Lifecycle ID and Lifecycle Data Management

Mark Harrison, Ajith Kumar Parlikad
Auto-ID Lab, University of Cambridge, UK

Auto-ID Labs White Paper WP-BIZAPP-032

Report Abstract: This paper focuses on issues that must be considered in the design of lifecycle ID and data management systems, considering both intra-organizational issues and inter-organizational issues.

Business Processes & Applications

1. Introduction

This paper focuses on issues that must be considered in the design of lifecycle ID and data management systems, considering both intra-organizational issues and inter-organizational issues.

Over a lifespan of 30 years, an aircraft part may be used in many different aircraft and may change custody and also ownership several times. Each organization that handles the part may record some information about it, while it is within their custody. Typically, these organizations will record such information in their own information systems and databases. At present, there is only limited sharing of information between organizations, which results in a gradual loss of ability to accurately define the current state of the aircraft and its components. The term “current state” here denotes all the parameters that are required to understand the identity, location, and condition of the particular product under examination. The loss of product-related information is one of the major obstacles for managing a product or asset over its lifecycle in an effective manner. depicts this behaviour of product data for different categories of products. The figure shows that for high-value products such as aircraft components, the problem of information loss is not as bad as other products due to reasons such as regulatory requirements for data management. For example, the Federal Aviation Authority (FAA) and European Aviation Safety Agency (EASA) require documentation to accompany installation of aircraft parts, to ensure that only airworthy parts are installed on aircraft. However, the high value as well as risks associated with these products means that any loss of information would be highly critical. In contrast, for a medium-value product such as a computer, it would be very helpful to have information about changes of configuration or upgrade/replacement of components (such as memory, disk drives, etc.) during the usage phase available for better end-of-life decision making – although currently, this data is rarely collected during use – and instead requires time-consuming inspection, although in some cases, there are technologies such as (Self-Monitoring, Analysis and Reporting Technology) [S.M.A.R.T.] for monitoring hard disk drives and predicting failure.

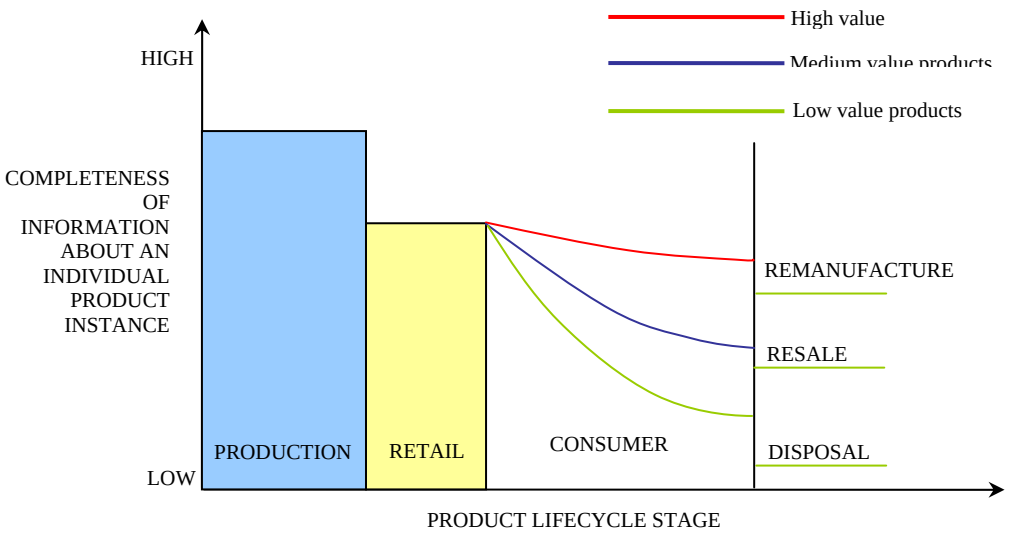

Figure 1: Information loss throughout the product lifecycle (adapted from Thomas *et al.*, 1999 [1])

1.1. Product lifecycle data for aircraft components

Availability of complete lifecycle information about a part could make inspection and repair processes more efficient, since details of previous usage, faults and replacements/ upgrades of sub-components may assist the repair staff in determining the cause of failures and avoiding trial-and-error approaches to repairing parts. Such information might include details of configuration (e.g. when it was installed / removed from a particular aircraft – and the ID of the aircraft), details of modifications to the parts, inspections and repairs made on the part as well as transfers to other organizations for maintenance, repair or overhaul – or in connection with loans of parts. In addition, data may be collected from sensors, either directly attached to the part – or mounted within the operating environment of the part, which may provide data for health monitoring of the part or diagnosis of faults or abnormal behaviour.

Furthermore, as manufacturers are increasingly shifting their business models to providing parts or entire aircraft as a rented service ('power by the hour') rather than as a one-off sale, then it is particularly important to them that they can detect where parts or aircraft are being misused or mistreated – and important to airlines to maximise the operational time of the parts and minimize time when parts are not in service, as well as minimizing inventory / safety stock.

The data about an aircraft part can be categorized as shown in Figure 2.

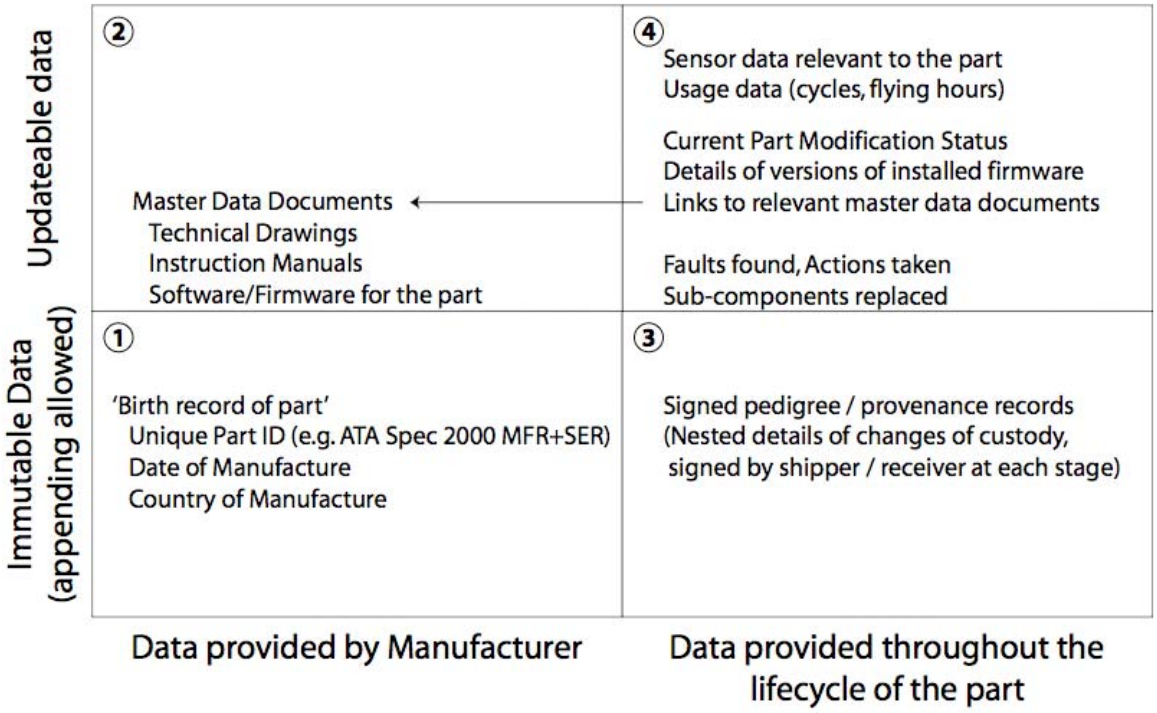

Figure 2 – Categories of data about a part over its lifecycle

Some data will be written once by the manufacturer of the part – and never changed. This forms an immutable 'birth record' for the part, which can be written once by that part manufacturer, then signed and locked and need never be changed throughout the entire lifetime of that part.

At the other end of the scale, there is also highly dynamic data obtained from sensors and observations of the part, which may be supplied by any organization throughout the lifecycle of the aircraft part and provides useful information for diagnostic purposes / health monitoring of parts. Furthermore, if this information can be made accessible in networked databases, then it should be possible to aggregate the data from many parts and detect any trends or correlations in failures or faults.

