Secure Digital Marketplaces supporting cross-organizational production processes.

NWO/STW Workshop “ICT with Industry 2016”
Lorenz Centre Leiden
Nov. 7-11th 2016

Prof. dr. Tom M. van Engers (Universiteit van Amsterdam)
Prof. dr. Robert Meijer (Universiteit van Amsterdam, TNO)
Dr. ing. Leon Gommans (Air France KLM Group ICT Technology Office R&D).
Dr. Kees Nieuwenhuis (Thales Nederland B.V., CTO Office)

1.0 Introduction

In the current ICT-driven global and competitive economy parties may benefit from creating cross-organizational production processes. Such cross-organizational collaboration however implies sharing of sensitive data with others, possibly resulting in loss of control over that data. The challenge of the Lorenz workshop was to provide a distributed systems concept, as well as implementation directions, that supports flexible digital collaborations between organizations. In particular, on basis of existing knowledge the workshop addressed and conceptually tackled the following issues:

- Support for major characteristics of the digital collaborations: 1) ad hoc workflows that are instantiated after 2) an ad hoc, fully automated auction (e.g., for the just-in-time delivery of 4 mechanical parts that was won by an enterprise) 3) where the (sensitive) information exchanged in the auction was securely removed from the domains of the losing bidders. The process is recursive, the winning enterprise, for instance, can subsequently create an auction for production and logistics capacity. Ultimately, factories and logistic chains are instructed (e.g., by scripts, programs) in detail what to do and when. In this systems-of-systems scenario, complexity explodes unless the digital collaborations are constructed from a repetitive pattern of ICT that also facilitates design space separation, cyber security and trust, and robustness. Similar issues appear in the engineering of complex (multiscale) machines, and in systems of collaborative robots (e.g. smart factories) and collaborative intelligent transport systems.
- Support for secure digital marketplaces that consist of a set of connected secured extranets, and transaction software which serves as trading platform, e.g. computers bidding on in an auction and subsequent production of demanded technologies. Communication between the system components is supported by open-linked data technologies that enable access to complex and sensitive data structures and services. The governance of such digital marketplaces requires access control mechanisms, provenance of data and rules for collaboration and monitoring and enforcement mechanisms. These rules include rules defining the collaboration (B2B) as well as rules defined by governments (G2B). In order to being able to safeguard security and introducing provenance mechanisms on top of the open-linked data technology we aim at combining digital ledger technology with open-linked data technologies. This combination will allow for advanced access control mechanisms and forms an important basis for trustworthy distributed data storage and sharing.

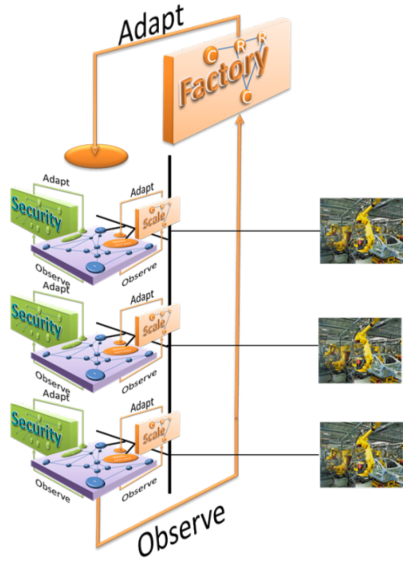


Figure 1 In this IoT concept, a robot arm is connected to a cloud based networking and IT infrastructure – a slice. The slice is experienced as a familiar (yet virtual) Internet environment that allows companies to interoperate their software on a familiar way. A security system takes care of cyber security and watches which information leaves the slice. A scaling and distribution system optimizes the performance of the slice in terms of capacity and latency and distribution over cloud data centers. The Factory manages the system of slices and how they interwork, e.g. how many robots are necessary and what they produce jointly. Furthermore, the Factory or another slice can control physical network connections, e.g. via SDN. Companies controlling a robot could use the slice to auction the production capacity of the robot. Factory software can be recursive, suggesting how complex IoT systems can be generated. In other cyber physical systems, the slices control cars, logistic services, farms, computers, ICT services, …

In the ICT with Industry workshop researchers worked together with the two business organizations that recognized the importance and potential of such secure digital market places, KLM and Thales. This report describes the result of the workshop. The main result is the reduction of the above two issues to their, single, essence. That could be stipulated using a "toy case" that was developed during the workshop. The toy case – termed KLM's fuel pump data sharing system- allowed the workshop participants to deliver a concept that effectively prevents the abuse of shared data. We recognized that data should not be shared with organizations but to computer programs. Then the concept was worked out. We describie essentially the use of an secured environment (slice, in the above figure) that ensures that operations on data is only performed by certified programs. We studied the legal basis and organizations that deliver certificates, compliance demands and sanctions and confirmed that technology was available to implement them.

Trusted Big Data Sharing for Aircraft MRO
using a Secure Digital Market Place mechanism.

2.0 The Trusted Big Data Sharing for Aircraft MRO use case contribution and approach motivating research into the question.

Our use case was target towards the following question:

"What is needed to allow aircraft condition based monitoring data to be shared in a trusted way ensuring the overall benefit of the aircraft MRO industry".

Modern commercial aircrafts are increasingly fitted with sensors, allowing aircraft systems and components to be monitored. A subset of this data is will subsequently be logged and stored. When such data is collected across many aircrafts of the same type, analyses of such data allows determination of a particular aircraft's health condition at any time between maintenance cycles.

