Virtualisation of information infrastructure for flexible management of value added supply chain

William Lorchirachoonkul, Action Transport Logistics Pty Ltd, Australia
John P.T. Mo, RMIT University, Australia

Abstract

Supply chain information infrastructure has been largely built on the basis of solid IT backbone using static identification technology such as barcode and RFID. However, very few RFID installations can integrate seamlessly. Small to medium enterprises which do not have the same resources as large multinational corporations are often left without RFID connectivity, and hence the information link of the supply chain is broken. In this paper, a virtualisation model which allows new mobile technologies to work in parallel with the existing RFID frameworks is proposed. The concept of virtualisation is to encapsulate a physical device to behave as multiple devices where the resources of the physical device are shared among the virtual devices. The new system capability is supplemented by the development of a GPS based virtualised identification technology “geo-fence”. This paper also describes the application of the virtualised infrastructure for wharf cartage operations on empty containers movement.

Keywords: Virtualisation, RFID infrastructure, mobile server, geo-fence, wharf cartage

1. Introduction

Different types of supply chains have different ways of adding value to the system. A “manufacturing based supply chain” containing a broad spectrum of partners, including manufacturers, third party logistics (3PL), distributors, retailers and so on, has a mixed mode of value adding processes [1]. An important success factor for this type of supply chains is the ability for the partners to identify and track products moving through the supply chain, using the latest information technologies (IT) [2]. Since the way that value is created in this type of supply chain varies substantially due to the nature of the partners’ business, flexibility of the IT infrastructure for supporting value adding activities is of utmost importance.

Supply chain information infrastructure has been largely built on the basis of barcode identification technology. Barcode has inherent deficiencies, for example, it cannot provide item level identification. Radio Frequency Identification (RFID) is an emerging technology that is being applied to supply chains [3]. The main advantage of RFID over barcode is its unique coding scheme supported by Electronic Product Code (EPC) and its ability to be scanned without line of sight [4]. Studies illustrated that the functionality of RFID meeting business requirements are often associated with large-scale RFID applications [5]. However, most supply chain management (SCM) information infrastructures have been largely built around existing IT infrastructure of the companies involved in the supply chain and do not provide the flexibility for adapting new technologies [6]. Experience in a number of RFID pilot projects show that RFID systems are not reliable enough for general business application without significant supplementary infrastructure support [7]. The EPCglobal
model adopted in these projects is based on the assumption that a solid network infrastructures and RFID readers are already in place. The IT infrastructure of these supply chains relies on the availability of static, pre-installed fixed communication framework.

The current EPCglobal model is based on the assumption that a solid network infrastructures and RFID readers are already in place. However, the fact of the matter is, they don't. Most logistics and manufacturing companies operate with a very narrow profit margin. Capital expenses are spent on purchasing operating infrastructures such as trucks, trailers and forklifts and very few on IT infrastructures. Therefore many companies are not willing to invest in such technology such as RFID, with the fear that the technology is unstable and not mature enough to be introduced to their business [8]. Moreover, there is the cost of training and implementing such technologies which also reduce their already narrow margin. Hence, it is very difficult to assess the true economical impact of these technologies [9]. Small to medium enterprises (SME), which do not have the same level of investment as large multinational corporations are therefore unable to link to the global supply chain. Ironically, large organisations, which already embrace RFID technology, will often need to communicate with SME that may not choose to implement RFID due to resource constraints [10]. Since there is no other physical way in that the RFID tags can be read or updated in some parts of the supply chain, the entire information link is broken.

Other important factors are supply chain companies do not like to share or publish their data, such as their customers, delivery details and product details to a third party provider. Therefore getting the full cooperation across the entire link in the supply chain is always a challenging task and will need to be managed carefully. This is also one of the key reasons why the EPC-IS are located behind each company’s firewall in the EPC based projects [11].

Most major companies have IT policies that naturally direct information to a global fixed network structure, the supply chain information backbone is built based on the assumption that future IT infrastructure will be directed to the Internet [12]. From the architectural point of view, the peer-to-peer characteristic of the Internet is an ideal information architecture backbone between trading partners in most supply chain networks. It is a common practice for supply chain companies to outsource their physical activities to 3PL providers, where transaction data are shared via peer-to-peer communication over the Internet. It is the responsibility of the 3PL providers to manage the physical process as well as interacting with external authorities, such as shipping line, terminal operators and local customs officials to lodge shipment information in a timely function before they can physically process each consignment.