In order to prove a secure chain of custody for parts, another type of lifecycle data consists of signed pedigree/provenance records, which are appended and digitally signed by each successive custodian.

The information in Figure 2 can also be classified into data which is unique to that individual part serial number – and 'master data' which is unique only to a particular part type (e.g. all parts corresponding to a particular Part Control Number (PCN) within the Air Transport Association (ATA) Spec 2000 standard [2] – but common to all instances of parts of that type. An example of the latter are master data documents, such as technical drawings, instruction manuals etc.

The technology infrastructure varies considerably between organizations, from those who primarily use paper-based record systems to those with computer databases and a high degree of integration and cross-referencing between their internal systems.

The key requirements that we have identified for effective management of product data over its lifecycle are that the data is:

- accessible over a long duration of possibly several decades.
- retrievable in an efficient manner from various sources
- able to be correctly interpreted, allowing for some degree of automation
- authentic with respect to the part, with no risk of falsification or misdirection

In the next section, we shall describe the structure of this report, which is designed around the requirements listed above.

1.2. Structure of the report

This report is structured around discussing the issues related to the above requirements for lifecycle data management. We shall rationalise the requirements and discuss possible solutions that could lead to satisfying those requirements.

Section 2 of this report is concerned with ensuring that lifecycle data remains accessible for periods that span more than the expected life of the associated components. These are general issues of best practice, which need to be considered by each organization involved in the lifecycle of the part and apply irrespective of the type of data being stored. Section 2.2 also discusses the use of data schema to ensure that the data, once retrieved, can be correctly interpreted.

Section 3 puts forth arguments for using a coherent unique identifier as a consistent way of retrieving information about the part, wherever the information is stored – and throughout the part's entire lifespan.

Section 4 is concerned with mechanisms to ensure that the both the lifecycle ID and lifecycle data are genuine, including the use of digital signatures to provide for authenticity and integrity of the data.

The design of user interfaces for application program software which makes use of lifecycle data is discussed briefly in Section 5, with particular emphasis on making the software easy to use and avoiding the need for users to scroll through large amounts of data or look for particular serial numbers or patterns in a list.

Finally, in Section 6, some topics for further detailed work are highlighted, together with an indication of which organizations might take a leading role in each topic.

Closely related to the issues of lifecycle ID and data management are the issues related to the synchronisation of data that is stored on board the ID technology and that stored elsewhere in databases. The Data Synchronization report [3] provides additional details about the issues to be considered in the following situations

When some additional data about a part should be stored in the user memory of a RFID tag

The need to correctly synchronize between data that is stored on the RFID tag and data that is stored on the networked information systems.

In the next section, we examine the first requirement for efficient management of product lifecycle information in the aerospace industry.

2. Long-term data storage and data access

In this section, we shall discuss how lifecycle data stored in data repositories can be ensured to be accessible over long periods.

As mentioned before, it is common for airframes and many aircraft parts to typically have lifetimes of more than 30 years. During such a timeframe, it is highly likely that underlying technologies for storing lifecycle information about aircraft parts would change or evolve as new data storage technologies replace older technologies. It is therefore essential that any system that is intended to manage lifecycle information about the parts should not only be designed to last for several decades but also ensure continuous access to the information, even when the underlying technologies for storing the data change over time.

The two key issues that we will examine in this section are:

- Compatibility of physical data storage media as they evolve over time, and
- Compatibility of data formats as new standards are adopted over time.

2.1. Ensuring compatibility of physical data storage media

Since the dawn of computing, the physical media on which data has been stored has changed dramatically, from punched holorith cards and punched paper tapes to magnetic tapes, floppy disks of various sizes, hard disks and optical storage devices such as CDs and DVDs. Over the decades, the capacity and density of information storage (amount of information per unit physical volume) has also increased by several orders of magnitude. It is likely that this trend will continue for many years into the future and that even more advanced data storage technologies will displace the storage technologies we use today. The higher capacities offered by new storage technologies enable more detailed and complete information to be stored. This in turn drives the expectation and need for even higher storage capacities.

Unfortunately, as new technologies displace old technologies, it often becomes increasingly difficult to access data from older storage technologies. For example, today, many of us would have difficulty retrieving information from holorith cards, punched tape or even 5.25 inch floppy disks, since the hardware equipment to read these, as well as the software interfaces have disappeared from widespread usage / availability. For this reason, it will be necessary to regularly monitor the development of new storage technologies and as appropriate, plan a strategy for migrating historical data to new storage mechanisms, if long-term access to the historic data is still required.

These considerations apply not only to disk-based storage but also to mechanisms that are used to store the ID and additional data on components. For example, already some older barcode symbologies (e.g. CODABAR) are now obsolescent – and companies that still need to read such old barcode symbologies already have difficulty in finding barcode scanning equipment which is capable of reading it.

If RFID technologies are used to store identifiers and data, the fact that RFID tags cost more than barcodes and store more data means that it will be even more important to select RFID tags which are based on the latest state-of-the-art air protocol standards, where there is a serious commitment to ensuring future readability of today's tags for many decades to come.

2.2. Ensuring compatibility of data format

Electronic sharing of information between organizations (and even between different applications within an organization) requires:

- A mutual understanding about the data transmission protocol
- A mutual understanding about the structure and encoding of packets of transmitted data

Assurance about the authenticity and integrity of the data – i.e. that it can be established who wrote the data and that the data content has not been modified between being written and being received.

Where there is a need to share information between organizations (either at the present time or in the future), then it is pertinent that globally (or industry-wide at the least) standards be adopted by all organizations for sharing of data. This would ensure that the data format is compatible with the different information systems that are being used by the various partners in the supply network. In addition, standardisation of data formats would make it easier to reconfigure the supply network by adding, changing, or removing supply chain partners when the need arises.

There are already numerous standards concerning the data transmission protocol, i.e. the mechanism of transmitting data packets from sender to receiver. These include internet standards from W3C and IETF, concerning TCP/IP [4, 5], HTTP [6], XML [7], WebServices [8] etc., as well as various industry standards on electronic data interchange (EDI) mechanisms.

Regarding the structure and interpretation of the transmitted data packets, the technologies of eXtensible Markup Language (XML) [7] and Abstract Syntax Notation One (ASN.1) [9] are two dominant methods of encoding structured data in a way that can be easily understood by computers.

ASN.1 has been a standard since 1984 and is widely used in the telecoms industry (it was originally an ITU-T standard) and other sectors for communicating structured data in a much more compact manner than XML. Because of this, it is also being used as the basis for a compact binary XML format [10] such as Fast Infoset [11] and for Fast Web Services [12].

XML is based on Standard Generalized Markup Language (SGML) [13] (ISO 8879 standard, published 1985) – but it is more bloated or verbose than ASN.1 – since the whole of the data is tagged, including each repeating data element in a list of values. By way of contrast, ASN.1 defines the structure of the data in a preamble or header, so that it is not necessary to place tags around each data element.

It is possible for each industry sector to devise their own data dictionaries and schema, to define the data fields that will be transmitted and to unambiguously indicate the encoding rules for representation as XML data or ASN.1 data. Within the aerospace sector, the Air Transport Association (ATA) is taking a leading role in defining the data dictionaries and encoding, in terms of their Spec 2000 standard[2].

In addition to XML and ASN.1, the STEP (STandard for the Exchange of Product data) standard, which has been ratified by ISO (ISO 10303) aims at providing a standard means of representing product-related data throughout the lifecycle of the product in a system-agnostic manner. In the early days of its development, this standard focused on standardising the format of describing the data that is associated with the design of the product (size, features,

etc.). However, in the late 1990s, the Organisation for the Advancement of Structured Information Standards (OASIS) began to extend this standard to include data required to support a product throughout its lifecycle. This has now been ratified and included with the STEP standard as ISO 10303-239 (PLCS – Product Life Cycle Support) [14], and would be a good candidate for standardisation of product data within the aerospace industry.

