A critical view on two new Industrial Automation initiatives

By Ted Angevaare, TAPS, 7th of November 2019

The Open Group, an initiative of ExxonMobil called OPAF, has organised an information sharing event in Amsterdam on the 4th – 7th of November 2019 with the goal to reach out to a larger audience and to create more partners. Today more than 700 members have joined this initiative.

Not only The Open Group, but also **NAMUR** in Germany has create a similar initiative to evolve the Process Industrial Automation architecture into a world of new connectivity, called **NOA**.

The question rises what's so good about these new initiatives and why is the industry overwhelmed by this with so many followers/members? Are the many members just followers because they are afraid that they cannot comply to the new standards and interfaces created by these initiatives or are they afraid to miss business if their name is not on the list or are they believers of the technical advantages?

One of the objectives of OPAF is to **remove Vendor lock-in**. In the days of the large DCS systems, proprietary systems and later UNIX Control systems, once chosen for a certain Vendor, that site was forced to continue with that DCS Vendor forever. For system upgrades and expansions it was economically more attractive to buy the same brand/Vendor, or the entire installed base had to be changed out. As a result the DCS Vendors could increase their price such that it was still economically attractive not to replace the Vendor. Sometimes the price was more than doubled and the End-User had to pay. If the OT systems could be changed such that modules could be changed out for another brand and the interoperability is similar, the cheapest and best solution could be purchased.

The Industrial Automation world is fast changing and evolving since the introduction of Windows in this space and because of this new threats have been introduced such as **OT-Cybersecurity**, the threat of malware and hackers to our industry. Are these new technologies helping us to become more robust against these threats or not? One thing is certain and that is that the IT (Office Automation) and OT (Industrial Automation) are merging faster than legislation, people, standards and work processes can keep up.

ISA95, an initiative of ISA (The International Society of Automation) has created and published new standards and models for the integration of Industrial Automation Systems from the sensors and control elements at the production floor all the way up to Enterprise level and this this the Purdue Model was used.

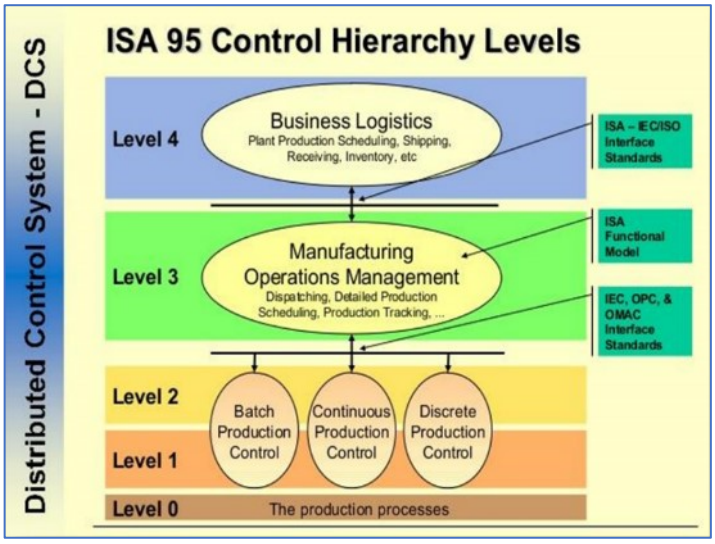

Figure 1: PERA (Purdue Enterprise Reference Architecture) 1992

In the 1992 Theodore J. Williams and members of the Industry-Purdue University developed the **Purdue Model** for architecture in Industrial Automation. The model consists of 5 levels, i.e. level 0 to level 4, as described in ISA95, an International Standard.

In the 2 decades after the ISA95 was published the industry has followed these standards and slowly industrial infra-structures started to look like this, mainly because the principles became more clear and created protection

against OT-Cybersecurity. The ISA standards also helped in the segregation of responsibilities of people. Who is responsible for which system, who's the system owner, who will do the maintenance and who will design it. Organisation have invested heavily in the adoption of these work processes and staff and Vendors have been trained and learned to obey these rules not to create a dangerous situation. The work processes, such as designs and maintenance have been optimised.