When a modern aircraft lands, it will have logged many gigabytes worth of data during its flight. By 2026, it is expected that the overall fleet of approximately 20.000 aircrafts will have collect 98 Exabyte of data per year [1]. The question then becomes: "Can this data can be shared for the benefit of the airline industry?". Considering the research topic of the ICT with Industry workshop 2016 more specifically: "How can a digital marketplace play a role in sharing data within the aircraft MRO context?" and subsequently "How could a digital marketplace be organized and implemented" ultimately allowing aircraft data, and associated algorithms extracting its value, to be shared in a trusted way ensuring that benefits across the aircraft MRO industry are shared in a balanced way.

To provide more insight into above questions, we will first consider the legal context and need to share data in aviation industry context. We will start with describing a legal perspective and see how such context can be supported by an industry standards body that develops standards that could identify the need to share Big Data Assets (i.e. data, methods and algorithms) across the industry. We then picture a framework and some infrastructure models that could become part of a research approach.

3.0 Context.

In 1944 a United Nations convention on International Civil Aviation in Chicago initiated the creation of the International Civil Aviation Organization (ICAO) [2] that was tasked to define and coordinate the core principles allowing international air transport to be performed according to a uniform system. These principles are implemented by member authorities such as the Federal Aviation Authority (FAA) or the European Aviation Safety Agency (EASA). The principles that determine the airworthiness of aircrafts and its continuation is an important topic addressed by ICAO.

3.1 EU perspective.

In EU member states, EASA determines that the continuous airworthiness of an aircraft must be organized by an approved Aircraft Maintenance Program. Part M M.A. 302 [3] states an Aircraft Maintenance Program (AMP) must (in short) establish compliance with:

1. Instructions issued by the competent authority
2. Instructions for continuing airworthiness issued by the holders of the type certificate
3. *Additional or alternative instructions proposed by the owner or the continuing airworthiness management organization once approved.*

Observing clause 3, organizations certified to perform aircraft maintenance, can provide additional instructions to an AMP that subsequently needs to be approved by the competent authority. Approval of such additional instructions could be helped if the instructions are based on standards developed by an industry standards body. SAE International [4] is an example body working on such standards for the aviation industry.

Considering Acceptable Means of Compliance, describing tasks that implement an AMP, AMC MA301 prescribes: *a system of assessment should be in operation to support the continuing airworthiness of an aircraft.* In short a system of assessment should:

1. Highlight significant incidents
2. Highlight repetitive incidents
3. Monitor deferred defects
4. Analyze unscheduled component removals
5. *Analyze the performance of aircraft systems as part of the AMP efficiency.*

In addition, AMC M.A. 302(d) recognizes the need for a reliability program as part of an AMP. Here clause (1) includes *condition monitored components.* Regarding the purpose of and AMP clause (3) states it is *to ensure that the AMP tasks are effective and their periodicity is adequate.*

3.2 A Standards Body perspective.

Considering the development of AMP's to ensure Continuous Airworthiness, SAE International , as industry standards body, develops and provides Aerospace Recommended Practices (ARP's). One of its efforts examines a comprehensive construct of Integrated Vehicle Health Management (IVHM) capabilities. Integrated Vehicle Health Management (IVHM) is an end-to-end capability that transforms system data into operational support information to help enable optimized maintenance actions; improved readiness and availability; enhanced vehicle safety and reliability; product life extension; and product improvement and new design paradigms.

IVHM is based on components equipped with health monitoring capabilities providing information about a component's condition.

As a part of its IVHM effort, SAE created a working group to develop an ARP document on Data Interoperability (ARP 6904) [5]. Its charter states: The purpose of this document is to outline the recommended approach to adopt, manage and develop data interoperability. *With the number of stakeholders involved and the amount of data sharing required, there is a clear need for data interoperability to support the maintenance, logistics, operation and engineering analysis*. This document may require frequent updating to ensure the latest knowledge is incorporated.

Scope:

In order to realize the benefits of Integrated Vehicle Health Management (IVHM) within the aerospace and defense industry there is a need to address five critical elements of data interoperability within and across the aircraft maintenance ecosystem, namely