Figure 2 of Section 1 of this paper made an attempt to categorize the data associated with an aerospace part into data that is provided by the manufacturer 'at birth' and data which is collected during the entire lifecycle of the part. When considering the data that is stored in the user memory of an RFID tag, memory capacity is at a considerable premium compared with the cost of storage in networked databases. For data elements which must always be present in the 'birth record' or in each 'transaction' of lifecycle data, it may be possible to use a fixed-length field format for those elements, such that the data for a particular element is always read from a particular range of bytes of memory, for a particular version of that data format. This would avoid the need to include a header or XML tags around data elements which are always required to be present in the same well-defined locations in memory.

2.2.1. Handling binary data / documents relevant to the part

Some of the data field 'values' may be binary data files – such as images, manuals in Portable Document Format (PDF) [15] or raw sensor data, etc. Binary data files generally require specialized application software to open the documents and display or extract the data in a meaningful way.

Thought needs to be given to how to ensure that these remain readable in future versions of the software applications used to view them. In many situations, the binary data consists of documents that are applicable to all parts of a particular type or part control number – rather than being unique to a particular part with a unique serial number. In this case, the documents are described as 'master data' documents. Example might include technical drawings or instruction manuals, as well as software or firmware to be installed with a specific part. If there are one or more authors or publishers of master data documents, then it may be advisable for each authority issuing the master data documents to maintain a document repository and to take responsibility for ensuring that the content of the master data documents they issue remain readable with currently available application software, as well as providing some legacy support for the same content in older file formats.

The approach described below is modelled on the concept of a Digital Object Identifier (DOI) [16], which is already used by most publishers of scientific and technical journals to provide a permanent machine-readable citation link [17] to electronic copies of journal articles, independent of any changes to the URL [18] hyperlinks used in the publisher's websites. i.e. a DOI provides a permanent address for where a particular document can be found.

We suggest the following approach to extending the usefulness of the DOI:

- Each part manufacturer creates a centralized repository for the master data documents, which is accessible via a network address or URL. The repository may hold each document in multiple formats and file formats; this is distinct from revisions to the intrinsic data content of the document are logically separate documents which may be linked to the previous revisions. Each logical master data document in the repository should have a unique permanent network address (permanent URL or DOI)
- As new versions of the viewing/authoring software is released over time – or as new file formats displace older file formats, ensure that all documents in the repository which use that binary format are converted to the new format – and that all versions (old formats, new formats) of each document are preserved and available via the network using the unique document DOI as a lookup key on the centralized master data repository.
- Wherever the particular master data is embedded or referred to, a link should be provided to the appropriate document DOI in the master data repository. For example, if an instruction manual or technical diagram is ever stored as data on an RFID tag, then it is advisable to also provide a link to the corresponding document DOI in the master data repository, where the document can always be found (including versions in older and newer file formats)
- If possible, the master data repository should provide a mechanism for automatic content negotiation so that a client requiring the binary master data may indicate which file formats and versions it is capable of handling – and then receive the binary master data in the appropriate format and version. The available formats may be indicated using MIME [19] types, which are widely used on the internet for distinguishing between different file formats and finding the appropriate client reader application to open them (e.g. for knowing which program to use to open an e-mail attachment or web download). For example, the MIME type ‘application/pdf’ indicates a file in Portable Document Format (PDF), whereas ‘image/jpeg’ would indicate a JPEG image. Some MIME types provide for additional version information – but in any case, the master data repository should store the version of the software which was used to create or open the document (e.g. Adobe Acrobat 6.0).

This approach to a long-lived repository for master data documents is summarized in Figure 3

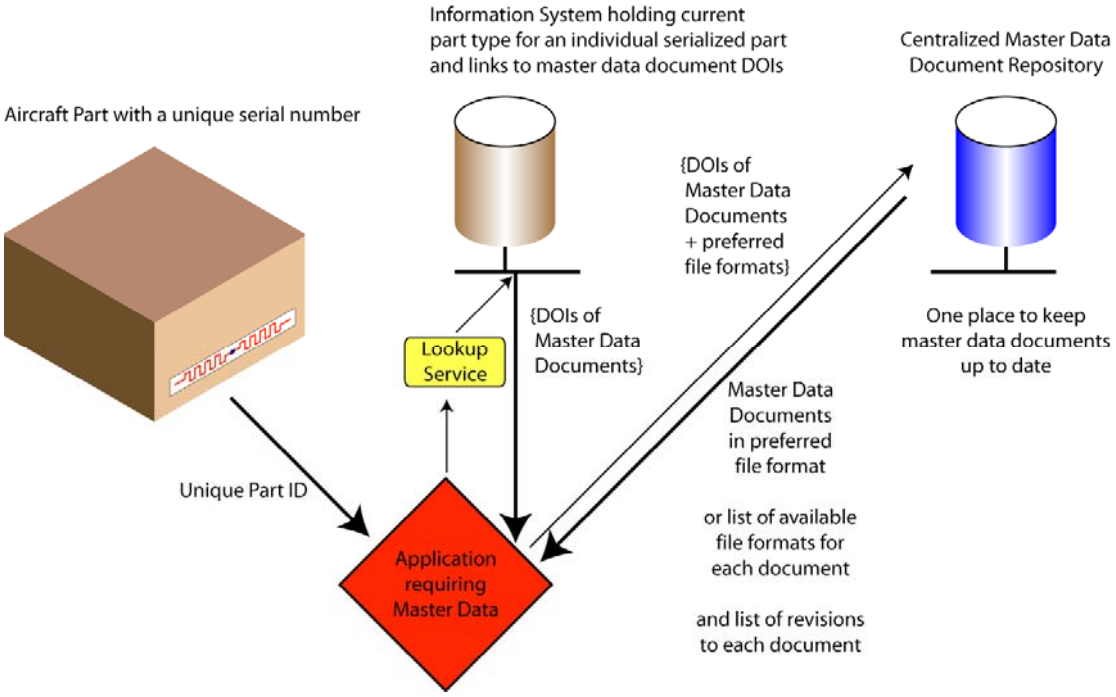

Figure 3. Retrieval of master data documents via Digital Object Identifiers (DOI) as permanent references to the current version of the document

2.2.2. Handling simpler data values, lists and tables

The data that is collected and stored for an individual aircraft part may consist of a simple value (such as an integer, floating point number or string) or a list or table of such values. Examples include the number of duty cycles or flying hours of operation, the date of last overhaul, date of warranty expiry – or a series of data records from sensors.

There is also a need to indicate how such data should be interpreted – for example, do they correspond to a series of measurements of a particular physical property (e.g. temperature) with particular units or collected at a particular timestamp? Clearly there is a need for some structural information in addition to the raw data values, to provide context and avoid ambiguity about how the raw data values should be interpreted.

The structure of the data is usually indicated by a schema document, which usually indicates the allowed sequence and nesting hierarchy of data elements, as well as the data types for each element. Schema documents are therefore very useful for performing data validation and type-checking to ensure that data is correctly formatted in the format required by applications (e.g. use of XML schema (XSD) [20] etc. to validate XML documents). They can also be used to generate skeleton class structures for programming code. For example, tools exist to convert an XSD schema file into a Java bean class and appropriate get/set methods for the data fields (properties) nested within that data structure.

For data stored on an RFID tag, it is not necessary to embed the actual schema – a URL link or even a version number (provided that the schema URL can be unambiguously reconstructed from this) is all that need be embedded on the tag besides the data formatted according to that schema.

The question of whether the structure is expressed using XML formatting, ASN.1 formatting – or another approach (e.g. Text Encoding Identifiers (TEI) as in ATA Spec 2000) depends on a number of factors including:

- importance of ease of human readability
- availability and cost of tools for processing structured data in an automated way
- impact on file-size or file transfer speed.

Another factor which should be considered when deciding on the data structure is the ability for the data to be both forwards-compatible and backwards-compatible to allow for additional data elements/attributes or vendor extensions, so that:

1. newer versions of the software can read older versions of data
2. newer versions of the data can be read by older software (even if some data in new extensions is not interpreted or acted upon).

This can be achieved by the use of extension points in the schema which define the formatting rules to which the structured data must conform. For example, in XML, an extension point may be indicated in the XSD schema[21, 22].

