# From integrated operations to remote operations: socio-technical challenge for the oil and gas business

Vidar Hepsø[1] and Eric Monteiro[1]

[1] NTNU Norwegian University of Science and Technology, Trondheim, Norway

**Abstract.** Remote operations started with integrated operations (IO) some years ago where designated tasks and roles were shifted from off- to onshore. Remote operations, however, is more than remote control as the operational model or concept is key: it defines the scope for the tasks to be conducted remotely. With this increased ambition and scope, sociotechnical concerns play an increasingly important role. With increased autonomy and automation in the oil and gas business, the reliance upon digital representations of the process conditions that the center/ control room follow up becomes more complex, technically but not the least organizationally and institutionally. Operational, organizational and information infrastructure issues are key considerations for remote operation including employer-employee relationships and collaboration with vendors. How will these new centers differ from traditional control rooms and the previous generation of collaboration centers that came with integrated operations 10-15 years ago? What are the key capabilities around which you build scalability and replicability in the design of such control centers? We discuss and empirically illustrate different configurations of remote operations.

**Keywords:** control room, remote operations, integrated operations, information infrastructures, autonomy, operational model, center of calculation

## 1 Introduction

Technologies for collaboration within the oil and gas industry Integrated Operations (IO), allowed real-time data sharing between remote locations that challenged traditional geographical, disciplinary, and organizational boundaries [1]. According to the Norwegian oil industry association (OLF) [2] the first generation (G1) processes would integrate processes and people onshore and offshore using ICT solutions and facilities that improve onshore's ability to support offshore operationally. The second generation (G2) processes would help operators utilize vendors' core competencies and service more efficiently. Utilizing digital services and vendor products, operators would be able to update reservoir models, drilling targets and well trajectories as wells are drilled, manage well completions remotely, optimize production from reservoir to export.

In this paper we address this development of opening of boundaries into ecosystems, from integrated operations to remote operations. This process took many years and we analyze it as an *infrastructuring* process [3,4]. Infrastructuring highlights the ongoing, provisional and contingent work that goes into working infrastructures of IO or remote operations. Working infrastructures share similar properties to ecosystems as they evolve along with their spread. Our analysis of integrated operations and remote operations specifically targets the evolution of emergent infrastructures over time. The key here is to focus on the increasing degree of entanglement of the infrastructure with internal and external stakeholders and agendas [5] in an everchanging ecosystem.

Crucially, an infrastructural perspective on IO emphasizes how collaborative practices are achieved through collections of – rather than singular – artefacts. One of the key components related to IO was the establishment of onshore support centers which enabled companies to move work tasks from offshore platforms to land. To enable such control centers several artefacts and practices were bundled: fiber-optic networks to shore, proper standards for communication and sharing of data, collaboration tools and new work practices and competence. This was a socio-technical bundling that made it possible for local and bounded distinct readings/data to be transferred to any place in a larger ecosystem [6]. Bruno Latour's [7] concept of *centers of calculation* underscores an important precondition to understand the unboundedness that comes with the development of IO and remote operations [8]. Collaboration centers and collaboration rooms were centers of calculation. Our research question is: *How do infrastructuring process transforming IO to remote operations change the content of the centers of calculation?* IO collaboration centers opened bounded offshore sites a process that has expanded with remote operations where boundaries are more obscure and where all control functions ultimately can be operated from anywhere given the proper barriers and cyber security mitigation.

IO grew out of Human Factors work methods and the research and consultants that worked with control room and control center development around the legacy of ISO11064 'Ergonomic design of control centers'. Even though the ISO standard had ways to deal with communication outside the control room, this method was still bounded in space. It was also criticized for not dealing with the change management and the multifaceted stakeholders and challenges that came with IO. It focused to a large extent around the development and construction of a control room, a bounded centre of calculation. Much of the new demand in IO came from understanding collaboration/work and IT support outside the control room, in the interaction between onshore and offshore staff during maintenance and operations and collaboration inside and across company borders more in general. Finally, how the existing situation could be changed through change management. The traditional HF methods could not address the ecosystem perspective and the existing methods were not able to address the dynamic features of the larger ecosystems [9]. New MTO/HF methods and conferences were developed as joint industry/research developments (see example center for integrated operations (https://www.iocenter.no/ and CRIOP (www.criop.sintef.no) to deal with this challenge where HF methods and around risk and change management were incorporated into new frameworks to address the increasing boundaryless features of IO.