1) Approach
2) Trust
3) Context
4) Value
5) Security

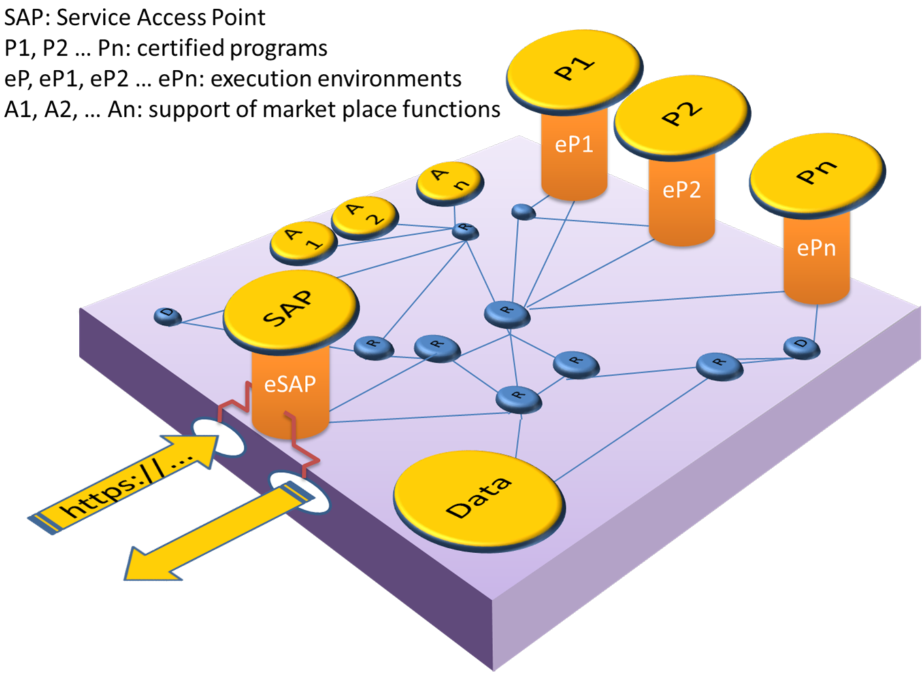
In Integrated Vehicle Health Management (IVHM) data interoperability is the ability of different authorized components, systems, IT, software, applications and organizations to securely communicate, exchange data, interpret data, use the information and *derive consistent insight from the data that has been exchanged to derive value*.

Rationale:

At present the rate of development of data management and sensing technology is very high. Emergent technologies such as Big Data, the Industrial Internet of Things (IIOT) and fourth generation manufacturing means data interoperability will be in a continuous state of flux for some time.

4.0 Researching the Secure Digital Market Place concept.

The Lorenz workshop outlined a secure digital market place (SDMP) concept as an approach for creating an ecosystem facilitating the exchange of Big (and small) Data Assets (BDA's). BDA's are defined as data, methods and algorithms that represent value when exchanged between autonomous market members creating value chains. A SDMP allows BDA exchanges to happen in a trusted way providing adequate protection of member interests. The dominant aspects of 'trust' in the virtual world of an SDMP, are transparency and (enforceable) control as a means to reduce risk. The use of the term 'market place' is on purpose and allows us to compare, and where necessary differentiate, behavioral user-interaction, technical and functional and organizational aspects with those of the physical world market places that we are familiar with.
An SDMP provides an IT infrastructure that facilitates the creation of a secure, policy based operational trading environment allowing administration and enforcement of market rules. Figure 2 shows a technical realization. Market rules also admit members that are subsequently licensed to trade data and/or algorithms and exchange its associated value in the context of a particular agreement. The SDMP offers a number of IT deployment models that members can select to implement agreements in a particular way to ensure data security.



SAP: Service Access Point
P1, P2 … Pn: certified programs
eP, eP1, eP2 … ePn: execution environments
A1, A2, … An: support of market place functions

Figure 2 A slice that implements a digital market place, courtesy of M. Makkes (Thesis, UvA 2017). Typically, the ovals represent applications that are distributed over virtual machines and interconnected with their own overlay network of IP tunnels. The network also comprises routers R. A1, A2, … and An are auxiliary programs that supports the functions of the market place. P1, P2, …Pn are programs that are allowed to operate on Data, and execution environments eP1, eP2, … ePn, check their certificates and observe, log and constrain their actions. The eP might offer services based on physical unclonable functions, that amongst others provides CPU identification and proof of execution. Interactions with and output of the digital market place is controlled by the SAP, that could be implemented with a web-server. The SAP in combination with the execution environment eP essentionally implement and enforce market rules.

In the context of this document, the SDMP is expected to allow data & algorithm interoperability between aircraft MRO organizations needed to support aircraft maintenance programs as addressed by the SAE ARP 6904 effort. Within the airline industry, many other SDMP's can be imagined for example in the context of Cargo Logistics, Passenger Operations, Passenger Experience, Cybersecurity, etc.

4.1 Secure Digital Market Place characteristics

The workshop identified below main characteristics of a digital market place in the context of data & algorithm sharing:

- Secure Digital Market Place (SDMP) is a member organization as **independent legal entity.**
- Goal of the SDMP is to **organize trust between members** wanting to gain a particular common benefit of sharing data no single member can gain on its own.
- Members of the SDMP can be a supplier or consumer of data or both.
- All members have **equal rights** within a SDMP.
- SDMP is **governed by a board of members** in which all members can participate
- The **board of members** is considered the **highest governance body** of a SDMP.
- SDMP establishes regulation consisting of the **market rules (including cost- and benefit sharing) and membership (admission-) requirements.**
- SDMP appoints a **market master** in charge of market operations
- SDMP establishes a regulation for **conflict** settlement
- SDMP appoints an **adjudication committee**
- Members can **obtain rights** (licenses) from the SDMP within the framework of the SDMP regulation to act in a particular defined market role.

4.2 Gathering Secure Digital Market Place requirements

A digital market place must fulfill a set of essential requirements. The workshop determined that gathering a set of essential requirements, based on a large and diverse set of use cases, is a worthwhile topic to be considered for further research.

Within Aircraft MRO context the output a collaboration with the SAE ARP 6904 WG looks promising due to a clearly defined common benefit with a need for regulatory compliancy. Other NWO/STW top-sector efforts could be also be used as additional input for example in in the area of Logistics, Healthcare, Agrifood, etc. In particular TKI Dinalog / NLIP efforts such as iShare [6] are applicable. But also in the context of the Smart Industry (or Industry 4.0) agenda, the SDMP concept can provide a solution to further extend the Security for Smart Industry roadmaps as an element for the digital transformation of sustainable supply networks.