3. Efficient information management

The aerospace industry is handling parts, many of which have a lifecycle of 30 or more years. Some organizations adopted the use of barcodes and databases to maintain internal information about aircraft parts. However, the early adopters may have developed systems for internal use within their organization, without necessarily designing them for use across the entire supply chain. Many of these information systems may have been designed and developed in-house and may be approaching the end of their useful life, perhaps due to limitations on the obsolescent hardware (computer systems, barcode readers) for which it was originally designed. In some cases, a piecemeal approach to the design of information systems has resulted in a very loose coupling between the systems and in some cases, a proliferation of multiple identifiers for a part, where different identifiers are used in order to access information from different information systems.

3.1. Permanent globally unique identifiers for parts

The characteristics and design of globally unique persistent identifiers has already been described by Paskin [23], Sollins [24]and Engels [25]. The following two sections discuss unique identifiers for parts and for data retrieval.

Traditionally, aircraft parts have been identified by a combination of part number (PNR) and serial number (SER) – although the part number is required to change when the form, fit or function of a part is modified. Clearly this traditional combination of part number and serial number does not provide a globally unique identifier that is valid for the entire lifetime of the part. In recent years, the Air Transport Association (ATA) has proposed in its Spec 2000 specification[2] that parts should carry a unique identifier that is valid for the entire lifetime of the part. For new parts, their unique identifier consists of a code representing the original manufacturer (prefixed by MFR) and a serial number (prefixed by SER). The manufacturer code and serial number may be concatenated to form a universal serial number (prefixed by USN)

For in-service parts, the unique identifier consists of a supplier code (prefixed by SPL) and a unique component ID number (prefixed by UCN). The supplier code and unique component ID number may be concatenated to form a universal tracking number (prefixed by UST). For new parts and for in-service parts, the manufacturer code is usually based on the 5-character CAGE code [26] (or NCAGE code for organizations outside the USA), while the serial number may consist of up to 15 alphanumeric characters, which should be unique within the CAGE or NCAGE code. These are represented schematically in Figure 4.

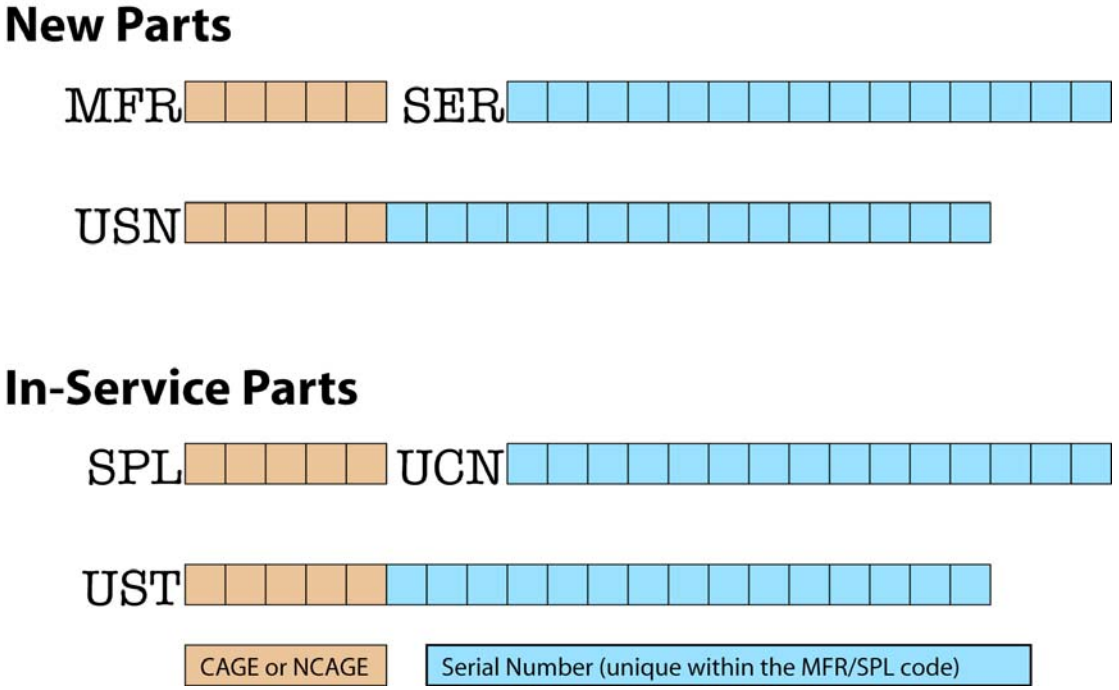

Figure 4 – ATA Spec 2000 Identifiers for permanent part marking

Because it does not include the part number, the Spec 2000 identifier does not need to change during the lifetime of a part and can therefore be used to identify the part across all organizations and for the entire lifetime of the part.

Even if the barcode or ID tag becomes detached from the part, it should be possible to attach a new barcode or ID tag with the same ID as previously, provided that the former ID can be retrieved (e.g. from direct part marking or from documentation accompanying the part). If a new identifier is used because it is impractical to recreate the previous identifier, then the information systems should provide a link between the previous identifier and the new identifier, in order to connect the previous historical data for the part with the future data to be accumulated about the part.

3.2. Use of unique identifiers for data retrieval

The use of a unique identifier brings benefits for networked information systems both within an organization and across the supply chain, since the unique identifier can be used in all systems to identify records that are relevant to that individual part. Furthermore, it can be used in lookup services across the entire supply chain to find information systems that hold information about that particular part.

Previously, when attempting to track a part between multiple organizations, it may have been necessary to follow a trail of links involving purchase orders, shipping waybills, delivery notes etc. By using a unique identifier throughout a part's entire lifetime, there is no need to maintain a complex collection of links between a part's old identity and its new identity in order to be able to gather complete information. It may sometimes be necessary to replace a barcode label or an RFID tag, but it should be possible to write the same identifier into the replacement barcode label or RFID tag, although it would be necessary to update the ID authentication records to link the identifier to the Tag ID of the replacement RFID tag (since this is factory-written and locked by the tag vendor and should be different from the Tag ID of the previous RFID tag which was replaced).

When RFID tags are attached to parts that are not normally serialized, it may nevertheless be necessary for the RFID tag to at least contain a unique ID for the purposes of distinguishing between different objects or parts in situations when multiple objects or parts might be within the read range of a reader. For example, even if lifejackets are not required to be serialized by law, an RFID system would require each lifejacket to have a different identifier in order to count the total number of them, since an RFID system can usually only report on the total number of individual IDs detected; two tags with the same EPC and the same Tag ID would be indistinguishable from a single tag being read twice in succession. This problem might be avoided by relying on the factory-programmed Tag ID to be different for each RFID tag – but it is probably more advisable to actually program unique item identifiers or unique EPCs into each tag, since the filtering middleware (such as filtering middleware based on the EPCglobal Application Level Events (ALE) v1.0 standard) might

otherwise discard tag reads with the same unique item identifier (EPC) as being duplicate reads of a single tag.

In some regions or states, there may need to be further discussions with regulatory agencies (e.g. FAA) to explain the need for unique identifiers on parts that would not normally be serialized, in the case where none-line-of-sight technologies such as RFID are applied to those parts, in order to enable reliable automated counting/detection of each individual part in a correct manner.

3.3. Centralized vs distributed information

Maintenance decisions about aircraft parts may require information arising from all the phases of the part's lifecycle, and as shown in Figure 2, we can classify this information into static and dynamic classes depending on whether the information changes over the part's lifecycle. If dynamic data needs to be embedded in the part, the technology used obviously should have read/write capabilities. This evidently eliminates the use of barcode technologies as they are read-only. With RFID tags with sufficient memory capacity, it is possible to update their contents throughout the life-cycle as information about the part is collected or changed. Dynamic part data may also include information regarding the usage of the part such as operating conditions (e.g. environmental factors), usage rate, number of cycles, flying hours etc. We shall now examine some of the sensor-based systems proposed in the literature directed towards collecting such information regarding the usage of a part throughout its lifecycle.

Appropriate information systems, if used in conjunction with RFID, could provide necessary information about the part in a readily available manner. However, if the data is stored on the tags, it is not necessarily available at other points in the supply chain. It is possible for readers to both write data to the tags and also to update the same data in a database, but then one should manage the issue of synchronizing the data stored on the tag and in the database. In addition, there is also the risk of data loss if the tag is physically damaged during its lifecycle.

