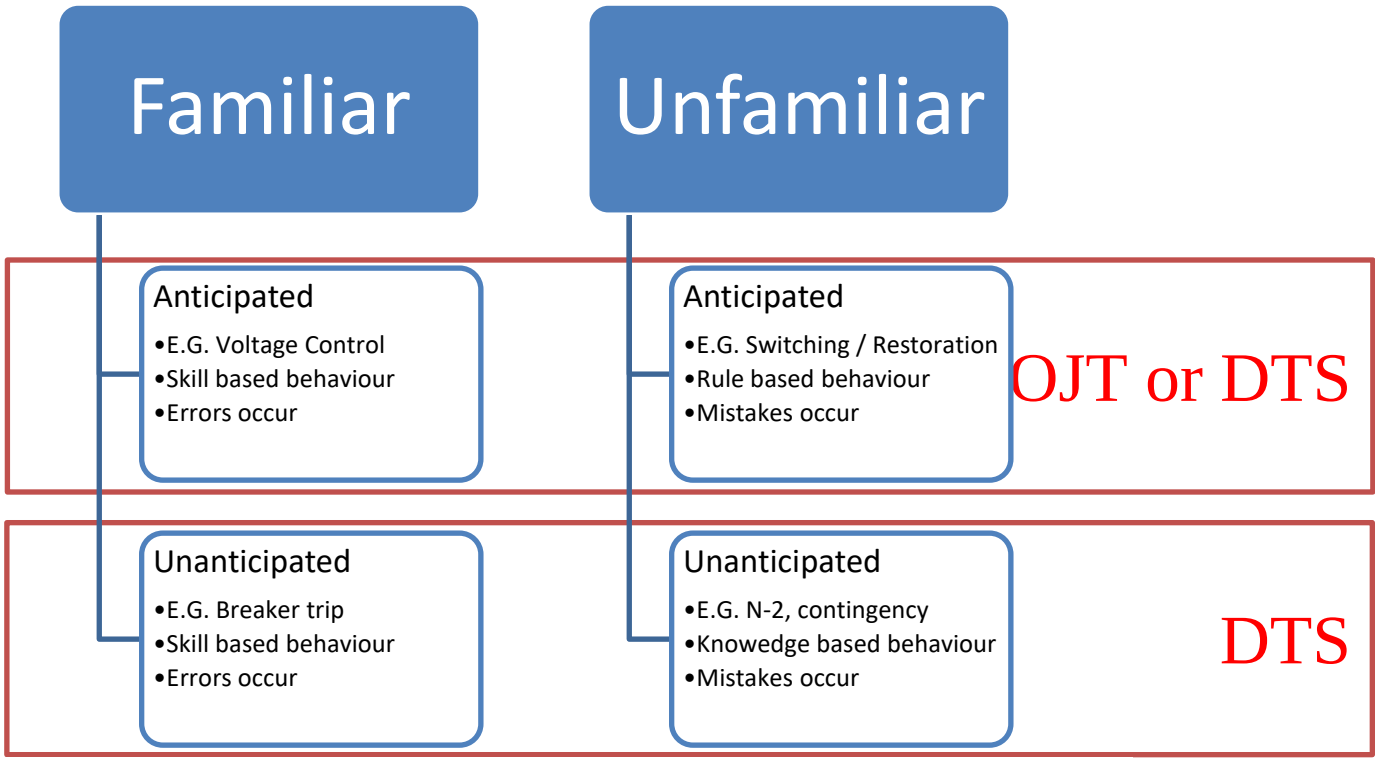

Figure 6-1 Graphic illustrating the scenarios faced by operators in RT operations and the most appropriate training types

(events that occur on the system but are less likely to occur during OJT). Unfamiliar / unanticipated events must be trained using a simulator, since the severity of the event cannot be worked through in real time. These events include switching restoration, blackstart, N-2 outages etc. Mistakes tend to occur during unfamiliar unanticipated events where operators must make decisions without the aid of procedures or previous experience. Testing for and evaluating these mistakes in a simulator is the ultimate aim of training.

Dispatcher Training Simulator

The vast majority of transmission system operators around the world utilize a Dispatcher Training Simulator (DTS). This is a room similar in nature and layout, but smaller, than the control center, which is intended to be a shadow operations center, used specifically for training operators. The desk, screens layout etc. is intended to be mimic real time operation and to be familiar to the operator so as to be as close to reality as possible.