Nowadays with new initiatives like **IIoT** (connect sensors to the Cloud) and **Industry 4.0** (smartness in industry) the Purdue model doesn't help, because each level is often protected by a firewall and End-Users see this as a limitation of connectivity, but is this true? Are these Purdue levels not helping us?

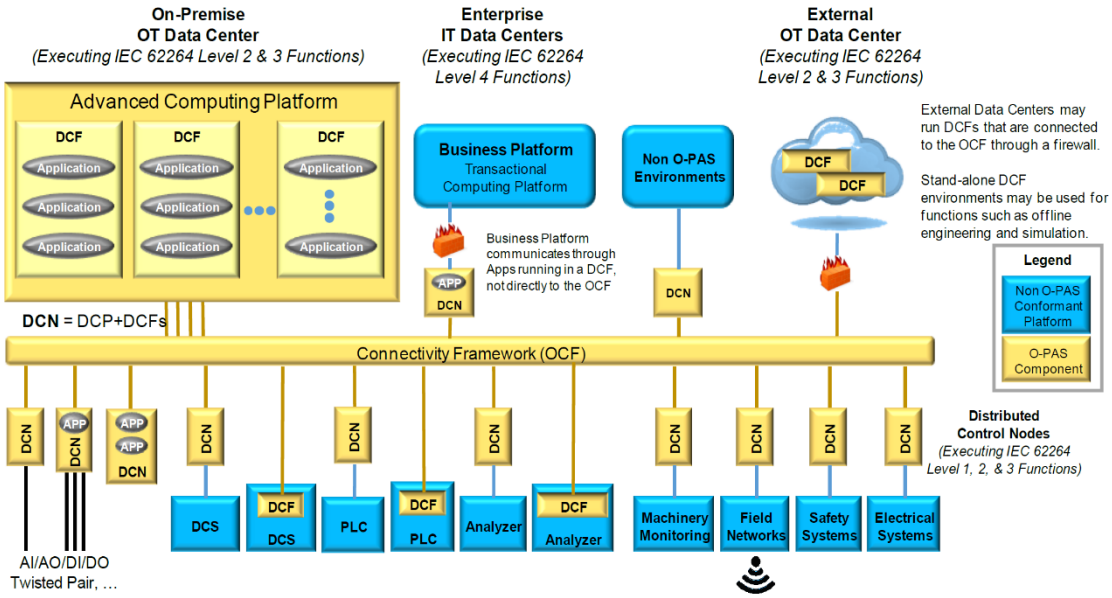

Figure 2: Concept Diagram of a Process Automation System of O-PAS Conformant Components

The Initiative of the Open Group is a logical step in this evolution and that is to create more standards, preferably one big Industrial bus, deal with OT-Cybersecurity and create more and better certification of products that are allowed to communicate to this bus (OCF), but more importantly allow exchange of modules/functions to eliminate Vendor Lock-in.

When the above OPAF architecture is compared to an ISA95 architecture it is clear that there are some major differences.

Connection of the Safeguarding Systems (SIS) is a sensitive subject. In the past the SIS modules were only connected to the ICS (integrated Control Systems) as indicated in Figure 3. Also a keyswitch functionality was added to the SIS connection that can disable and enable configuration changes of the SIS modules. In this way the technical integrity (the safety aspects) are protected by 2 firewalls and a keyswitch when looking from the L3 as a source of the cyber-attack.

The Triton attack (also called TRISIS) in Nov. 2017 proved that **the quality of the keyswitch** is very important and that this should be hacker-proof. The Triton attack was an attack on a Triconex SIS and via the EWS (Engineering Work Station) an attack was launched on a petrochemical plant by changing the SIS module configuration. The learning from this is that the keyswitch is an important component in the defense against Cyber Attacks.