However, under the following circumstances, there is an argument for storing data directly on the tag:

- Real-time decisions. In certain applications (e.g., automated sorting), decisions have to be made in real-time within fractions of a second. In such situations, it might be inefficient for the manufacturing system to access necessary information about the part from a database held elsewhere on the network – or impossible to pre-position the relevant information if the expected configuration data about parts installed in an aircraft is not accessible in a suitable electronic format. Here, storing data on the tag could be a more efficient method of data management as real-time decisions require real-time availability of information.

- Real-time data capture. There are many situations where data needs to be captured and recorded in real-time throughout the lifecycle of the part/tag. An example of such a case is monitoring of temperature variations in automobile components. Here, temperature sensors might be attached to RFID tags and variations/abnormalities could be recorded directly on to the tag itself.
- Data access/update at remote locations. Another reason why data might be kept on the tag is if data needs to be available immediately in a place where access to a networked database isn't available. By doing this, for instance, even repairs conducted in remote locations can be recorded directly onto the tag.
- Frequent data access. Throughout the lifecycle of a part, there are various decisions that need to be taken, which in turn uses different sets of information about the part. Some information would need to be accessed more frequently than others, and hence this is a very important factor that needs to be looked into during the design of information systems for parts. There is always a trade-off between the cost of storing data on tags (which significantly increases the cost of tags) and the cost of storing data in networked databases (which increases the cost of data retrieval and transmission). In situations where the frequency of data access is so high that the cost of data retrieval and transmission is greater than the cost of writable tag, it is prudent to store data on the tag itself.

The arguments mentioned above are neither exhaustive nor conclusive. They are rather indicative of the applications and scenarios where holding information directly on the part would be useful. Such solutions are evidently more expensive to implement and maintain, and would require rigorous cost justification in order to do so, as the cost of memory on an RFID tag is at a significant premium, compared with the cost of the same amount of memory in a computer database. In most situations, information about the part can be stored on databases linked to the product through a network connection, using a unique part identifier as the cross-reference.

Provided that the handheld RFID reader is connected to a portable computing device (e.g. PDA or tablet PC) which can be regularly synchronized with the network, it may also be possible to consider a hybrid solution whereby the relevant additional data about the configuration of an aircraft and the additional data for each part is pre-positioned to the hard drive of the tablet PC during a synchronization process before the task begins – and any updates are temporarily stored on the tablet PC and subsequently synchronized back to the databases via the network in a synchronization process which happens after the tasks are completed and when the tablet PC is returned to its network-connected 'docking station', which may simply be an office or maintenance stores with a wireless LAN connection. In this hybrid solution, the RFID tags attached to some parts could be relatively low-cost tags, storing primarily a unique item identifier and perhaps some useful data to ensure safe handling of the part (e.g. nominal weight, hazardous materials, electrostatic sensitivity, etc.) – while the lifecycle data is stored on the networked database and temporarily cached for read/write via the portable computing device attached to the reader.

As far as data location is concerned, two methods for managing networked information about parts emerge: (a) a centralised data repository, or (b) distributed databases. Data storage in a central database is a viable solution where data capture and access happens within a single organisation. There are also high-security applications where the sensitivity of data often demands that access to the database be rigidly controlled, and in such cases, centralised data management is often the only acceptable solution. However, such systems offer only a part of the information required to make effective part maintenance decisions. They are not capable of providing accurate information about the state and structure of the part throughout its lifecycle because they may fail to incorporate modifications made and additional data collected after the part left the manufacturer, unless other organizations agree to provide this information to the central data repository. Moreover, with the global nature of today's supply chains, centralised product databases are mostly impractical, since not all information about a single part can necessarily be kept by one company. In most cases it is practical to distribute the data among multiple databases.

At present, there is hardly any mandatory sharing of information about aerospace parts between organizations except for the transfer of the FAA form 8130-3 serviceability / airworthiness certificate [27] and the data contained within it.

Many of the benefits of lifecycle data are only obtained when there is sharing of information between organizations (e.g. about details of faults found, actions taken, number of service hours/cycles, number or removals/installations from/onto aircraft, warranty dates etc.)

Currently, many organizations store their own information about their own parts or other parts which they handle (e.g. for service/repair operations) but only share the minimum that is required by law, unless specifically requested to do so.

There are good reasons for why lifecycle data is likely to remain fragmented across multiple organizations [28] – but for more efficient operations in future, there will need to be an automated mechanism for exchanging data in a controlled way at serial number level between organizations. This has two pre-requisites:

- The ability to mutually understand the data format and data query mechanism – discussed in Section 2.2.
- The ability to automatically find which other organizations may have information about the part, via lookup services.

3.3.1. Pedigree/provenance records for parts

The FAA and their counterparts such as EASA are keen to encourage better traceability of parts. At present, this consists of paper FAA 8130-3 forms, which may soon be superseded by electronic 8130-3 forms including appending with additional shipping/receiving details and additional airworthiness data, followed by digital signature by each successive custodian. However, even the electronic version would normally only be transmitted onwards with the

part, rather than the traceability information being available symmetrically to all previous custodians, if required.

There may be very good business reasons to separate information about business transactions involving the part from information that is intrinsic to the part's airworthiness to current modification status, in order that financial or commercially sensitive information does not 'leak' between organizations because it travels with a part. However, the security of information should be achieved via appropriate authentication and authorization mechanisms for networked databases and careful consideration of which data fields should be stored on a part or included in an electronic pedigree document; it is not a justification for using a complex series of different identifiers for an individual part which makes the gathering of complete lifecycle information difficult.

3.4. Gathering of complete information

3.4.1. Robust access to data via URLs

Uniform Resource Locators (URLs) [18] or hyperlinks may be used to link to individual data elements on networked databases, as well as linking to schema documents that describe the structure of data.

The URL should be designed for longevity. This means that it should identify a particular organization but should not indicate the underlying database technology nor the web technology used to access the information. This means avoiding structures within the URL which are likely to change over time. Examples include '/cgi-bin/', .asp, .php etc. – the URL should simply be a logical structure e.g.:

https://hostname.provider-domain.com/uniquePartID or

https://hostname.provider-domain.com/uniquePartID/dataElement

where the unique Part ID might be an ATA Spec 2000 identifier and the data element might be an ATA Spec 2000 TEI data field indicator

It should also be noted that SITA already manage the '.aero' domain for the aerospace sector and provide lookups based on airline codes, airport codes – so it may also be logical for them to provide lookup or redirection services based on the MFR/SPL or CAGE codes.

3.4.2. Lookups of data from the manufacturer or supplier

If the original manufacturer (MFR) or supplier (SPL) code is immutable, then there is always at least one provider of authoritative information for the part, even though there may be additional providers of lifecycle data for the part.

[To avoid confusing the reader, it should be noted that EPCglobal and particularly the Object Name Service (ONS) specification use the term 'authoritative' to mean data provided by an object's manufacturer or originator – and the term 'non-authoritative' to mean additional data gathered across the lifecycle / supply chain which might not known at the time of manufacture; this does not imply that it is not genuine data – just that this data was not available to the object's originator at the time of manufacture]

The unique identifier based on the ATA Spec 2000 identifier should be the primary key for lookup services, in order to obtain links to information services holding information about the part at any time throughout its life.

Even though a lookup service may provide links to multiple information services, the providers of each information service would control who has access to information – and the level of access or detail for each user.

The manufacturer or supplier code could be read from the identifier – and a fairly static link to their information systems provided using Domain Name System (DNS) [29] technology. This is the principle behing EPCglobal's Object Name Service (ONS) [30] which is implemented using DNS.

In this way, the manufacturer or supplier code is simply being used much like a web address, except that there is no guessing about the domain name, since the hostname is always of the same format:

e.g. MFR.lookupService.aero or SPL.lookupService.aero

or MFR.aero.id.onsepc.com SPL.aero.id.onsepc.com

in terms of the hostname used with EPCglobal's Object Name Service.

N.B. In the examples above, 'lookupService.aero' and 'aero.id.onsepc.com' are for illustration only and should not be construed as definitive.