The facility is known at the DTS, but the software deployed is many cases similar or identical to the real time SCADA / EMS. EMS vendors offer modules of the base system as a DTS package for use in training but there are other vendors that offer standalone training software using a model of the system being trained on. (E.G IncSys, Dutrain)

One of the difficulties in training is to develop the case within the software that is suitably realistic and to make the simulator work effectively for the operators as they respond to the simulated event. Currently trainers require a number of additional personnel in a “shadow” room to the DTS to

control the simulation, provide feedback, answer calls during a training session, depending on how many operators are being trained at the time.

For example, a blackstart simulation exercise will require multiple operators in the DTS piecing the network together, making phone calls and other coordination. This requires an equivalent number of training staff to effectively manage the simulation. Training in a simulator is not a straightforward exercise, having a fit-for-purpose simulator environment will help to ensure initial and continuous training and certification is maintained to the highest standard. This will be more necessary than ever as the system evolves

Challenges with Training for the Future System

One of the challenges of modern operator training is the challenge of identifying realistic operations scenarios and making them work in the DTS software model. In the past, the failure modes of a power system may have been relatively easy to identify, e.g. near a large nuclear facility or busbar fault. However, as the system has evolved, the failure modes are impossible to identify, and OJT training is not adequate for this.

A good example is the August 2019 incident in GB. This was an N-1-G-G event caused by issues at a generator and windfarm. This means the normal system was disturbed by a lightning strike trip-reclose (familiar-unanticipated) followed by the loss of two generators (unfamiliar-unanticipated). While operators responded adequately to this event, training for this would have to have been carried out in a DTS since OJT training would never have thrown up an event similar to it in nature. This emphasizes the need for a DTS facility to ensure operators are trained for these types of events.

Likely Increase in High Impact Low frequency Events

The GB 2019 event is unlikely to be a one-off major system disturbance for a number of reasons:

- The move to decentralized power sources such as distributed energy resources (DER), over large centralised power sources.
    - This is reinforced by the NGESO initiative to use DER in the blackstart and restoration process [24]
- The decrease in stability, primarily frequency stability, as a result of lowering inertia is likely to result in weaker transmission grids, especially grids like SHET with higher renewables and high transfers across its boundaries.
    - This is reinforced by the NGESO initiative on the stability pathfinder project to improve stability across the GB system [25].
- Increased climactic activity as a result of climate disruption, there will likely be an increase in storms, high wind events, flooding, etc these will all cause an increase in events impacting the transmission system in Scotland and GB.
- The increase in Active Network Management, power electronic devices such as HVDC, flexible AC transmission devices (FACTS) on the system and active network managers will likely have an impact on future grid stability. This is due to how different control modes interacting causing previously unseen or under-modelled failure modes to manifest themselves.

Pandemic Training Issues

During the 2020 pandemic for COVID-19, training became a very important issue facing transmission operators for a number of reasons:

- The likelihood of an outbreak amongst operator shift staff crews, would render the system potentially at risk due to the highly skilled nature of grid operation.
    - If one operator tested positive the other crew members may have to quarantine. This could only be sustained for a few cases before operations was untenable.
- There may not have been adequate cover from backup operators, so previous operators who had previously worked shift but had let their certification lapse were drafted in to cover.
- On the Job training was severely impacted, since sitting and working in close proximity to the already system-critical staff was restricted.
- Computer based training programmes were not set up for training in a pandemic or were inadequate for the task at hand.

The DTS proved very effective for system operators during the pandemic. For a number of reasons

1. Since it is set up to mimic the real control center it can also be used as a shadow control center in real time, where the EMS can be deployed within the DTS instead of the training software.
2. It is usually already within the cyber/physical security perimeter (which is the intention with the new SHET control center) so there are no extra security requirements needed to staff the DTS.
3. It can be used as a method of OJT training without in-person contact. Operators can be trained on the real system in real time (by the trainers, with communication to real operators if required). Operators cannot interact with the system but can observe in real time the normal, familiar system operations tasks.
4. It is an effective classroom type environment where it is set up for demonstrations by the trainer on screens and DTS can usually accommodate multiple people at a time.

