c21-Virtual

The Connected Digital Oilfield

June 22nd

Mohamed Heshmat – Telecoms Commissioning & Maintenance Lead Engineer

Project Arctic SPG2 (Tengizchevroil / Chevron / Technip... Novatech)

Practical on-Field Telecoms Solutions for Various Systems …

Upgrades from the Past 5 Years and Expectations for the Next 5 Years

What is meaning of Telecoms Solutions? And the importance of them?

Telecoms solutions varies widely from a simple binary signal to switch on or off a more bigger control system, to network sensors implemented to monitor and analyze the flow of data through out a certain process/control network which help detecting cyber-attacks or unauthorized data exporting.

If it wasn't for those simple and complex solutions, then all field equipment, instruments, and gauges will be monitored and controlled manually. A control room operator would then send field operators to check all gauges and manually control valves and all other equipment. Which is time and money consuming and more importantly would create an operational facility that's not safe at all.

So, what we see as a small DCS, PLC or SCADA system is in fact a very complex system that would not only save money or time, but we won't even have any reliable operational facility without.

And from that point we can all agree that, telecoms are really important but since it uses invisible protocols that runs through the background we often forget how important they really are. Except, when they stop working.

What is the difference between a practical and a non-practical Telecoms Solutions?

That is a really important question for all the engineers involved in the FEED and FAT phases. A Telecoms System Integrator can offer you a variety of solutions and its up to the FEED engineer to assess and approve one of them. For example, a site-wide WIFI access can be implemented by Mesh Network Access Points with Gateways and Repeaters albeit a simple fibre Access Points can be used instead. Another example would be Servers and network management systems. Allocating a server for backups, a server for antivirus, and another server for logging activities and so on, can be one solution, while 1x main server + 1x backup server with the use of virtual machines can be a more feasible solution. After all, it depends on

the plant' needs and for sure the allocated budget. But, without an experienced FEED engineer, the cost and function can exceed exactly what is required. (imagine using a truck to transport a 10 kg box of material) did you get the point?

A facility that contains a maximum of 20 to 30 network servers would keep their infrastructure on-site, doing the management, upgrades, patching, and maintenance would consider that solution practical as they would have the manpower to do it since 30 network equipment are not hard to manage.

But, a facility where more that a 100 server would rely on cloud computing services to do all of those tasks. And that would be more reliable to them.

So, classifying a solution is practical or non-practical depends on the plant requirements. And overdoing it doesn't always mean it would be better. As simple as that.

What are the changes that can be seen now in contrast to what were there 5 years ago?

We can all agree that over the past 5 years, not much has been seen on the hardware side of things, but certainly plenty of changes happened on the software side. Whether it is for functionality upgrades, patches, cyber security mitigations but we can see it changing really quickly around us. And lots of the attendees here can recall a maximum of "Let's say" 2x hardware migration tasks on one system but at least 5x software upgrades over the same period of time.

For example, in a previous facility we used to receive an emergency call from the plant SPA instructing us to disconnect the internet line connected to our 1st layer network, whenever the cyber security department confirms that a cyber attack is underway or imminent in the near future, but the downside for that is we never know if a data breach occurred or a malware was implemented or not until we do our post-incident analysis. Which is considered to be a very high risk for any operational oil & gas facility. From that point, network giants like Microsoft, Amazon or even Citrix came up with the Process Control Network Data Analysis Platforms, which uses mainly DELL Sensors for that task.

In which a network sensor to be installed to monitor, collect and analyze all the data traffic in real-time and it's capable of detecting whether the data being transferred is classified as Safa Data or Compromised Data,,, by analyzing any anomaly in the size, type of the data being exchanged or even the source and destination of the data. All of that is being done by SaaS or (Service as a Software) which is one of main aspects of the cloud computing technology. In my opinion it is considered as a state-of-the-art service regarding cyber security.

Another example would be, Cloud Computing, where you can utilize the IaaS (Infrastructure as a Service) or PaaS (Product as a Service) to replace most of your onsite network infrastructure, which leads to saving space, power consumption and all the maintenance hassle. Such solutions we couldn't even dream about in the last decade, but it is considered to be the go-to for many Telecoms Systems Integrators at the moment. Now, Imagine what will happen in the next decade?