The lookup service itself might not provide any public access to links to information services; users may be required to authenticate with the lookup service and to be authorized to use the lookup service. It should be noted that lookup services that are based on DNS (such as EPCglobal's Object Name Service (ONS)) do not currently provide for authentication or authorization, although they generally only link to the manufacturer's information services, rather than providing the more commercially-sensitive links across the entire supply chain.

3.4.3. Lookup services for distributed lifecycle data

A secure serial-level track and trace lookup service could be the logical next step beyond electronic pedigree/provenance records. This could provide any authorized organization that has had a legitimate involvement with a particular part to track forwards to find where the part is now, as well as tracing backwards to find all previous custodians. The technical requirements need further development – but need to consider the volume of 'link' records required (e.g. number of parts x number of custodians per part, which has implications for how such a distributed database is implemented), as well as access times required and any additional meta-data needed for filtering purposes (e.g. filter on a particular part number – or a particular kind of data – e.g. look for only links to organizations providing data elements of a particular type (e.g. with a particular three-letter ATA Spec 2000 Text Encoding Identifier (TEI) prefix)

Technologies such as Web Services Security [31] and Distributed Hash Tables [32] are likely to play a major role in the design of serial-level lookup services. EPCglobal are due to begin standardization work in this area, under the name of 'EPC Discovery Services'. It is therefore very important that the aerospace industry should engage in this work, to ensure that their industry requirements are taken into account,.

An alternative approach to conventional DNS may be needed for serial-level tracking across the supply chain (what EPCglobal refer to as 'Discovery Services'), both in terms of a much higher level of scalability and much lower latency times for updating and also an interface providing greater security and privacy of the link information.

If it is required to limit the results to only those links or information corresponding to the period when the part had a particular part number (i.e. when the part had a particular form, fit or function), then it would be conceivable to provide the part number (PNR) as a second parameter to the lookup service or information service, for filtering purposes, to limit the amount of data returned to that which is relevant.

4. Authenticity of ID and lifecycle data about the part

A unique lifetime ID and lifecycle data for a part is only truly useful if it is authentic and can be trusted. At the present time, networked databases and network security technologies are more tried and tested than some security mechanisms found on tagging technologies such as RFID – and also easier to apply in a cost-effective standardized way, without significantly increasing the complexity and cost of the tagging technology. Perhaps for these reasons, the FAA does not currently accept data stored on the tag as being suitable for a system of record – and it is more likely that the networked databases will be the next accepted systems of record as paper records are replaced with machine-readable data.

4.1. Authenticity of the unique identifier

A unique identifier can be used to uniquely identify and securely authenticate a part only if there is a high level of assurance that no other part carries the same unique identifier or if there is a mechanism by which it would be possible to detect parts with duplicate IDs in circulation.

In terms of combating counterfeiting, unique identifiers combined with dynamic item level lookup/authentication services allow the rapid detection of duplicates of genuine IDs as well as detecting 'invalid' serial numbers which have not been issued – or which were not issued for parts of that type (e.g. original part number). It is not essential and may in fact be inadvisable for parts manufacturers to issue serial numbers sequentially, leaving no gaps. Manufacturers may choose whether or not to embed any additional logic into their own serial numbers, e.g. to allocate particular ranges to specific manufacturing sites – or to embed the lot/batch number within the serial number.

Many ID technologies allow anyone to read an object's unique identifier, without any requirement for the reader to authenticate themselves nor any checking about whether they are authorized to read the unique ID. This flaw would make it possible for counterfeiters or suppliers of unauthorized parts to attach unique identifiers that are simply duplicates or clones of the identifiers of genuine parts, in order not to arouse suspicion.

In the world of 1-D or 2-D barcodes, it is possible to replicate the barcode pattern simply by using a high resolution scanner or digital camera and a printer or other patterning mechanism, to reproduce the characteristic pattern of lines or dots, even if the information content is encrypted or cannot be trivially deciphered.

Some radio-frequency identification (RFID) tags partially overcome this flaw in a number of ways:

4.1.1. Factory-programmed Tag ID

Some RFID tags consist of multiple memory banks or at least separately lockable blocks, to allow for storage of a user-programmable unique identifier (e.g. an EPC or ATA Spec 2000 identifier) in one memory bank – and to store a hard-coded Tag ID in another memory, where the Tag ID is factory-programmed by the tag vendor at the time when the tag is constructed and cannot be changed.

Provided that the vendor of the RFID tag issues different Tag IDs to different tags and that the manufacturer of the part writes an additional unique identifier (e.g. EPC or ATA Spec 2000 identifier) to the tag, then the manufacturer is able to maintain the association between a particular Tag ID and a particular unique identifier (e.g. EPC or ATA Spec 2000 identifier) which they wrote on that physical tag.

Currently, EPCglobal's UHF Class 1 Generation 2 specification [33] provides for a 32-bit Tag ID – although by itself, this is clearly insufficient to guarantee global uniqueness for all tagged objects.

The manufacturer would typically keep the records of association between the tag vendor's Tag ID and the manufacturer's unique ID private – but provide for a challenge-response mechanism to authenticated, authorized trading partners for them to verify that the identifiers match.

This makes it technically more challenging for counterfeiters, since the tags they use must contain two identifiers, both of which must match with the records of association stored in the manufacturer's database. The counterfeiter would need physical access to several genuine objects and to read both the Tag ID and EPC and compile their own table of associations for genuine products, which they then use for cloned tags. It is clearly very important to secure the manufacturer's database of associations, since the ability to hack into this would allow a counterfeiter to change the records of association, and potentially trick the ID authentication mechanism into accepting cloned tags and even rejecting genuine tags.

4.1.2. Access password

Some modern air interface protocols (e.g. EPCglobal's UHF Class 1 Generation 2) [33] provide for an access password, which must be communicated to the recipient and sent to the RFID reader in order to read the unique identifier or the TagID memory banks.

This should provide a further challenge to counterfeiters – although it may be possible to read the unique identifier (but not the RFID Tag ID) from an independent identifier mark (e.g. barcode or dot peening) where this is provided for robust access to the unique identifier, even if the tag fails.

4.2. Authenticity of the part

The previous sub-section discussed checking the authenticity of the unique identifier. However, this is not sufficient for checking the authenticity of a part, because a barcode or an RFID tag could be removed from one part and attached to another part, e.g. removed from a genuine part and attached to a counterfeit part. In this case, it is also necessary to connect the unique identifier of the barcode or RFID tag to some other physical security features that are characteristic of that individual part – but which are different for other parts of the same part type but with different serial numbers. For other industry sectors, physical security markings might include the use of ultra-violet invisible inks, microprinting, holograms, etc. Some of these may be applicable for those aircraft parts that are not subject to hostile environments. For other parts, it may be necessary to use more robust security markings,

such as those which can be achieved by acid etching, laser ablation or dot peening. For example, the security mark might consist of a unique combination of letters and numbers etched or engraved onto the part, using a different pattern or combination of letters and numbers for each unique serial number. There should be no obvious correlation between the part's unique identifier and the characteristic pattern or combination of letters and numbers which make up the security mark – although it should be possible for anyone handling the part to verify the part's authenticity via a challenge-response mechanism, whereby they supply both the unique ID and the security mark to a product authentication service provided by the part's manufacturer, which provides a Boolean (YES/NO) response about whether the part is genuine or not.