Summary

Training is a critically important aspect to the resilience of the transmission system and its operators. An integrated approach to training is essential. This should include a program of initial and continuous training to meet the needs of operating the evolving system, as well as simulator training and on the job training. This chapter discussed the need for a structured training program, the methods of training and the types of training required. DTS and the difficulty in training for the future system and the increased likelihood of an increase in HILF events were also addressed. The key points related to training were:

- A dedicated training program and certification is required for all system operators by European regulation. There is a list of topics that must be covered within the training programme listed in this chapter.
- Training programmes need to be structured, as both initial and continuous.
- Training programmes need to be reviewed regularly in light of the changing system

- OJT training is suitable for anticipated events both familiar and unfamiliar. DTS training is required for unanticipated events on the system both familiar and unfamiliar.
    - It is difficult to train operators OJT for unanticipated events
    - It is possible to train operators in the DTS for all categories of events (but not all events)
- The vast majority of transmission system operators around the world have a DTS environment for training operators either on-premises or in the backup facility.
- Unanticipated “high impact low frequency” events are going to become more common for many reasons in the future, continuous training is essential to avoid major incidents or to improve response to incidents when they occur
- A DTS within the control center facility provides the flexibility to offer a specialist environment for training that can be used for both OJT and simulator-based training (tests), as well as a backup room for operation of the system if required.
- OJT training may become difficult or impossible in the context of pandemics, where physical distance is required to be maintained. A DTS can be effective for OJT training and classroom-based teaching as well as simulation exercises.
- As a recent concrete example, during the recent COVID-19 pandemic, many system operators used their DTS as a backup facility within the security perimeter or for training operators using OJT methods on the real system in real time and for actually operating the system.

7 BLACKSTART ON THE SHET SYSTEM

Specific Needs for Blackstart

Preparing for the worst case scenario is a key element of effective resilience planning and operations. It is likely that a blackstart scenario would be the worst case scenario faced by system operators and SHET is no different. There are a range of specific needs for a blackstart / restoration scenario that should be in place for all transmission system operators which will be discussed in this chapter. Three key aspects to be discussed in detail are:

1. Training for blackstart with a simulator and coordinated training
2. Situational awareness of the distressed system
3. Facilities for lodging, rest and refreshment

Training for Blackstart

As discussed in Chapter 6, a dedicated training programme for unanticipated events can only be carried out using a dispatcher training simulator (DTS) where the pre-planned event can be modelled, and trainers can control the environment and test for errors. Having a DTS that is linked or integrated with the control center is very beneficial for this type of training, Since blackstart training cannot be carried out on the job, simulator and classroom training is the most commonly used approach around the world.

Another aspect of blackstart training is the coordination with other facilities and stakeholders. In the SHET case these would be, primarily NGESO, SHEPD, generators, gas companies, wind farm operators, and government. Carrying out these multi-sectoral cross-functional training exercises, with a simulator and meeting rooms are a useful way of preparing for the worst-case scenario. NGESO recommend 3 year refresh training in blackstart for all certified operators, but the method is not clear. NG ESO also state in STCP-006-1 that they will carry out blackstart training and make this available to TO staff.

Situational Awareness of the Destressed System

When the system is blacked out, SHET must act as the system operator for the footprint, including starting generation, balancing the island and coordinating with distribution system operators and NGESO. To perform this level of functionality, a wide-area Tier 1 (see chapter 4) display of the system and its key parameters would be required. This is so that operators, ordinarily unfamiliar with balancing and restoration can have a wide area view of the system and for their own situational awareness. The facilities in Inveralmond house would not be effective or adequate for the task of operating a blacked-out island system or restoring a large part of the network, due to lack of overview displays and lack of coordination room facilities.

Facilities for Lodging

In the event of a blackstart in any system, the likelihood is that restoring the system will take many hours to fully complete. Experience shows that the operators who are working in the control rooms to restore blacked out system spend many hours in position and work closely with all staff to get the system restored as soon as possible. Restoration can last days in the worst case scenario. Having lodging facilities for operators on-site is a very useful facility, to allow operators who may be working many hours on-site over many days can rest between shifts. Having adequate kitchen facilities for food preparation is also an important aspect that goes hand in hand with lodging facilities.

Other Aspects of Blackstart

Other key aspects of an effective blackstart plan and facility are:

- Highly Resilient Communications
    - To NGESO, DSOs, Generators and also the network for switching
- Storage Facilities
    - For exigencies related to overnight lodging, food etc.
- Incident Management Facilities
    - The blackstart and restoration will have to be managed by senior management in a Gold incident command and control structure. Communications with the outside world are also needed and if possible, these elements should be shielded from real time operators who will be busy restoring the system.
    - Having adequate meeting room facilities, in close proximity to the control is critical to allow close coordination, instant accurate updates and guidance provision.