However, IO lost remote operation along the way. When Rosendahl and Hepsø [1] co-edited the book on Integrated operations, 2012-2013, remote control had not proven to be as important as heralded, largely due to the socio-technical complexity of operational and technical aspects of remote operations. There were two main lessons that were incorporated according to Edwards[10].

The first was a move from the understanding that the operational model of the installation was a consequence of design, where the operational model was recognized as a precondition for the design rather than the other way around. Linked to the first lessons was a focus on maintenance hours. As Edwards et al argue [10], they are normally a function of how much equipment you have on the installation that will require maintenance. Maintenance hours is a key parameter for how many people you will need to maintain the proper technical condition of the installation. When one was able to combine these two lessons into a profitable business case, the path to remote operations was possible. Edwards [11] describe the road to low manning, remote operation as a configuration of complexity of the installation systems, instrumentation needed to remotely control and a low number of maintenance hours. All these together form a path to an operational model based on remote control.

As a consequence of these two lessons the focus changed from the technical concept of remote control, that includes the technical capabilities that needs to be in place to make remote control possible, to remote operations that is a socio-technical configuration. This is where the operational model/concept is the key and where the technical, organizational and competence capabilities are included in the concept.

## 2 The current centers of calculation

In what follows we describe the main configurations of centers of calculation as they appear with remote operations. We use the IOGP recommended practice as the basis for these types of configurations [11].

### 2.1 Remote onshore control room

This is the first centre of calculation configuration. It can exist in various socio-technical realizations based on instrumentation level, manning and operational principles, installation reliability and maintenance load. It can also operate several installations from the same location regardless of geography. The main control room is located outside the production site boundary and in a safe zone. This location can be far away from the actual production site but is within the premises managed by the company. The primary purpose is to remotely control and operate the production site(s), but it may also include dedicated remote engineering or maintenance rooms. As these connections allow interaction with the production process or equipment, physical access controls are typically strictly enforced. Remote control refers to remote actions such as control commands (including: adjusting plant or equipment operational parameters, set point changes, alarm acknowledgement, manual start/stop commands), set point changes and operations monitoring on detailed graphical displays (e.g., process conditions, equipment status, alarms, errors). Safety functions can also be performed from the remote-control room (such as executing manual shutdowns, operating critical action panels, etc.). Remote control requires read and write access to the system to enable operator interaction with the process and equipment on the production site. There are different preventive controls and recovery preparedness principles/ measures in manned or unmanned situations and if there are people on site, or not. This is sought presented in the four-field table below (Figure 1). This table describes four ideal situations, normal operations vs. emergency and if the installation is manned vs. unmanned installation.

| | **Normal operations** | **Emergency** |
|---|---|---|
| **Manned installation** | • Lean crew close to emergency preparedness requirements<br>• Onshore control room always in control<br>• Can use operators to verify situation in the field | • Traditional onsite emergency organization and roles<br>• Offshore has most functions<br>• Offshore crew can verify situation in the plant, if safe |
| **Unmanned installation** | • Normal situation is unmanned<br>• Onshore control room always in control<br>• Campaign based maintenance and ad-hoc visits when necessary<br>• When unmanned must use instrumentation/ actuators, camera, mobile fixed sensors to verify a situation in the field, ad-hoc shuttling last resort<br>• Crawling, swimming or flying drones for check and report | • During campaigns normal emergency preparedness on site<br>• Unmanned, the standard, roles filled by onshore or by nearby installation<br>• Automatic or camera, fixed/mobile sensor identification during emergency |

**Fig. 1: Four ideal situations of remote operations**

A remotely operated but manned installation can have a local offshore control room, but during normal operations the command and control of the installation are conducted from an onshore control room. Examples of this on the Norwegian continental shelf are the Martin Linge (Equinor) and Ivar Aasen (AkerBP) installations. Such an installation typically has a lean organization close to the emergency preparedness role requirements and the crew are always on the installation in shift rotation. During an emergency the local control room can be manned, and the offshore organization performs emergency preparedness roles. The offshore organization has a fully manned emergency preparedness organization. Compared to traditional oil and gas platforms the biggest difference is that the onshore control room is always in control. We exclude subsea installations here since they are always unmanned and remotely operated. Subsea fields like Ormen Lange and Snøhvit that are controlled from an onshore control room, but most subsea assets and tie-ins are usually controlled from the installation into which they deliver their production.