One last example would be Firewalls, this field is rapidly moving every quarter to catch-up with all the zero-vulnerability threats which surface every day. Hence, we see new brands taking over the old ones. Next-Gen Firewalls like FORTIGATE

(& NETGATE to some extent) seems to be conquering that field as they combine the functionality of traditional firewalls with deep packet inspection (DPI) and machine learning to bring enhanced protection to your network. In this way, FortiGate can identify multiple threats and block them while tracking both active and inactive users. And I expect most of the oil & gas companies to migrate to one of them (Specially FORTIGATE) in the coming years.

Why implement a solution that is limited in capabilities instead of using a superior one?

The answer is really simple, yet not so visible for all parties, as the 3x main reasons.

1- Functionality: When the simple system fulfills the required function, or multiple simple systems can achieve what is needed, then a complex system with many capabilities is not required in that case. A line of sight intrusion detection system paired with a PLC controller can be implemented instead of an image processing detection system in CCTV perimeter defense systems.
2- Cost: There is no denying that the initial project's cost plays a vital part in choosing and modifying systems, and sometimes leads to discarding of the designed functionality in favor of cost. As long as it won't do any major changes to the needed result.
3- Cyber Security Reasons: On-site air-gapped network servers are eliminating the online cyber attacks far better that using cloud computing services.

Hence, we most of the time go for the simple systems instead of the complicated ones.

Will we ever see one of the non-practical solutions implemented or even replacing the currently used solutions?

This is where it matters the most from what I have mentioned earlier. There is are countless numbers of telecoms solutions being developed every single day, but among all of these only a few can be seen in the oil & gas industry. As we all know, systems integrators will always go for the practical solutions that would cause less headache and cost less money. Cloud computing for example has been on the stage for almost 17 years and yet to be seen widely utilized in our industry, why? The answer is, because it is not in demand at the moment and I don't think it will be in the near future. Except for sure for some cases where money doesn't matter for the client "which is non-to-zero".

But the exception for that can be found within the oil & gas giants whenever they design a facility that would need to be the shining star among the other companies, other than that they always rely on the previously proven solutions (at least for major telecoms systems).

So, the short answer is I don't see it happening anytime soon at least for major systems, Unless it became a necessity.

ST Engineering iDirect @ The Connected Digital Oilfield . Virtual Conference . June 22nd . 14.00 (UK Time)

What will happen to the currently in-use solutions during a 5-years period?

I am really optimistic about the coming years as I believe plenty of changes are about to happen to some systems. Some systems will be replaced completely, and some to be modified to the new generation.

One of the most interesting systems that I've had the chance to commission is the Wireless Corrosion & Erosion Monitoring System. As most corrosion monitoring systems at the moment relies on wired communications, there is a prospect of a wireless system surfacing and dominating that field in the near future. EMERSON is a manufacturer of such systems. And upon having a close look at the technology behind it I was really amazed from the simplicity yet the accuracy and efficiency of it, it offers so many features upon the client's requirements. And I really encourage all my colleagues here to read about it.

To make it a little bit interesting for all the fibre optic specialists attending today, I myself must admire the engineering work behind the Fibre Optic Sensing Systems. Although, the first patent of a fibre optic sensor was more that 30 years ago, but a reliable solution didn't see the light until 2005. In the oil & gas industry it can be found in the modern Electrical Control Boards, but sadly still not widely used yet. It uses the physical properties of light as it travels along a fiber to detect changes in temperature, strain, and many other parameters, as it utilizes the fiber as the sensor to create thousands of continuous sensing points along the fiber core. That led to:

1- Temp sensors.
2- F&G Leakage sensors.
3- Vibration sensors.
4- Intrusion detection sensors, and many more.

Imagine having sensors that can accurately detect the movement of humans, vehicles, and even animals. Not only that, but it can detect the speed, direction, and weight of that object too. In my opinion, I see this being implemented widely in the near future.