4.3 Establishing Secure Digital Market Place functional elements and architecture.

Using a few expected essential requirements allows composition of below architectural sketch (fig. 4.1), identifying some functional elements of a SDMP that needs further exploration of its applicability. Customer(s) find suppliers of data and algorithms and agree on a particular expected outcome. A registry function can be asked to capture such agreement and check compliancy with market rules. The market place provides a number of deployment models that can be selected to allow (marketplace certified) algorithm(s) to act on supplier data to obtain the expected results whilst observing rights of data & algorithm suppliers. A selected deployment model can be parameterized and provisioned with the appropriate authorizations to allow creation of Internet Slice to facilitate the operation of analyses application. An Internet Slice is a Future Internet concept researched by projects such as NSF GENI [7] or EU FED4FIRE [8]. Chapter 5 will show a few deployment models that could be explored. Transactions that access data and algorithms could be accounted and audited, allowing market members to clear and settle value exchanges and enforce compliancy to market rules.

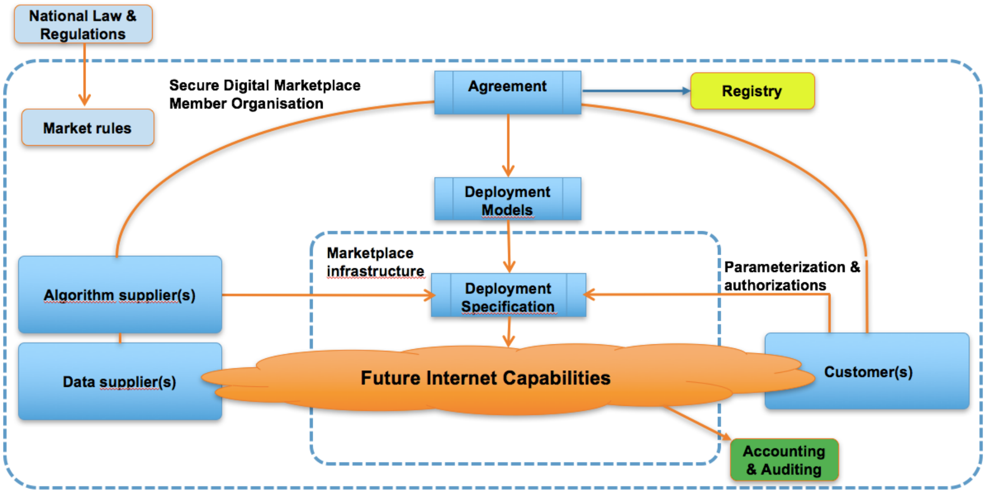

National Law & Regulations
Market rules
Secure Digital Marketplace Member Organisation
Agreement
Registry
Deployment Models
Marketplace infrastructure
Parameterization & authorizations
Algorithm supplier(s)
Deployment Specification
Data supplier(s)
Future Internet Capabilities
Customer(s)
Accounting & Auditing

Fig 4.1 Architectural sketch of a Secure Digital Market Place.

4.4 Scaling Secure Digital Market places

SDMP's are membership organizations that will reside under a particular jurisdiction. Organizing SDMP's across the globe will need to recognize the fact that legal context of organizations may be different. Scaling may be achieved by creating interoperable SDMP's that recognize this fact and create umbrella ruling that allow SDMP's to collaborate, i.e. create a confederative structure.

Output of research involving global academic institutes and industrial participants utilizing an international testbed (see chapter 5) could potentially contribute.

5.0 Secure Digital Market Place research approach and objectives.

Researching the creation of a SDPM involves the establishment of a membership organization that will govern the establishment and operations of a digital market place infrastructure. Fig 5.1 shows a high-level framework of a digital market place hat could be used as a starting point of the research. The framework is based on extending the research performed on the Service Provider Group approach [9].