In the OPAF architecture all this is replaced by one **DCN** (Distributed Control Node). It is unknown how good is the DCN and if this can replace two firewalls and one key switch? During the Open Group event in Amsterdam the specifications of the DCNs were not shared and this left a lot of questions. When asked it was stated that the DCN would be an extremely secure device…

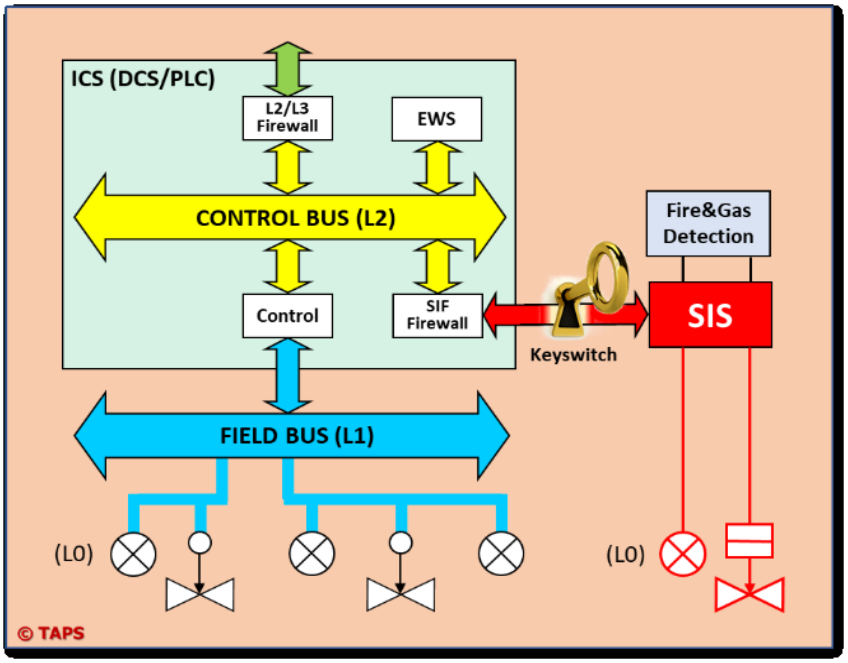

Figure 3: The SIF is only connected to the ICS and protected by Firewall and Keyswitch

Another big difference between the ISA95 architecture and the OPAF architecture is that the layered concept is replaced by a flat Connectivity Framework (OCF). Purdue level 2 and 3 components and functions are all connected to this bus. The OCF, being a L2/L3 bus is directly connected to L4, the Enterprise IT Data Centres and Business Platform via a DCN and Firewall, with the statement: 'The Business platform (L4) communicates through Apps running in a DCF, not directly to the OCF'. The many new abbreviations here may be a bit confusing, but the DCF is a Distributed Control Framework and a DCN = DCP + DCF. A DCP is a Distributed Control Platform.

It is difficult to comment on this, because the security quality of the new DCNs are unknown, but it looks like that another Purdue Level have been removed from this architecture and that authenticated connections will take place between the IT-domain (L4) and L2 (the Control and safeguarding layer) applications. Is the OT-Cybersecurity robustness the same as what we had before, or is it worse or improved?

Many good new initiatives are embedded in OPAF, like all the new standards issued by the IEC 62443 to improve OT-Cybersecurity. Not all of the IEC 62443 standards have been issued yet, but this is a good step forward. Also reference is made to other well known standards, such as OPC UA, TOGAF (The Open Group Architecture Framework), Foundation Fieldbus, HART, WirelessHART, Modbus TCP/IP, etc. So End-Users don't have to replace their entire installed base to comply to OPAF, but can modify into this new way of infra-structure to unlock Vendors.

OPAF is **in full development** as we speak and products are being developed and tested to comply to this new way of thinking, but a lot of information, especially specifications are only available to the members and that makes it difficult to judge if this is a way forward and a better solution….

A detailed Risk Assessment of the architecture with a **focus on the SIS connection and the L2/L4 connection** would help to create more confidence, but also this is unknown.