Summary

Blackstart and restoration is a key function to be carried out by a resilient transmission system operator. The three most important aspects of blackstart planning and management are:

- Training for blackstart with a simulator and coordinated training with other associated entities.
- Situational awareness of the destressed system,
- Facilities for lodging, rest and refreshment.

The needs for all three are discussed in this chapter. Any future resilient control and operations center should incorporate these needs to manage high impact low frequency emergency events like blackstart. Being prepared and trained in advance of emergencies is crucial to safe secure and economically optimal restoration, ensuring customers are without power for the minimum possible time.

8 SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

The SHET proposal to Ofgem as part of the RIIO ET2 submission for a new Resilience Operations Center was rejected following an analysis of the EJP. Following a review and parsing the information from the review documents, the proposed resilience operations center project was most likely rejected primarily due to:

- **A lack of justification of needs**
- **The proposed solution was disproportionate to the needs identified.**

When assessing the response to the EJP, it was clear that a more detailed justification of the needs for a new control center was required. Chapter 2 assessed the actual requirements for a control room to operate effectively in the GB system. It assessed the current control room environment and facilities, in consultation with SHET engineers and also the future needs of a control center to manage and operate the system of the future. A gap analysis was conducted, comparing actual needs to operate effectively, limitations of the current facility and the likely future needs.

When assessing the needs and justification as well as the proportionality of the solution, it is essential to assess the risks of maintaining operations from the current facilities. This would essentially be the "Do Nothing" case. Chapter 3 highlighted some of the key risks to maintaining operations at current main and backup facilities as they are today around the broad topics of safety, security, system security and cost.

The most commonly used models of situational awareness emphasize the need to observe the current status of the system or perceive the system at it currently stands. As it's the first step in the framework, this is arguably the most important aspect of real time operations of system critical grids. Observing or perceiving the system with a wide-area overview is a key element of best practice human interface display design which has a hierarchical approach to displaying information. Tier 1 is at the top of the hierarchy. Tier 1 displays should have a wide area overview of the transmission system as well as key indicators of system status.

Due to the nature of the facility at Inveralmond house, maintaining cyber / physical security at both the main control room and at the backup at Buroughmuir can be a challenge, and presents risks to the resilience of the system. Chapter 5 contains some of the risks as documented by CPNI as well as some of the mitigations that can be used to offset the risks. As the facilities are transmission control centers, they will likely have to be upgraded to CPNI security standards since they need a heightened level of security for the protection of critically important system assets in the UK. The evaluation process is ongoing.

Training is a critically important aspect to the resilience of the transmission system and its operators. An integrated approach to training including a program of initial and continuous training to meet the needs of operating the evolving system, as well as simulator training and on the job, training are foundational elements of any training programme.

Blackstart planning is a key element of a resilient transmission system operator. The three most important aspects of blackstart planning and management are: Training for blackstart with a simulator and coordinated training, situational awareness of the destressed system, and facilities for lodging, rest and refreshment. These are documented in Chapter 7.

By assessing why, the proposal for a new resilience control center was rejected and then identifying the needs and risks associated with both the new facility and retaining the existing facilities there is strong justification that a new control center facility would improve resiliency for operating the SHET system. This increased resiliency of the power system and the business over the long run should improve the reliability of the system, reduce human error and safety incidents and provide consequent benefits to all electricity customers.

9 REFERENCES

[1] SSEN, "Engineering Justification Paper Resilience - Operations Centre - T2BP-EJP-0003," SSEN, 2019.

[2] EQ Communications, "SHE Transmission Operations Stakeholder Workshop," EQ Communications, 2019.

[3] Atkins, SNC Lavalin on behalf of Ofgem, "RIIO-T2 TO Submission Review Summary Report," Atkins, London, 2020.

[4] Ofgem, "Consultation - RIIO-2 Draft Determinations – Scottish Hydro Electric Transmission," Ofgem, London, 2020.

[5] Ofgem, "RIIO-2 Draft Determinations - Electricity Transmission Annex," Ofgem, London, 2020.

[6] L. W. Efthymios Karangelos, "From reliability and resilience towards a holistic approach to power system risk management," in *Electric Power Control Centers 2010*, Reykjavik, 2019.

[7] Andy Ott, "Reliability and Resilience: Different Concepts, Common Goals," PJM, [Online]. Available: https://insidelines.pjm.com/reliability-and-resilience-different-concepts-common-goals/. [Accessed July 31 2020].