An unmanned installation can have a local control room, but command and control are always undertaken from an onshore control room. There can also be no offshore control room or just simplified control and shut-down functions on the installation. The remote sensor capabilities (CCTV coverage, remote actuation capabilities of equipment and sensor systems) are more advanced since the installation is operated most of the time without any crew. The visit intervals are dependent upon the maintenance load and instrumentation level of the installation, often scheduled in maintenance campaigns. Ad-hoc visits by helicopter can happen as last resorts. Maintenance campaigns typically range from manned for two out of six weeks, to as little as one or two scheduled short campaigns in a year. Examples of such installations are Valemon (Equinor) that are unmanned four out of six weeks, or well-head platforms like Oseberg H (Equinor) that have two scheduled campaigns every year. When unmanned the emergency function is handled onshore or by a nearby installation. In a period with campaign manning a simplified emergency organization exists locally (rescue teams) on the installation while emergency management functions can be divided between a nearby field or by the onshore organization. The normal operations model-unmanned in Figure 1 above is the emerging model on the Norwegian Continental Shelf but this is already the standard in highly automated domains like wind-farms and power production/utilities more in general.

We do not have the possibility to address the larger ecosystem around remote operation in this short paper, but we mention these other types of centers of calculation since they bear witness of the movement from local control to centralized global or unbounded control more in general. Neither do we address the cybersecurity aspects and risks around control functions executed through these types. These ideal types also build on the IOGP recommended practice for control systems [11].

The first is the remote collaborative centre which is the collaboration center we recognise as a center of calculation from IO. Remote collaborative centre refers to an open office-based environment where personnel from multiple disciplines collaborate to manage the performance of one or more sites or specialised system across sites, like monitoring of rotating equipment.  Such centres typically host collaboration, monitoring, visualisation, and analytical functions. They are similar to remote control rooms in terms of geographic location but may sometimes be distributed over several locations (i.e., multiple interconnected collaborative centres). Collaborative centres sometimes have less access controls than a control room however this depends on operational or security risks. Remote collaborative centers typically perform remote monitoring, or monitoring and diagnostics of production, operations and equipment conditions remotely using data generated and exported from the production site outside the control room. It also includes remote security monitoring using systems and network logs. It requires appropriate data needs to be available at the remote location. Access is usually made available inside the company firewall with either a vertical or horizontal integration, see next section. Remote at vendor premises also came with IO and refers to a centre of calculation at a remote location belonging to a vendor (or subcontractor). This location is usually located in private premises managed by the vendor or contractor. Contracts may define physical access and security restrictions at the vendor premises. Connection to these premises usually involves communications links via public networks. The external user at the vendor location accesses a fire wall (DMZ) with a strong user authentication process. This center normally does monitoring but can also conduct remote operation of equipment given the right access and cyber physical safety. Both these two centres and their access solution existed in the IO period, but they now can execute more control functions than earlier. The newest center of calculation is remote access from anywhere. Here control can in principle be done from any external location, in a private or public area (e.g., a home, hotel, or airport) where people can sit distributed outside company/vendor premises and can access/ execute control functions given the proper access rights and functions. This option is increasingly seen as an opportunity with the coming of Internet of Things and becomes possible via control of devices via cloud services and new standards developed like OPC UA coming with Industry 4.0.

## 3 Basics of Industrial automation and control systems (IACS) and enterprise systems OT and IT

IACS refers to collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process [11]. This area is called the operational technology (OT) domain. Most IACS can be remotely operated. Most new facilities include connections to enterprise networks to enable data export for plant monitoring, and other types of administrative systems whether these are collaboration systems, portals that are more open to the external world. The latter is the administrative domain defined as IT. Typically, the separation between OT/IT are implemented using firewalls that create a zone and conduit model to achieve appropriate network segmentation and restrict any direct connections between the OT/IT systems. An intermediate network or de-militarized zone (DMZ) network between OT/IT networks is typically used to prevent direct connections between enterprise network and control system networks. This makes it possible for office network-based systems and users to view data from control systems in a secure manner. The DMZ acts as a protection gateway between the safe zone and the enterprise network. Remote connectivity to control systems can be provisioned in two key ways, referred to here as ‘horizontal’ or ‘vertical’ connectivity [12]. First as ‘horizontal’ connectivity, an extension of control system ‘zones’ whereby the local control network is extended to a remote location. This provides identical level 2 control system network access and functionality at the remote location to that at the local site or operational site. The remote location retains the same security requirements as the IACS on the main site as they are fundamentally on the same zone. A ‘horizontal’ connectivity essentially maintains the remote functions within the IACS zone, thus relatively reducing the potential for external access as compared to vertical connectivity. But it increases the access points on the network, making them more distributed and may create new vulnerabilities or common mode of failure especially when the extension is not using dedicated network infrastructure.