Since the availability of microcomputer devices in the last century, the rate of computer hardware development is extremely fast. Device compatibility for old systems accommodating new inventions is always a key issue. To cope with the rapid advancement of hardware platforms, the concept of virtualisation has been evolved [13]. Virtualisation is to encapsulate a physical device to behave as multiple virtual devices where the resources of the physical device are shared among the virtual devices. In the case of RFID applications, if the RFID readers themselves can have virtual machine built-in. The implementation and maintenance process would be more efficient under the virtualisation scheme and the overall costs of ownership reduced.

In this paper, the techniques for virtualisation that can be used to manage variety of devices in a typical value added supply chain are discussed. The virtualised IT infrastructure works
in parallel with the existing RFID framework based on the EPC Network. The virtualisation infrastructure allows alternative technologies to verify the position of the RFID tags and then update the existing RFID framework to ensure that the traceability of the RFID tags remain intact, even there is a broken section in the supply chain. The “geo-fence” model which is made possible by virtualising the tracking system with mobile devices is introduced. The virtualised infrastructure is illustrated with a transparent gateway which incorporates and manages all information for the EPC network and the “geo-fence” at a substantially lower cost.

2. EPC based supply chain network infrastructure

Several large scale projects were conducted in the last few years to investigate the properties and limitations of EPC technology for fast moving consumer goods (FMCG) supply chains [14, 15, 16]. EPC is a product identification numbering system administered globally by the industry organisation EPCglobal (http://www.epcglobalinc.org/). The National EPC Network Demonstrator Project (NDP) used full stack of EPCglobal standard protocol for facilitating exchange of product information across company boundaries when the goods were moved between two cities: Melbourne and Sydney [17]. Figure 1 shows the NDP EPC based IT infrastructure. The NDP identified the business benefits of sharing information securely using the EPC Network, providing authentication to interacting parties, and enhancing the ability to track and trace movement of goods within the entire supply chain involving transactions among multiple enterprises. As each tag was read by each member in the supply chain at different times and locations, the information was stored locally in the EPC-IS database which could then be queried by external authorised parties.

![Figure 1: NDP IT infrastructure](image-url)
In these EPC based projects, managing information infrastructure of value added supply chain relies on the availability of static, pre-installed fixed communication framework. However, the EPC Network is constrained by the need to use static IP addresses and maintain continuous connectivity. Each EPC Information Server (EPC-IS) stores EPC data locally behind the company's firewall (Figure 2).

Since the information from the RFID readers must be relayed from the middleware to EPC-IS, the link between sites must be high quality. However, it may not be cost effective to establish such WAN connection. In some remote sites, where the land value is lower for new warehouse to be built, the link may not be possible. These Australian and European projects [14, 15, 16] used connections in established areas, where the network has been operating in an ideal optimised condition and hence the roll-out of this technology to other parts of the supply chain was problematic [18].

However, in the 3PL environment, where a single warehouse location can be used to represent different suppliers and customers, the RFID readers cannot be modelled as fixed assets and are only updated by a single EPC-IS which belongs to a single entity. After the tags are read and filtered by the middleware, it will still need to be managed by an intelligent decision system, that ultimately routes the information to the correct EPC-IS, where the information is translated to a meaningful business function and process. A set of queries can be sent to multiple EPC-IS at the same time to query an order that consists of multiple tags. However, if one of the links is broken due to system response, connectivity, security or other reasons, that request may not be executed and if the result of that particular query is required to trigger an event or change of ownership, we may end up with a potential dead-lock.

Figure 2: IT Infrastructure for a multi-site EPC Network
Moreover, a gap exists between those supply chain members who are fully EPC compliance and those who do not have such network infrastructure in place. Although EPCglobal has published a universal EPC standard, individual countries are still free to impose further restrictions to the frequency band and power ratings that EPC devices can be used on their land. EPCglobal has been widely used amongst European and western countries. However there are other RFID framework being utilised around the world such as China National Product Codes (NPC) (http://www.chinapt.com/CptNpc/En/Npc_e.aspx) and Japan's Ubiquitous ID (UID) (http://www.uidcenter.org/english/introduction.html), which is supported by many Japanese companies including Sony, Toyota, and Mitsubishi. Infrastructures built on these network standards are incompatible to EPCglobal.