[8] Ofgem, "TRANSMISSION LICENCE STANDARD CONDITIONS," Ofgem, London, 2020.

[9] National Grid ESO, "Future Energy Scenarios - July 2020," National Gid, London, 2020.

[10] Scottish Government, "Scottish Energy Strategy - The future of energy in Scotland," Scottish Goverment, Edinburgh, 2017.

[11] M. Endsley and D. Jones, Designing for Situation Awareness (Second ed.)., CRC Press, 2016.

[12] F. Osinga, Science, Strategy and War - The Strategic Theory of John Boyd, The Netherlands: Eburon Academic Publishers, 2005.

[13] ISA, "ANSI/ISA 101.01-2015 Hunman Machine Interfaces for Process Automation Systems," ISA, 2015.

[14] B. Hollifield, D. Oliver, I. Nimmo and E. Habibi, The High Performance HMI Handbook: A Comprehensive Guide to Designing, Implementing, and Maintaining Effective HMIs for Industrial Plant Operations, Houston, TX: PAS Inc., 2008.

[15] Health and Safety Executive UK, "Working safely with display screen equipment," Health and Safety Executive UK, [Online]. Available: https://www.hse.gov.uk/msd/dse/assessment.htm. [Accessed 29 July 2020].

[16] Elia Group, "Advanced Machine Learning to support dispatching," Elia Group, [Online]. Available: https://innovation.eliagroup.eu/projects/advanced-machine-learning-to-support-dispatching/. [Accessed 29 July 2020].

[17] J. Reason, "Human Error," Cambridge, Cambridge University Press, 1990.

[18] R. F. Matthew Grissinger, "Sidetracks on the Safety Express - Interruptions Lead to Errors and … Wait, What Was I Doing?," Pharmacy and Technology Journal, 2015.

[19] Ofgem, "Physical Security Upgrade Programme submission May 2018," Ofgem, London, 2018.

[20] Centre for Protection of National Infrastructure, "Physical Security," Centre for Protection of National Infrastructure, [Online]. Available: https://www.cpni.gov.uk/physical-security. [Accessed 20 July 2020].

[21] NERC - North American Reliability Corporation, "CIP Standards," [Online]. Available: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx. [Accessed 20 07 2020].

[22] NERC - North American Reliability Corporation, "CIP-014-2 — Physical Security," NERC - North American Reliability Corporation, Atlanta, GA, 2014.

[23] European Commission , "Commission Regulation (EU) 2017/1485 establishing a guideline on electricity transmission system operation," European Commission, Brusells, 2017.

[24] N. G. ESO, "Distributed ReStart Project," NG ESO, [Online]. Available: https://www.nationalgrideso.com/future-energy/projects/distributed-restart. [Accessed 12 08 2020].

[25] National Grid ESO, "Stability Pathfinder Project launch," NG ESO, [Online]. Available: https://www.nationalgrideso.com/media-test/national-grid-eso-launch-stability-pathfinder-phase-one. [Accessed 12 08 2020].

[26] National Grid ESO, "Future Energy Scenarios 2019," National Grid, London, 2019.

[27] Ernst & Young, "1. Deficiency in training oeprators for unanticipated events will result in delays in restoration or inadequate response.," Ernst & Young, London, 2018.

[28] J. Rasmussen and V. K, "Ecological Interface Design: Theoretical Foundations," *Trasnactions on Systems Man and Cybernetics*, vol. 22, no. 4, pp. 589-607, 1992.

A PICTORIAL EXAMPLES OF CONTROL CENTERS

What are examples of other control centers for similarly sized transmission owner/operators.

Figure 9-1 Ireland [Source: https://www.irishtimes.com/news/environment/inside-eirgrid-s-energy-control-centre-1.3560099]

Figure 9-2 National Grid ESO [Source: https://www.ft.com/content/49d94586-bb47-11e9-b350-db00d509634e]