'Vertical' connectivity – happens via implementation of connectivity from a remote, higher level (typically office / IT based) network to the local control network through a segregated and controlled 'zone' and 'conduit' architecture. Access to control system networks is managed through strong authentication and network traffic controls (typically a firewall or IDPS). 'Vertical' connectivity however connects control systems to enterprise network or external networks. This is sometimes achieved using third party networks. As all enterprise networks will have external, internet connectivity and often run a managed service to allow inbound connections, 'vertical' connectivity typically introduces the threat of external access to control system networks. In most facilities, some form of 'vertical' connectivity between control systems and enterprise networks as well as 'horizontal' connectivity are used.

Both the vertical and horizontal approach has its pros and cons. The recommended practice [12] describes the trade-offs and considerations that should be undertaken in the design process of the onshore control room. Thus, in the provision of remote operating centers, it is common that hybrid architectures will be present. The architecture is based on the IEC 62443 architecture reference model [11]. For details in the architecture and use-cases we refer to the IOGP Remote Control, monitoring and engineering architectures and security Recommended practice [12].

## 4 Quo vadis- remote operation industrial control systems

Each remotely operated facility has their own IACS (also referred to as safety and automation system – SAS) with functionalities for control and safety distributed between the facility itself (local) and the control center (remote). The dominant model for enterprise reference architecture in IACS is the Purdue Enterprise Reference Architecture (commonly known as the Purdue Model) for control systems and network segregation. Once the Purdue model became the industry standard, many companies started using these network models for safety systems. Purdue provides a model for enterprise control, which end users, integrators and vendors can share in integrating applications at key layers in the enterprise. Over time the industry has moved from a stable order informed by the Purdue model to a situation below where the network architecture is opening up, providing new possibilities and configurations coming with cloud infrastructures and IoT, but also new risks. In other words, Purdue has over time shifted towards an infrastructural system facilitating an evolving ecosystem.

## References

1. Rosendahl, T & Hepsø. V. (2013) *Integrated Operations in the Oil and Gas Industry: Sustainability and Capability Development*: IGI Global Publishing, PA: Hershey
2. OLF (Norwegian Oil Industry Association) (2005). “Integrated Work Processes: Future Work Processes on the Norwegian Continental Shelf”. [Online]http://www.olf.no/getfile.php/zKonvertert/www.olf.no/Rapporter/Dokumenter/05 1101%20Integrerte%20arbeidsprosesser,%20rapport.pdf (accessed 21 September 2009).
3. Karasti, H., Baker,K.S & Millerand, F. (2010) Infrastructure Time: Long-term Matters in Collaborative Development. Computer Supported Cooperative Work (CSCW) Journal Volume 19, Numbers 3-4, August 2010 (377-415)
4. Monteiro E, Pollock N, Hanseth O & Williams R (2013) From Artefacts to Infrastructures. *Computer Supported Cooperative Work Journal*, 22(4-6): 575–607.
5. Bossen, C & Markussen, R. (2010) Infrastructuring and Ordering Devices in Health Care: Medication Plans and Practices on a Hospital Ward *Computer Supported Cooperative Work (CSCW) Journal* 19(6): 615-637
6. Østerlie, T, Almklov, P.G & Hepsø, V. (2012) Dual materiality and knowing in petroleum production *Information and Organization,* vol 22, 2, pages 85-105
7. Latour, B (1987) Science in Action: How to Follow Scientists and Engineers Through Society. Harvard University Press: Cambridge MA
8. Rolland, K.R, Hepsø, V. & Monteiro, E. (2006) Conceptualizing common information spaces across heterogeneous contexts: mutable mobiles and side-effects of integration. Proceedings of the 2006 20th anniversary conference on Computer Supported Collaborative Work conference: 493-500
9. Hepsø, V. (2006). When are we going to address organizational robustness and collaboration as something other than a residual factor? SPE Intelligent Energy Conference and Exhibition, 11-13 April, 2006, Amsterdam, The Netherlands
10. Edwards A.R & Gordon B. Using unmanned principles and Integrated Operations to enable operational efficiency and reduce Capex and OPEX costs. SPE-Number-MS176813
11. IEC/TS 62443 (2009) Industrial communication networks – Network and system security https://en.wikipedia.org/wiki/IEC_62443
12. IOGP (International association of oil and gas producers) (2018) Selection of system and security architectures for remote control, engineering, maintenance, and monitoring. Report 626, October