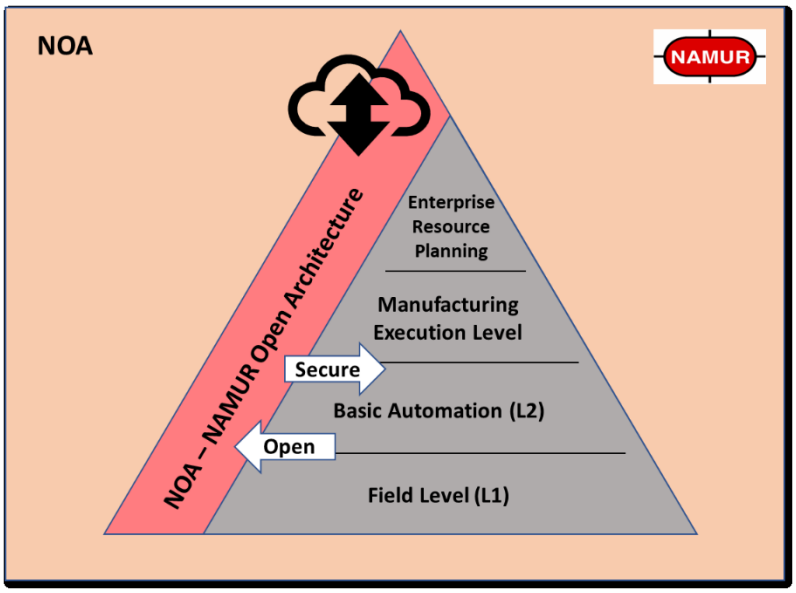

Figure 4: NOA - NAMUR Open Architecture

OPAF and NOA are joining efforts, although both solutions are out of sync in development completeness. At least both organisations have a process ongoing to join efforts. The NOA initiative is bolted on the old Purdue Model as an interconnection layer. Looking into more details NOA is installed on top of the control systems (ICSs).

In addition, the architecture allows for Los-cost multi-sensors and vibration sensors to be directly connected to the Plant M+O and the Central M+O. M+O stands for Monitoring and Optimisation and is intended to create a bridge between the ISA95 architecture and a more flexible infrastructure to accommodate Industry 4.0 and IIoT. The core task of the Plant Specific and Central M+O is to execute monitoring and Optimisation functionality and both functions are placed in a Cloud. Both Clouds could be secured private Clouds but not much is known about the specifications of these.