3. Concept of virtualisation

Virtual organisation is an important outcome of business environment expanding globally in recent years. Virtualization implies the use of IT and communication technology by organizations in managing their interactions and key business operations with stakeholders, such as customers, suppliers and employees. A survey on B2B organizations in Singapore showed that an increase in the level of net perceived benefits, external influences, and organizational capabilities had a positive effect on organizational decision makers’ intention to use virtualization [19].

In a virtualised environment, the virtual devices are seen externally as handling different functions in different hardware devices, although they run under one rigid physical container [20]. Such virtualisation technique has been used in medium to large scale information technology infrastructures, where vendor such as VMware, Citrix Xen Server and Microsoft Hyper V use a single physical server to host many virtual servers that perform a range of tasks as a band of real physical servers [21].

The normal practice of virtualisation is to implement an asymmetric virtualisation layer on top of the base operating system, in order to support the concurrent execution of both a real-time and a general purpose operating system on the same processor [22]. Virtualisation method can lower the interfacing complexity and improves the portability for reconfigurable Systems-on-Chip. The layer shifts the burden of moving data between processor and coprocessor from the programmer to the operating system [23]. For environments that require dedicated operating systems and should be installed on different machines for stability reasons. Virtualisation of these services on one high-capacity machine eases maintenance of the systems and reduces the hardware overhead especially for smaller clusters. This approach of hardware consolidation is not restricted to the grid infrastructure and may therefore be applied to simpler services [24]. Manual deployment of the application usually requires expertise both about the underlying system and the application. To support deployment of special automatic features, virtualisation is found to be highly flexible in supporting the services [25].

Figure 3 demonstrates how a typical physical environment (left) can be consolidated into a virtual environment (right). The physical servers and network appliances such as firewall, router, and switch can be emulated by the virtual environment resource pool. This is on the basis that each server on the physical environment are not being fully utilised. The virtual devices are stored in a file system, usually inside a storage area network (SAN) environment.
The physical servers in the virtual environment manage and emulate the resource allocation required by each virtual servers and network appliances.

![Diagram of physical and virtual environments]

Figure 3: Virtualisation of system

A virtualised supply chain information infrastructure will provide more value added support and management to EPC-IS that can be mobilised between servers from different vendors. Since supply chain participation is a loosely coupled relationship, an increased mobility of information infrastructure will significantly improve the efficiency of setting up the supply chain system and encourages more cost effective partnering relationships to be built.

4. Virtualisation by mobile devices

As mobile phones or smart phones (mobile devices) become more evolved, more manufacturers become open to allow more functionality to be included in their application program interface (API) to their devices. Therefore, there is a massive growth to the development of software applications for such mobile devices [26]. Most mobile devices operate with some sort of an operating system such as Microsoft’s Windows Mobile. However, there are also some manufacturers who manufacture their own device and operating system, such as Apple's iPhone OSX. Mobile applications developers can simply write their application to suit a specific operating system instead of a specific device, therefore making the application more available to broader audiences [27].
In Figure 4, the mobile device uses an operating system to manage the resource of device peripherals such as web browsing, and then interface with the mobile application, for example, users can access the mapping data, which are stored outside the devices via a high speed 3G or HSDPA modem. Hence, a mobile device can be used as a host to virtualise complex value added supply chain functions and interface these functions to the mobile network environment. An application that would be most useful for valued added supply chain applications is the incorporation of global positioning system (GPS) as a tracking data source in the mobile device. Many companies managing fleets (including 3PLs) use GPS [28]. Extension of GPS functionality using mobile servers has the potential to significantly improve the capability of such a tracking system throughout the supply chain. However, it also means a substantial increase in number of servers in the system, which imposes implementation issues in existing rigid IT infrastructure.