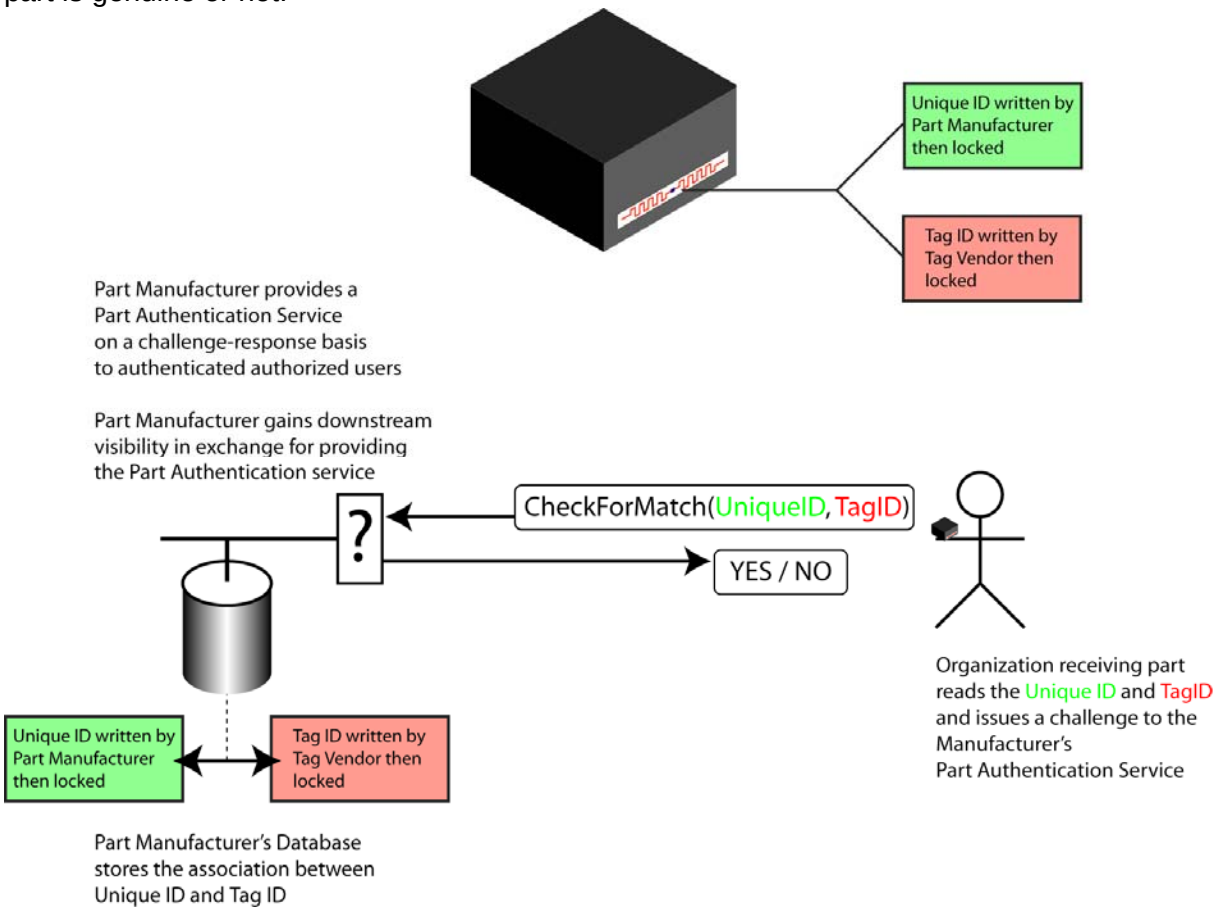

Figure 5. Concept diagram illustrating a challenge-response product authentication service to check that the Unique ID is still bound to the same RFID tag (Tag ID) that was originally tagged with that unique ID.

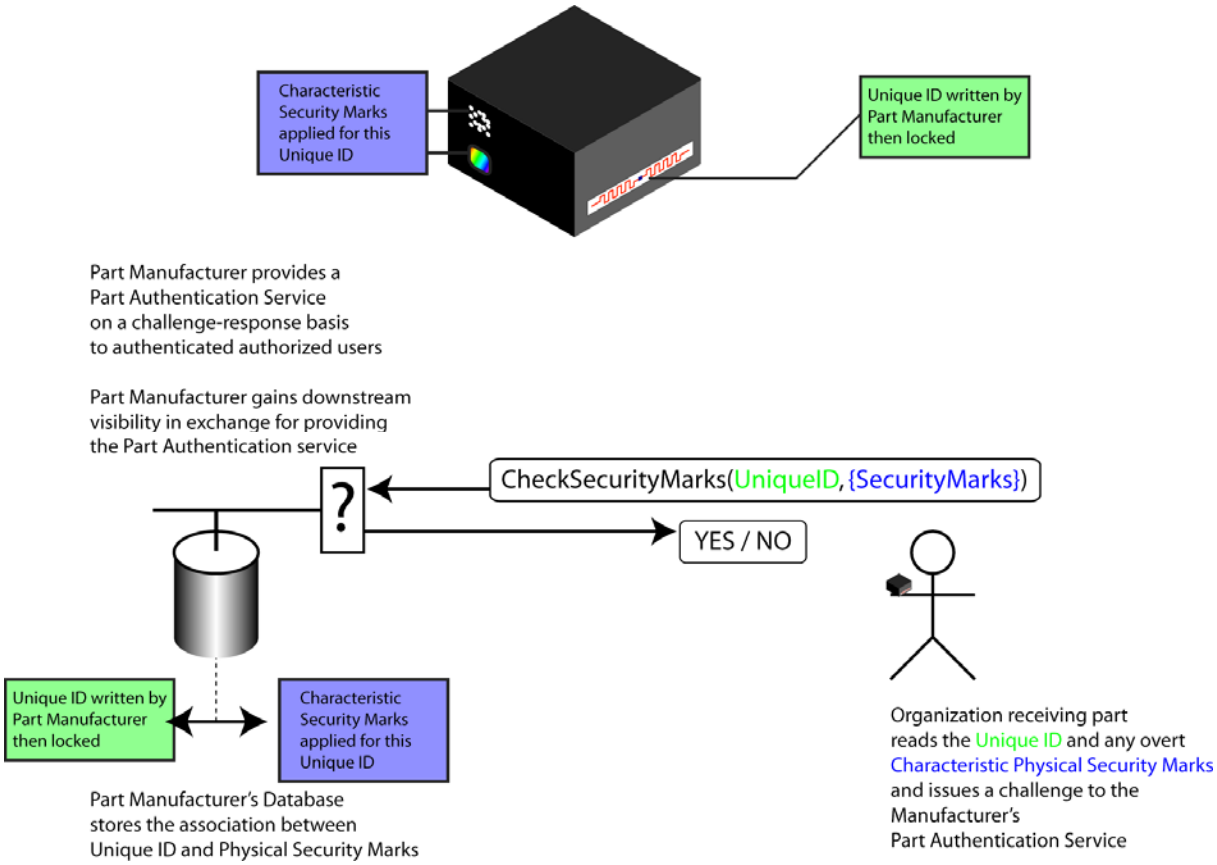

Figure 6. Concept diagram illustrating a challenge-response product authentication service to check that the Unique ID is still bound to the same physical part that was originally tagged with that unique ID.

Checking of the unique ID of a part against security markings on the physical object provides a stronger degree of assurance that the ID actually belongs to that particular part, although such checking may be more difficult to automate. In contrast, cross-checking of the part's unique ID and Tag ID is easier to automate but provides weaker authentication and weaker protection against detection of 'cloned' RFID tags that might not even belong to that part type.

4.3. Authenticity of the data

Digital signatures can be used to provide a much higher level of assurance about the authenticity and integrity of data than can be achieved using traditional handwritten signatures on paper documents. Like a handwritten signature on a paper document, a digital signature is associated with a particular individual (therefore providing for non-repudiation of

the signed data). However, unlike a handwritten signature, a digital signature is also dependent on the precise value of the data being signed, such that if even one bit of the data changed, then the digital signature would be radically altered. It is this feature that provides a mechanism to check the integrity of the data content which has been signed.

Digital signatures that make use of Public Key Infrastructure (PKI) are constructed in a three-step process as follows:

- The data is formatted according to an agreed canonical representation, so that there is no ambiguity about the format or any special control characters, such as line breaks and carriage returns, which may vary between operating systems.
- A message digest is calculated for the data in its canonical format. The message digest is a compact characteristic fingerprint of the document, such that if even just one bit of the data changes, the message digest changes completely. The message digest is calculated using one-way hashing algorithms such as Message Digest 5 (MD5) [34] and variations of the Secure Hash Algorithm, such as SHA-1 [35].
- The message digest fingerprint is then encrypted using the signatory's secret private key in such a way that it is possible to use their published public key (which can be obtained from their digital certificate) to verify that only they could have signed the data.

Further details about digital signatures are provided elsewhere [36] and in AEROID-CAM-007.