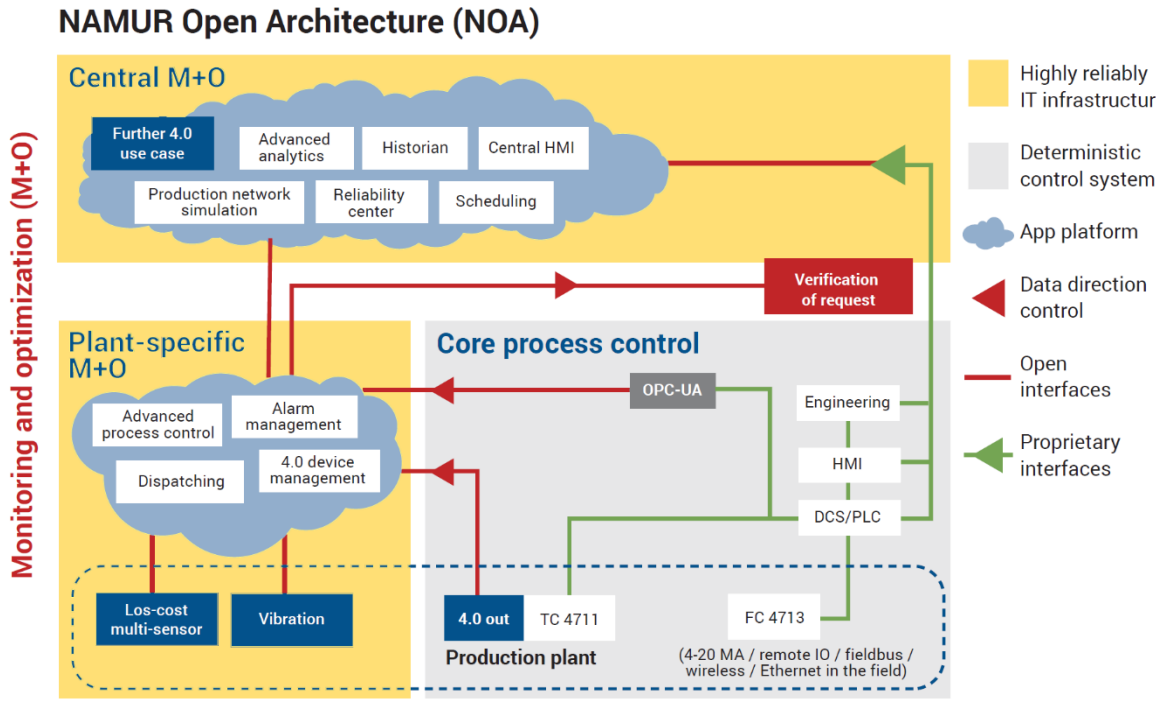

Figure 5: NAMUR Open Architecture (NOA)

NOA development is in a very early stage and it is not clear how NOA can be positioned on top of ISA95. Also here a Risk Assessment of the NOA architecture could create motivation to go this route.

Good is that Namur is in contact with many Vendors and OPAF and maybe both solutions can be merged into a new direction for the future.

The Namur Working Group 2.8 is working hard to make progress and soon more will be known about the advantages of NOA. But at this moment many answers are required, especially in the space of OT-Cybersecurity. The advantage of such an architecture is clear and that is to accommodate Industry 4.0, but is NOA the right way to go?

With a little effort OPAF and NOA can be made more secure by **merging ISA95, NOA and OPAF**. It is not that difficult to remove the new DCN of the Safety Systems and create a multi-Vendor connection to ICS only, like what we had before. OPAF efforts should go in the direction of multi-Vendor SIS / ICS connections. Also allow for only L3 / L4 connections and not for L2 / L4 connections, since L3 and L4 are already managed, often shared on the same hardware network and managed and designed by the IT department and not by Engineering of the End-User.

Another subject that has not been addresses is the location of the EWS (Engineering Work Station) in OPAF. Should the EWS be a dedicated SIS EWS or will it still be allowed to combine SIS and ICS into one EWS?

It would be **an advantage when two Secure Zones and Conduits, as per IEC 62443-3-2** are created to accommodate a dedicated SIS, the connection between the EWS and SIS and the EWS, with the possibility to remotely patch the EWS. It is not recommended to remotely patch the SIS Modules. Patching of SIS should be a local action and the plant should be in a safe condition, such as a shutdown, when the patching is happening. Patching of a life production facility could be dangerous and should only be allowed for the ICS and not for the SIS modules. The ICS modules can only be patched in a life production facility when redundant and when taken offline one by one to be patched.

The OPAF initiative has not shared any information about **patching** as well as redundancy of modules and both could influence integrity and availability of production facilities. Are the OPAF DCNs and DCFs redundant and if not how is the same availability created compared to an ISA95 solution?

It will be difficult to predict how the future will look like, but it will be certain that the industry will move to more secure protocols and architectures. However '**new is not always better'** and therefore well investigated and designed architectures and certification will be important if the industry will be able to withstand the OT-Cybersecurity threat that is evolving as well.

Next generations **SOCs** equipped with next generation **SIEMs** will be added to Anti-Virus and Firewalls when fast enough to stop the Cyber Attack at the front door. An integral solution with IT and OT will be instrumental to make this possible and developments in this space are taken place at this moment. White-listing, Anomaly detection and implementation of next generation firewalls will be the next step that the industry will take to a more secure OT. OPAF doesn't address these topics at this moment in time.

OT-Cybersecurity will be designed and embedded in our OT-systems of the future and certification and compliancy to our new standards will be critical. It will be very difficult for small Vendors to survive in this world and therefore general modules will need to be developed that can be used by the small Vendors to achieve the same level of OT-Cybersecurity matureness.

Also the systems that have been installed in the last decade(s) will be around for many years to come and bolted solutions are very welcome to make this possible. NOA and OPAF both can be bolted on existing systems.

The only way to fight the big monster of Cybersecurity is when the **Industry and its Vendors work together** and this is what OPAF is creating. OPAF is a great initiative, but a lot of work still is required to make this mature enough to be implemented.