GPS has been utilised in most Fleet Management System (FMS) for the last few years [29]. Within the FMS application, users can specify an address location and then set a perimiter around the area as shown in Figure 5. The GPS coordinates are transmitted from the personal digital assistant (PDA) which is mounted inside the vehicle at set time interval (e.g. every 2 minutes). If the vehicle is in an area that mobile reception is not available, the coordinates and timestamps are stored inside the PDA, until such time that mobile reception is re-established. A mobile server can then act as a middleware agent to filter out any invalid signal and feed useful information to an Event manager, which can trigger pre-defined process when the event profile is detected.
Figure 5: Concept of a geo fence, managed by a FMS module

In the process of goods tracking and tracing in logistics, the mobile application server keeps track of the GPS coordinates against the defined “geo-fence” zone. When a vehicle enters the valid “geo-fence” zone, an arrival timestamp is stored inside the FMS. An event manager would then trigger a set of predefine tasks to be actioned, such as update job status or even update an EPC-IS database (Figure 6).

Figure 6: Flow chart of device entering geo-fence
As the vehicle is unloaded and left the “geo-fence” zone, the departure timestamp can also be stored in a similar way (Figure 7) and hence vehicle loading time can be calculated. If the loading time is above those allowed in the customer’s service level agreement (SLA), additional charges can be added, where the billing system is triggered.

5. **The virtualised infrastructure**

The process in Figure 5 is made possible using current EPC shipment tags, Serial Shipping Container Codes (SSCC). SSCC are stored inside the supply chain’s EPC-IS databases, which are manifested to the vehicle connote system. As the event manager triggers an arrival event, it can at the same time update the EPC-IS directly and change the status of the tags as delivered to the destination with the arrival timestamp. Under the existing EPC network structure, only the local company database, which is only the sender of the shipment, will be updated. Hence, the virtualised system needs a number of integrated processes in conjunction with appropriate mobile devices. The challenge is to manage the information so that the recipient’s system acknowledges that the tags are now under their possession. The recipient’s system will need to trigger a process which is defined by the end customer, such as re-deliver part of the load to a retail outlet or receive it into inventory. At this point the tags location will need to be updated and if applicable, the ownership is transferred, regardless if the recipient has an EPC-IS or not.

In order for such system to function correctly, an intelligent decision system is required to route the data between physical readers via EPC-IS and those of a virtual emulation, via geo-fence. Since the intelligent decision system will become the bridge between the EPCglobal network environment and the virtualised devices, there is no reason why the same decision system cannot integrate other systems such as China's NPC or Japan's UID at the same time.
In order to synchronise different framework, a common gateway is required to route data from the virtual environment to those of the physical environment and from physical to physical environment. For ease of reference, the common gateway is coded as “Transparent” (Figure 8). The key function of the Transparent Framework is to create a trunk between various enterprise systems such as ERP via the Transparent Connector and translate the data packet and route it to either another virtual environment or back to the EPC network.

Within the Transparent Framework are components that work together to synchronise the information that flow between virtual and physical resources as well as between different network.

5.1 Transparent Connector
The Transparent Connector is a software module that transmits the scanned data between physical readers and virtual readers. It is also responsible for updating different RFID frameworks by writing directly to the middleware layer. Therefore data presentation will be identical as if the tags were read from actual physical scanners of different nature.

5.2 Trust Manager

Trust Manager manages the security profile of each trading partners. It will also store the environment profile of each trading partners and their inter-relationship. Therefore, Transparent Framework would know what method of transfer, such as physical to physical, virtual to physical or physical to virtual.

5.3 Packet Manager

The Packet Manager generates data packet which are sent and received via Transparent Connectors. It also contains the type of interface which describes the environment and configuration of each trading partners via the Trust Manager. The packets will be securely sent and received by the Packet Manager to the Transparent Connector.

6. Supporting wharf cartage operations

Wharf cartage operations are an integral function of 3PL providers, also known as carriers. The carrier’s objective is to pick up a full container from the wharf, deliver it directly to the customer, and return the empty container back to the shipping line’s empty container park. This process is part of the import process. The same process is applied in reverse for export operation. Information from various shipping lines need to be collected and synchronised before a freight operator can make a judgement on when and where to collect a particular sea freight container.