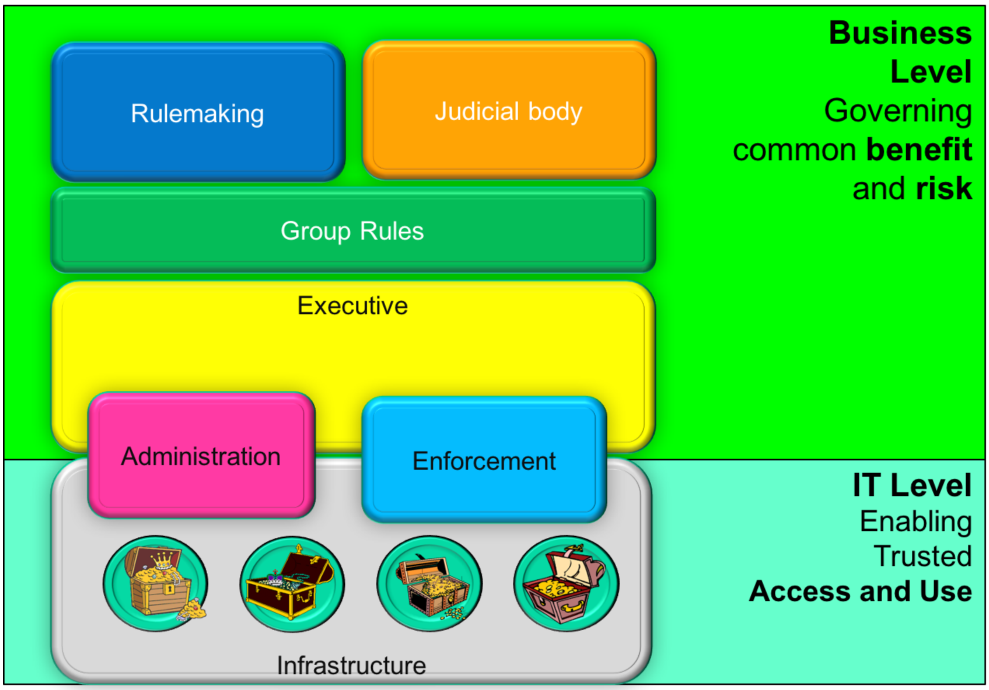


Fig 5.1 High level Digital Market Place framework.

At business level, the SDMP shows a number of essential functional elements of a membership organisation that organizes trust as a means to cope with risk and uncertainty, typical concerns raised by its members. The framework recognizes below main elements, inspired by the work of Charles de Montesquieu [10].

- A **rulemaking body** representing member stakeholders that are responsible for creating a set of membership rules allowing members to join and operate within a digital market place.

- An **executive body** responsible for administering and enforcing membership rules that are ultimately implemented in an infrastructure supporting members to join a marketplaces trading the value of their data (represented as treasure cases). Administration means in essence that members understand the market

- A **judicial body** responsible for resolving disputes amongst members concerning the interpretation of membership rules with the purpose to provide additional clarity and knowledge. If rules so determine, and member provide the power to this body, the body can determine a particular fine or other corrective measures. Note: Such action may be destructive to the trust in a particular member.

The SDMP allows members to create **“market stalls”** in which they can offer data products that can be accessed and used under certain conditions defined in an agreement, negotiated in compliance with the market rules. Interested members may request data products for a particular benefit or the SDMP can act on behalf of a group of members to achieve such benefit.

Research should focus on what part of such a structure can be digitized: Automatic negotiations between market members and understanding what is needed to maintain market stability appear as interesting topics.

The question also arises what infrastructure capabilities are needed to allow members to share data without infringing membership stakes. Members may not like to put their data into a central place as this could allow competitors to see one another's data, possibly infringing anti-trust regulations.

A research question therefore may be: "What kind of data sharing models allow trusted (big-) data sharing", considering all kinds of new developments in the infrastructure virtualization world and its programmability. Also, "What kind of role does virtually infinite bandwidth availability mean" and "What does the ability to create blockchain based general ledger mechanisms mean?" in this context. And what does the fact mean that *"The secret is not so much in the data, but in the algorithms used to extract value from this data".*

5.1 Researching deployment models

Fig 5.2 .. 5.6 shows a few suggest models that can be deployed in Internet Slices that can be studied for its applicability. Fig 5.2 shows the model that should be avoided.

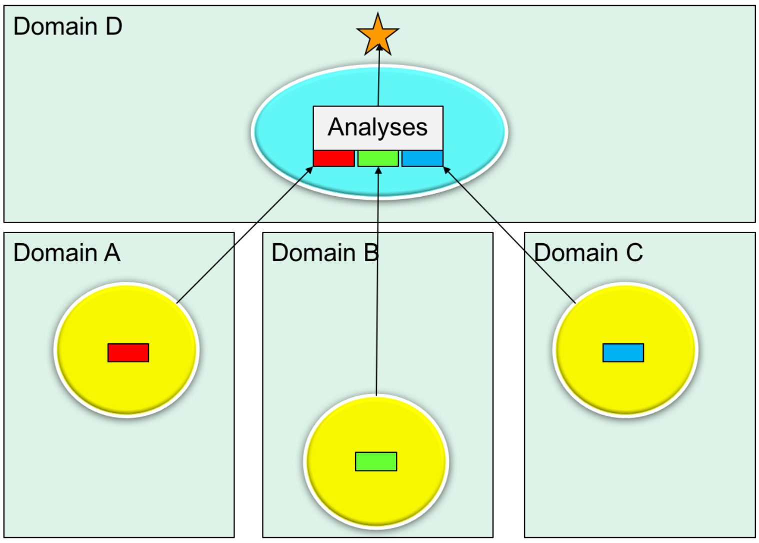


Fig 5.2: The traditional model sharing data at a central place raising concerns with domains A, B and C about keeping their data secure and the ability to make domain D liable for any infringements of local law and regulation domains A,B and C are responsible for.