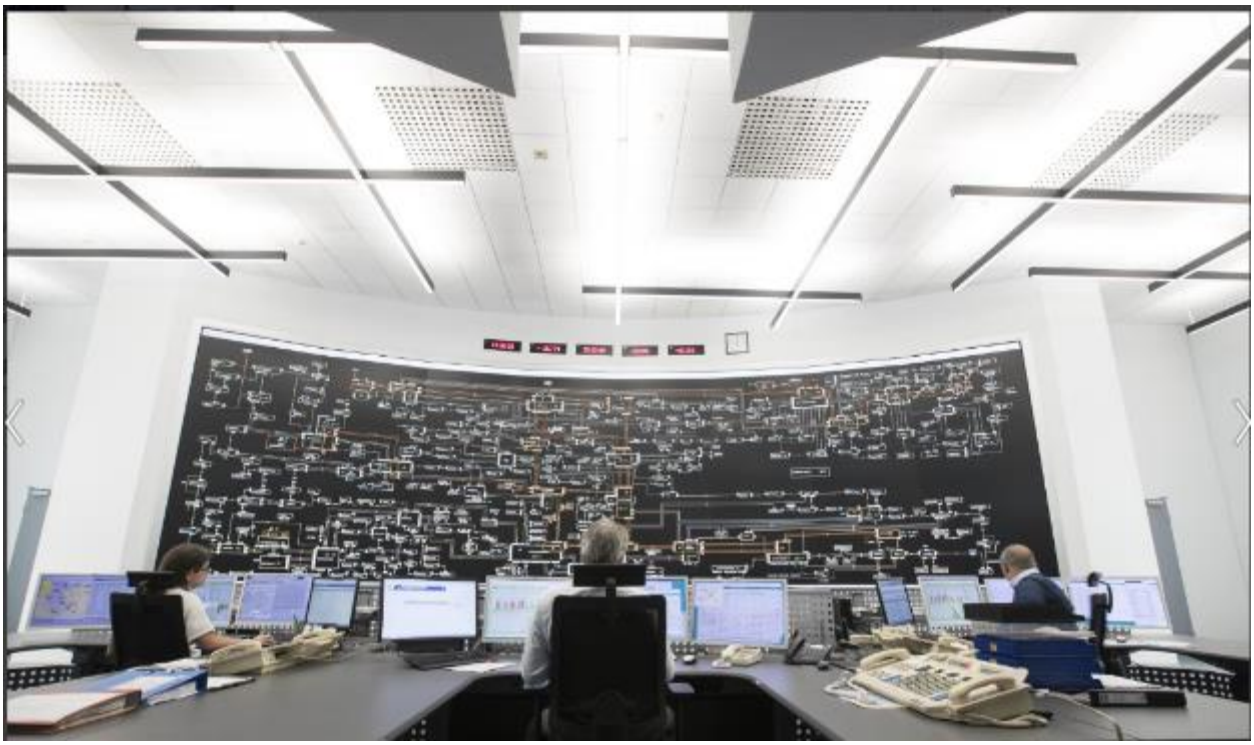

Figure 9-3 Greece IPTO [Source: https://www.linkedin.com/posts/ipto-admie_covid19-ipto-teleworking-activity-6648836875056480256-9K54/]