In order for this function to work, information about their container movement must be shared, and published across the supply chain network. Real-time information and planning of empty container movement must be made available to both external authorities including rival wharf cartage companies. With existing manual data collating process, this function is very tedious and leads to a lot of confusion. Recently, RFID has been considered for container applications with some level of success [30]. Since the containers can be tagged with RFID, the only information that needs to be ascertained after securing the container is to associate the RFID with a universal identifier within Transparent.

To ensure that each vessel is loaded with as little delay as possible, export containers are received at the terminal before import containers are unloaded. Before a container can be collected or delivered to each terminal, a carrier will need to request a time-slot (when and what containers are to be collected) from each terminal.

Once the container has been unloaded, the carrier is then notified, within 48 hours to pick up the empty container and returns to the designated empty container park. The carrier only has a limited time (usually 8 days) since the first day of vessel availability to return the empty container (de-hired) back to the empty container park, otherwise, the carrier is penalised by the shipping line. Since each external authority operates their own legacy system, the 3PL
providers will need separate security access for each external authority which will cause security and administrative issue across the supply chain. A typical 3PL provider may have multiple login with different authorities that shared similar information and perform generic functions within the supply chain [31]. Since the information cannot be accurately obtained without cross-referencing with another source, it is the responsibility of each 3PL to manually validate each data set manually. This process is extremely time consuming and prone to errors.

Figure 9 shows typical wharf cartage operations. A vehicle enters an empty container park when an empty container will need to be returned to the shipping line for an import operation. For an export operation, a vehicle collects the empty container and delivers it to the client for packing. The full container is then delivered to the wharf ready for export. Import and export operations are isolated from each other. While an import vehicle is returning the empty container to the empty container park, an export vehicle can collect the empty container for export. For this reason, empty container parks are always very congested. In order to increase productivity and vehicle utilisation, if an empty container park is congested, the empty container is brought back to the 3PL container yard where it can later be de-hired when the empty container park are less congested.

![Figure 9: Implementation of Transparent supporting empty container swapping operation.](image)

Using Transparent, an empty container is returned to the 3PL company’s container yard, it is possible for the company to publish the details of the empty container details (shipping line, type, size, etc) so that other 3PL companies nearby, who need a container of same specification for export operation, can coordinate the release of the container with the shipping line from a 3PL yard rather than the congested empty container park. The advantage
is the 3PL performing the import operation automatically de-hire the empty container without going to the empty container park. Meanwhile, the 3PL that performs the export operation can pick up the empty container without going to the congested empty container park, thus, improving the productivity and efficiency of physical container movement for both 3PL companies.

7. Conclusion

In this paper, the current issues with EPC based networks for supporting mixed mode value added supply chains are examined. Some of the major pitfalls identified include potential risks of broken link, network incompatibility, high investment and inability of global traceability.

With new developments in mobile devices, it is now possible to incorporate more intelligence in these devices for managing movement of goods, making on the spot decisions and communicating with different types of servers as required. The concept of “geo-fence” which has been proved to operate successfully within a real 3PL environment is introduced. The “geo-fence” model virtualises the processes of capturing field data from basically unlimited locations. The mobile devices are virtualised as the equivalence of an RFID device. A virtualised information infrastructure that can support existing EPC network as well as other virtualised devices such as “geo-fence”. With these new developments, a mixed mode value added supply chain can be managed flexibly and include any members in the supply chain, large and small, without the worry of information infrastructure investment incompatibility. This capability is illustrated with a wharf cartage operation.

While the virtualised information infrastructure is successful in extending the EPC network from a site based system to a global tracking system, the new infrastructure requires that more pre-processing of the goods and data must be done. This includes extra processes in associating the EPC data with the geo-fence identity. In practice, this means extra labour hours required to complete the registration and verification processes. Practitioners should also be aware that the new information infrastructure expects to see at least one PDA in each truck, and the communication infrastructure that supports the PDAs. These facilities may not be economical if the number of trucks (users) is small.

The geo-fence depends on the way the boundary of the fence is defined. It is possible to incorporate arbitrary polygons that make sure the geo-fence only captures container movements once. However, analysis of the polygons can be quite complex. Further research in fine tuning the entry recognition algorithm is required.

8. Reference