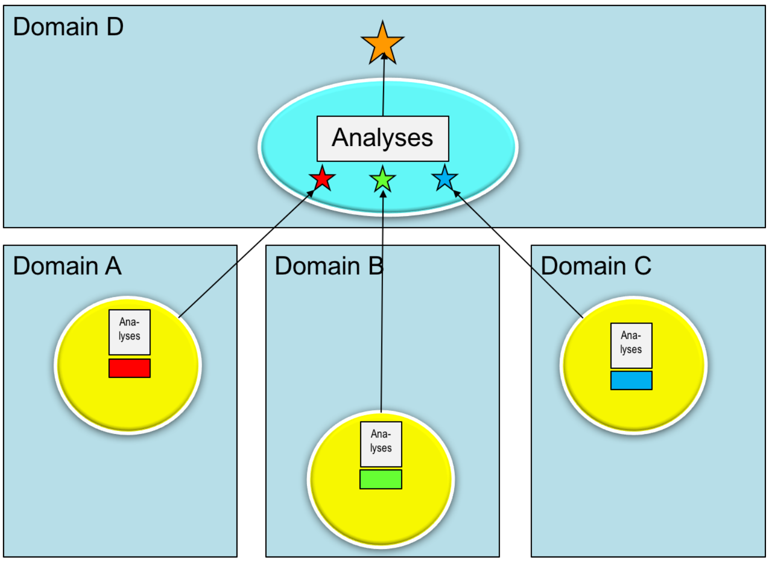


Fig 5.3: Sharing results by bringing the processing to the data of each domain may be a more secure way of sharing data if the end result can be achieved as such. Each domain can permit a particular approved and agreed algorithm to look at their data and monitor its activities.

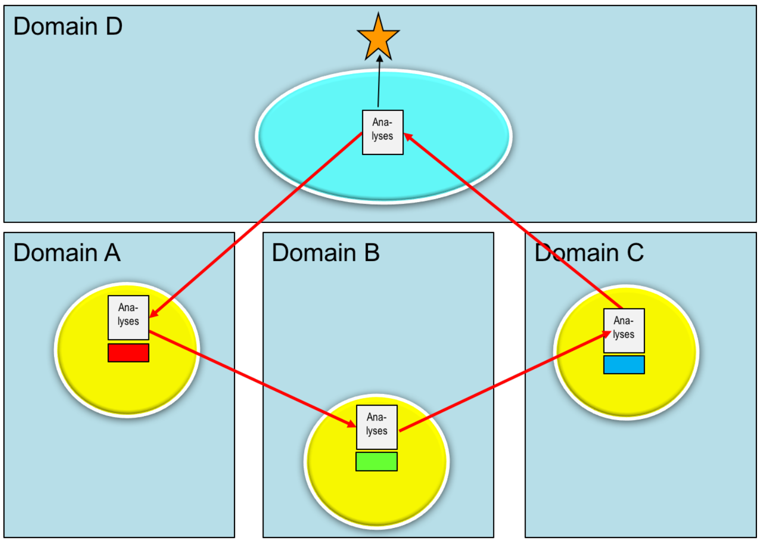


Fig 5.4: The turntable model: An approved algorithm visits each domain to collect results across the participating domains. The end result cannot show from which individual domain particular results were obtained. Ideal for searching patterns that are expected to be observed in data from different domains.

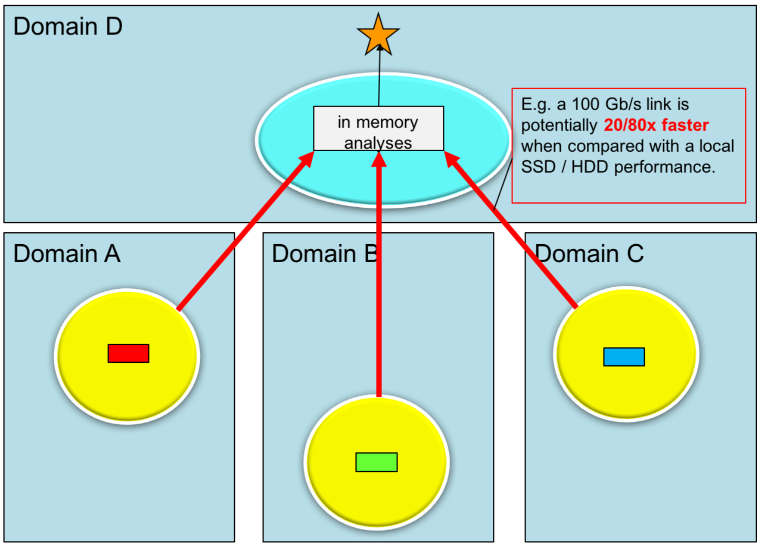

Domain D
in memory analyses
E.g. a 100 Gb/s link is potentially 20/80x faster when compared with a local SSD / HDD performance.
Domain A
Domain B
Domain C

Fig 5.5: What could virtually unlimited bandwidth mean?
A 100 Gb/s link is potentially 20x faster than a local SSD. This model allows data to be read from an in-memory analyses process at the hub. New data transfer technology developed by the research community makes study of such model feasible. (e.g. ESnet's DTN)

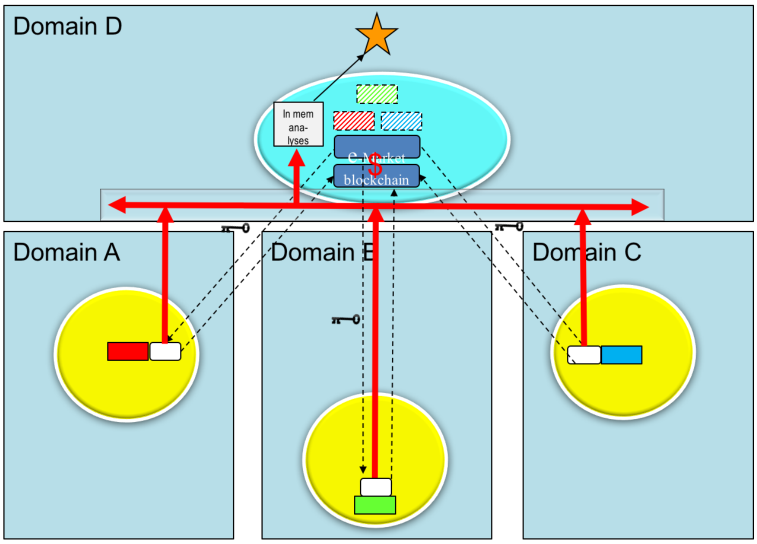


Fig 5.6: Bringing more functional elements into play:
- Authorizaton mechanisms in front of the data allowing specific access based on negotiation.
- An network hub allowing more scalability when hub members want to collaborate.
- Metadata directory at the hub allowing data to be more findable.
- A blockchain ledger keeping track of data transactions.
- A digital market place allowing rules to be established to organize trust.