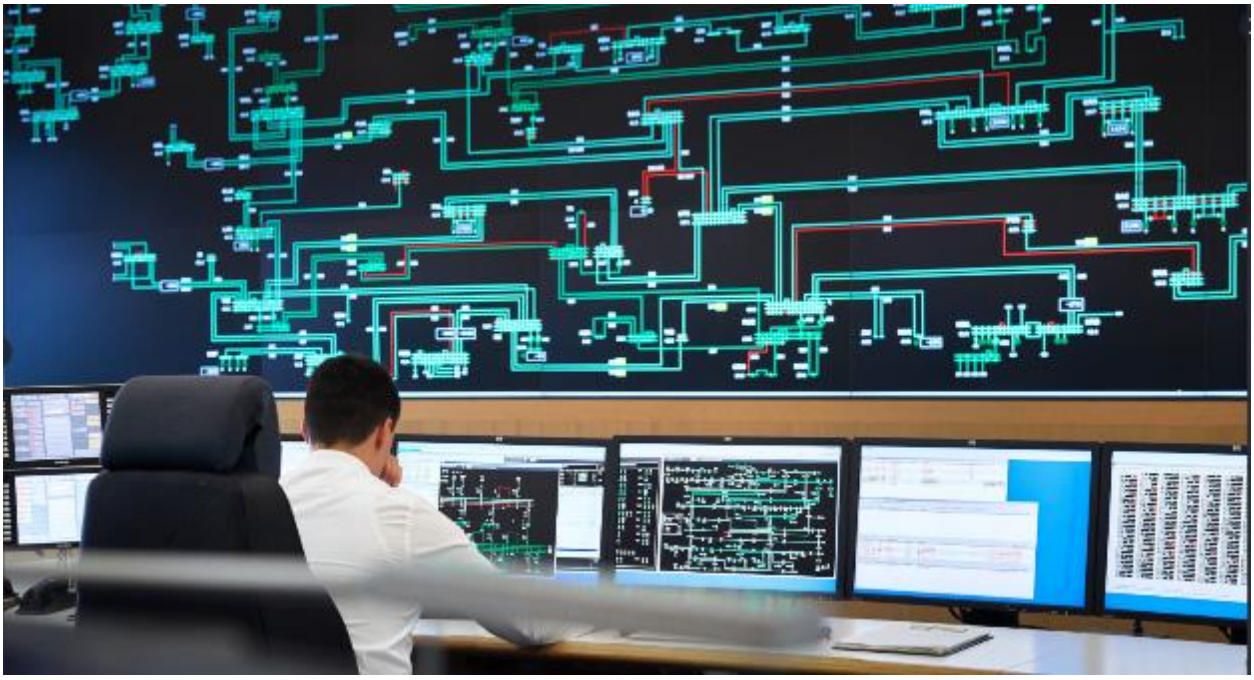

Figure 9-4 Germany 50 Hertz [Source: https://www.50hertz.com/en/Grid/Systemcontrol

Figure 9-5 Hungary [Source: https://www.linkedin.com/posts/mavir-hungarian-transmission-operator-co._tekintsd-meg-leg%C3%BAjabb-nyitott-poz%C3%ADci%C3%B3inkat-activity-6692366634625064960-pzZU/]

Figure 9-6 Denmark [Source: https://www.linkedin.com/posts/energinet-dk_jobienerginet-energinet-ingeniaeor-activity-6649232230151401472-9mob]

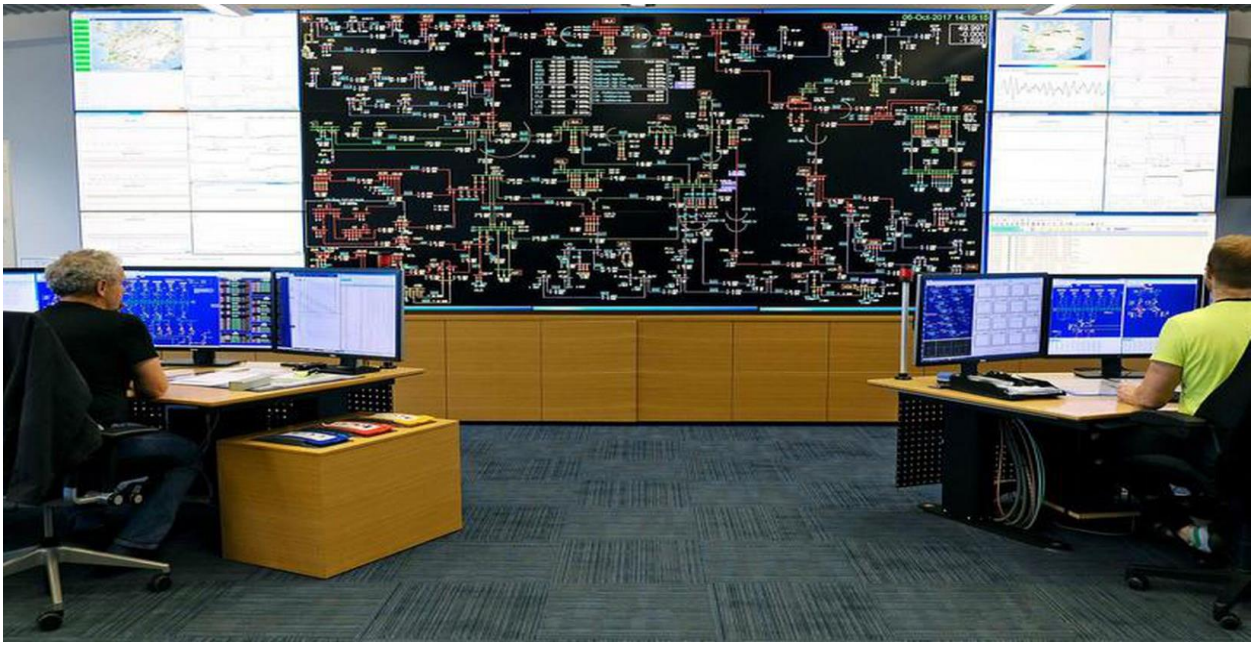

Figure 9-7 Iceland [Source: https://www.mbl.is/frettir/innlent/2017/10/12/kisilver_hafa_kuvent_umraedunni/]