6.0 Digital Market Place research testbed.

Researching the concepts presented in previous chapters at global industrial scale could benefit from creating a testbed as pictured in fig 6.1

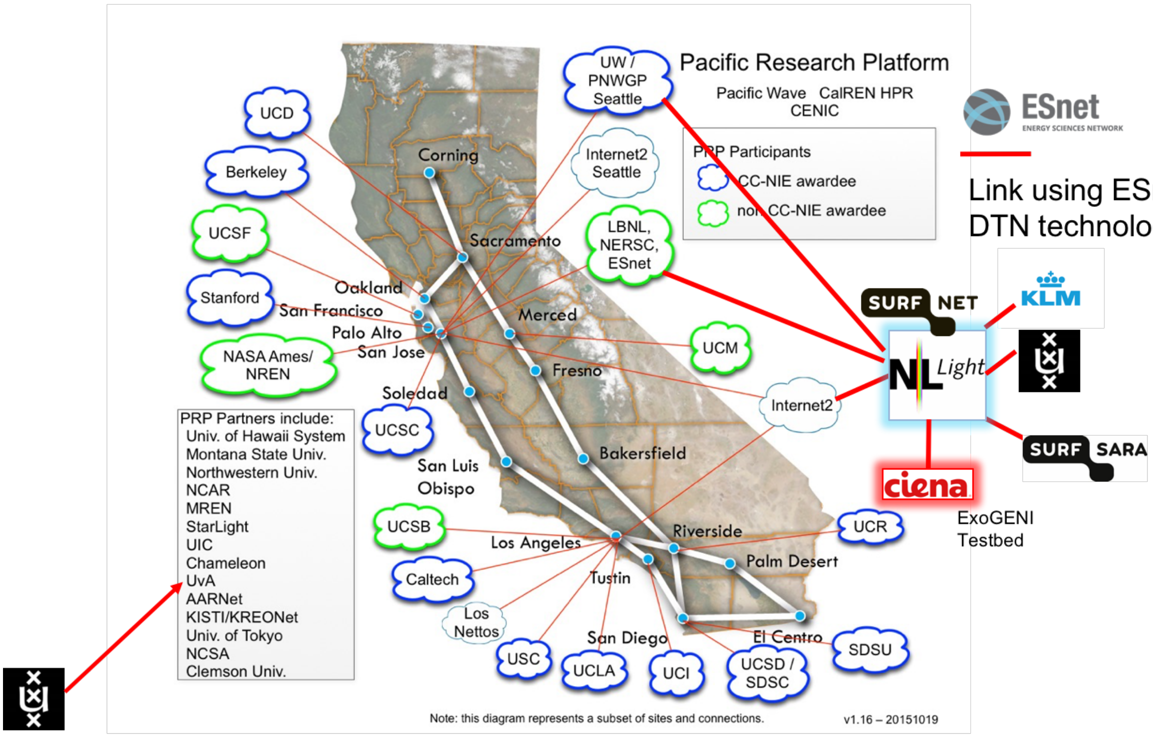


Fig 6.1 The NSF Pacific Research Platform platform researches the question how institutes shown in this picture can share their big data assets to perform multi-disciplinary research based on the fact that every institute has 100 Gb/s of bandwidth available to do so. Air France – KLM is allowed to participate in this infrastructure in collaboration with University of Amsterdam, PRP research partner, and SURFnet and SURFsara and Ciena.

Currently, the NSF funded Pacific Research Platform project is researching what is means to share Big Data assets amongst various science area's available from the US west coast institutes shown. University of Amsterdam is a research partner in the PRP collaboration and has been invited to help research what it means to implement trust when big data assets need to be shared amongst these institutes. The collaboration also welcomes industrial use-cases as it will make solutions more generic. The PRP collaboration and other network research partners have expressed to help facilitate industry use cases, e.g. University of Washington in Seattle has expressed to help in connecting to Boeing. SURFnet, the National Research and Education Network in the Netherlands and SURFsara, the national supercomputing facility, have also expressed their willingness to collaborate and will even provide Air France – KLM with a 100 Gb/s connection to a global network research facility (the GLIF), as such allowing us to explore a global scalable Big Data sharing models as shown in fig 6.2.