Figure 9-8 SONI Northern Ireland [Source: https://www.irishnews.com/business/2019/01/31/news/renewable-energy-now-accounts-for-36-per-cent-of-north-s-electricity-demand-1541125/]

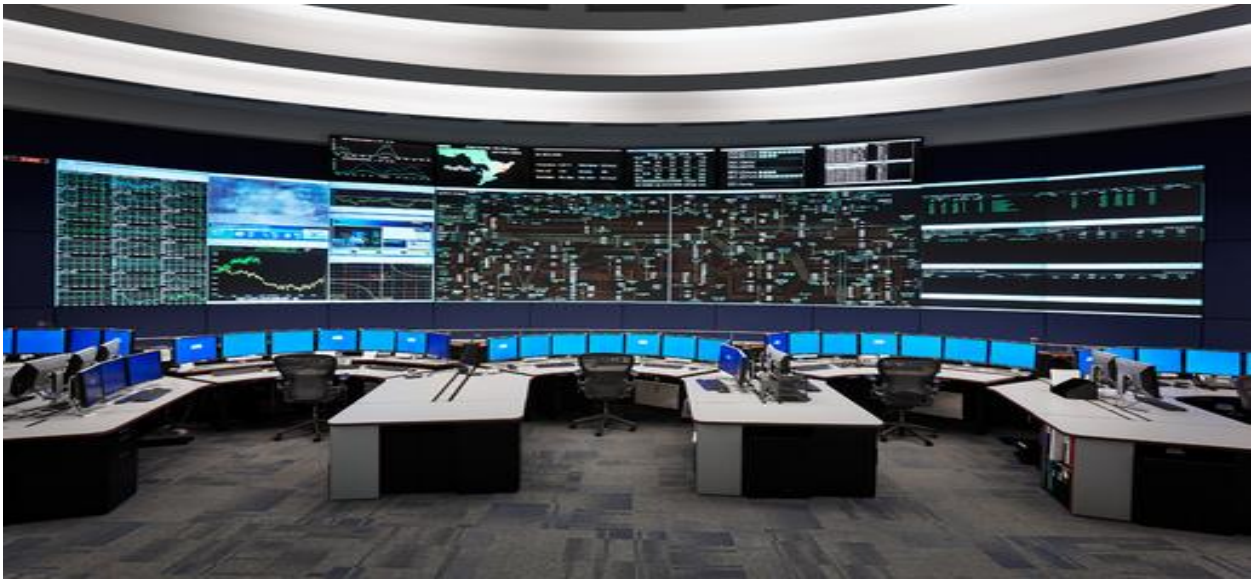

Figure 9-9 IESO Canada [Source: https://www.appliedelectronics.com/ieso-network-control]

B SPACE COMPARISONS OF SIMILAR CONTROL CENTERS

When assessing the space needs for a new control center facility, it is worthwhile to compare similar control center facilities in Europe, to assess how they operate in their control centers. What the space requirements for videowalls and desk space might be. This exercise is also useful for comparing proposed plans for the new facility to see if it matches with international best practice for control centers.

An assessment of 16 similar control centers from Europe was made and is shown in Table 9-1 below. Based on a visual assessment of publicly available images and based on some experience of visiting control centers, the average number of desks is approximately 9, the average video wall width is approximately 18 meters and videowall height is approximately 5 meters.

Table 9-1 Table of Control Center in Europe comparisons of video wall and console desk numbers

		Segregated Control Room	Number of Screens per Desk	Videowall Width (meters Approx.)	Videowall Height (meters Approx.)
Ireland	**EirGrid**	YES	12	6	2
Northern Ireland	**SONI**	YES	10	8	3
Scotland	**Scottish Power**	NO		10	2
England	**National Grid ESO**	YES	8	20	5
Iceland	**Landsnet**	Yes	6	10	3
Portugal	**Ren**	Yes	6	15	3
Belgium	**Elia**	Yes	10	30	5
Denmark	**EnergiNet**	Yes	7	30	5
Germany	**Transnet**	Yes	10	25	6
Spain	**Red Eléctrica**	Yes	7	25	4
Switzerland	**Swissgrid**	Yes	8	15	3
Greece	**IPTO**	Yes	4	20	6
Germany	**Amprion**	Yes	15	20	4
France	**RTE**	Yes	8	10	10
Italy	**Terna**	Yes	8	20	8
Sweden	**SVK**	Yes	12	N/A	N/A
Average			**9**	**18**	**5**