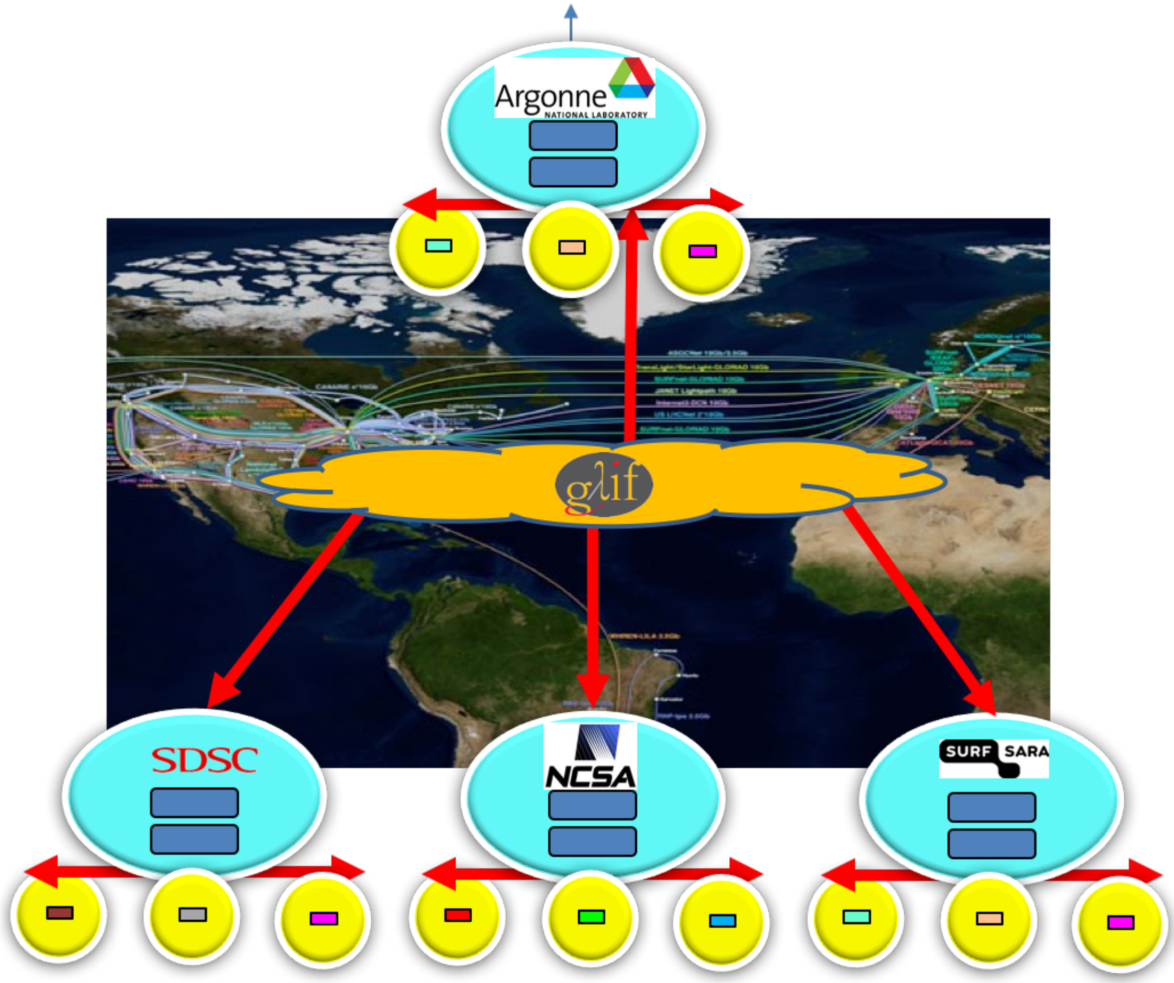


Fig 6.2 A global scalable digital market place concept that can be explored using international high bandwidth connectivity and supercomputer centers, acting as trusted hubs. The Global Lambda Integrated Facility (GLIF) may act as a backbone network providing virtually unlimited, software definable bandwidth across the globe.

7.0 Conclusion

The aircraft MRO use case, based on the Aircraft Maintenance Program concepts being worked out by the SAE ARP 6904 working group, serves a very well-defined purpose with a clearly defined common benefit for the aircraft MRO industry that depends on the ability to share data across the airline industry.

This context does suit the generic research question “What is needed to share Big Data Asset amongst multiple autonomous organizations, serving a common benefit, where trust is needed as a means to reduce stakeholder risk?” very well. Translated into the MRO context the question could be expressed as “*What is needed to allow aircraft condition monitor data to be shared in a trusted way ensuring the overall benefit of the aircraft MRO industry*”.

Explaining this use case to several research institutes and funding agencies (both NSF in the US and NWO/STW in the Netherlands) generated much interest. We therefore believe that, with the help of large industry partners such as Thales and KLM, we can use the pictured infrastructure and academic research capabilities (provided funding agencies are willing to provide adequate funding) on very interesting research use-case that could attract several highly qualified PhD students across the world.

The research approach is however generic and could serve many other use cases in top sector context.

References

1. Oliver Wyman Fleet & MRO forecast: www.planetstats.com/betterinsight
2. See http://www.icao.int/about-icao/History/Pages/default.aspx
3. See http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2014:362:FULL&from=EN
4. See www.sae.org
5. See http://standards.sae.org/wip/arp6904/
6. See https://www.ishare-project.org/
7. See https://www.geni.net
8. See https://www.fed4fire.eu/
9. See chapter 5 of Leon Gommans, Multidomain Authorization for e-Infrastructures, PhD thesis Dec. 2014, permalink: http://hdl.handle.net/11245/1.432647
10. La defense de L'Esprit des Lois, Charles des Montesquieu, Barrillot & Fils, Geneve, 1748.