5. Enabling decision-making based on lifecycle data

In order to avoid overwhelming staff or information systems with too much data, there needs to be a balance between actionable information vs raw data. In the design of the network database infrastructure and lookup services for supporting lifecycle ID and data management, it is important to consider the routing of data to the users and locations that produce and consume that data – and to allow it to be transmitted securely over a common shared infrastructure or even infrastructure owned by a third party company or rival.

Furthermore, the user interfaces to application software and tools for human beings to use must be carefully designed in a way that is intuitive, not cumbersome – and does not overload the human operators with excessive amounts of data – but rather, presents just the relevant information in a readily accessible way.

5.1. Filtering of data by applications – not human operators

Extracting actionable information or triggers for action may involve some filtering of the raw data to extract only the 'significant events' or the times when the numerical value of a particular data element exceeds a critical threshold value. In terms of human-interface design, the application programs which maintenance mechanics use should be written in a user-friendly way which pre-filters the data and provides a simple audio/visual alert (e.g. stop/go red/green lights or audible beeps), with the application doing the filtering of data, rather than the user having to scroll through the data or filter it.

If the unique identifier is only being used as a cross-reference, to retrieve additional data, then it may not always be necessary to display the unique identifier to the human operator.

If the flight crew are checking that safety equipment (e.g. lifejackets, oxygen masks) is all present in the correct locations, it may only be necessary to raise an alert when equipment is missing – and to alert them to the locations where it is missing – without them needing to know the details of the identifiers.

5.2. Local cache of configuration/expiry/safety data from networked information systems

For example, airline staff using a mobile RFID reader to check that all the required safety equipment is on board an aircraft and has not exceeded its expiry date should be given an application program which accesses pre-loaded cached information about what equipment should be on board that individual aircraft at each location – and the expiry date as recorded in the system of record backend database – and the reader merely checks for the presence of each piece of equipment at each location – and indicates a visual and audible warning if the equipment is not present – or is different from what was expected.

This example illustrates the need for the networked databases to maintain records at a serial-level for the bill of materials or 'configuration' for aeroplanes and sub-assemblies and also to perform time-based tracking of exchange/replacement parts.

6. Conclusions and areas for further work

This paper has identified several aspects of Lifecycle ID and Data management in the aerospace sector. RFID is a key technology to enable more efficient and complete data capture in various maintenance processes, with the added benefit of reducing the number of human errors, compared with manual / paper-based processes – and also generating information in electronic format that can be made available in a timely manner for record-keeping and also further analysis, such as detection of systematic failure trends or underperformance issues. However, RFID has the potential to automatically generate large

volumes of data – so there is a real need for a data processing architecture to ensure that the large volumes of raw event data are efficiently transformed into much smaller volumes of essential information, in order to avoid overloading existing applications, databases and network bandwidth. While automation has potential benefits to reduce the time spent completing or searching paperwork, there is a danger of placing too much reliance and trust in the data that is generated automatically – and a need to check that it is authentic. This applies both to reading of unique identifiers, as well as to data read from tags or received via the network. While some of these checks may still require significant human intervention, it should be possible to perform the checks when parts first enter an organization, at the same time as the accompanying documentation is checked. Following this authentication and verification process, the parts can then be released for use within the organization, with less need for labour-intensive authentication procedures at each stage of use.

There are clearly a number of areas requiring further discussions, prototyping and standardization, in order to enable industry-wide adoption and consistent implementation.

The table below lists some of these areas and suggests some organizations that may take a leading role.

Further work needed	**Organizations which may play a leading role**
EPC Network compatible representation of the ATA Spec 2000 identifier	ATA, Auto-ID Labs, EPCglobal Tag Data and Translation Standards work group, all parties interested in defining appropriate logistic filter values
Categorization of data fields for parts	ATA e-business RFID on Parts work group
Efficient storage of data on tags and translation to non-binary representations	Auto-ID Labs, ATA and EPCglobal Tag Data and Translation Standards work group
Planning for long-term data access via a consistent network interface (e.g. tidy URLs, web services interfaces etc.)	Auto-ID Labs, ATA, SITA, EPCglobal's EPC Information Services (EPCIS) work group
Electronic parts pedigree	ATA, FAA, EASA, Auto-ID Labs EPCglobal's Pedigree work group within their Healthcare & Life Sciences work group
Serial-Level Lookup Services and Product Authentication Services	Auto-ID Labs, SITA, EPCglobal's Discovery Services work group (when chartered)

User-interface to lifecycle data	Airlines, MROs, SITA, ATA
Pre-caching protocol as counterpart to storing additional data fields on the tag's user memory	Auto-ID Labs, SITA, VI Agents, BT, ATA, EPCglobal Overlap with Data Synchronization topic

References

1. Thomas, V., W. Neckel, and S. Wagner. *Information technology and product lifecycle management*. in *IEEE International Symposium on Electronics and the Environment*. 1999.
2. ATA, *Air Transport Association Spec2000 standard*. http://www.spec2000.com
3. Suzuki, S. and M. Harrison, *Data Synchronization*, in *Aerospace ID Technologies Programme*. 2006.
4. Postel, J., *Transmission Control Protocol DARPA Internet Program Protocol Specification - RFC 793*. 1981, USC / Information Sciences Institute. http://www.ietf.org/rfc/rfc793
5. Postel, J., *Internet Protocol - DARPA Internet Program Protocol Specification - RFC 791*. 1981, USC / Information Sciences Institute. http://www.ietf.org/rfc/rfc791
6. Berners-Lee, T., R. Fielding, and H. Frystyk, *Hypertext Transfer Protocol -- HTTP/1.0 - RFC 1945*. 1996, IETF - Internet Engineering Task Force. http://www.ietf.org/rfc/rfc1945
7. *XML - Extensible Markup Language*, W3C - World Wide Web Consortium. http://www.w3.org/XML
8. *Web Services* W3C - World Wide Web Consortium. http://www/w3/org/2002/ws
9. *ASN.1 - Abstract Syntax Notation 1*. http://www.asn1.org
10. Cowan, J. and R. Tobin, *XML Information Set (Second Edition)*. 2004, W3C. http://www.w3.org/TR/xml-infoset/
11. Sandoz, P., Triglias, A., Pericas-Geertsen, S., *Fast Infoset*. 2004, Sun Developer Network, Sun Microsystems. http://java.sun.com/developer/technicalArticles/xml/fastinfoset/
12. Sandoz, P., et al., *Fast Web Services*. 2003, Sun Developer Network, Sun Microsystems. http://java.sun.com/developer/technicalArticles/WebServices/fastWS/
13. *Overview of SGML Resources*, W3C. http://www.w3.org/MarkUp/SGML/
14. *Product Life Cycle Support (PLCS)*. http://www.oasis-open.org/committees/plcs/

http://www.pclsinc.org

15. *PDF Reference*. http://partners.adobe.com/public/developer/pdf/index_reference.html

16. *DOI - Digital Object Identifier*, International DOI Foundation (IDF). http://www.doi.org and ANSI/NISO standard Z39.84-2000 at http://www.niso.org/standards

17. *CrossRef resolution service for Digital Object identifiers*. http://www.crossref.org

18. Berners-Lee, T., L. Masinter, and M. McCahill, *Uniform Resource Locators (URL) - RFC 1738*, in *RFC*. 1994, IETF - Internet Engineering Task Force. http://www.ietf.org/rfc/rfc1738

19. Freed, N. and N. Borenstein, *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*. 1996, IETF. http://www.ietf.org/rfc/rfc2046.txt

20. *XSD - XML Schema Definition*, W3C - World Wide Web Consortium. http://www.w3.org/XML/Schema

21. Orchard, D., *Versioning XML Vocabularies*. 2003. http://www.xml.com/pub/a/2003/12/03/versioning.html

22. Orchard, D., *Extensibility, XML Vocabularies and XML Schema*. 2004. http://www.xml.com/pub/a/2004/10/27/extend.html

23. Paskin, N., *Towards Unique Identifiers.* Proceedings of the IEEE, 1999. **87**(7): p. 1208-1227.

24. Sollins, K. and L. Masinter, *Functional Requirements for Uniform Resource Names - RFC 1737*. 1994, IETF - Internet Engineering Task Force. http://www.ietf.org/rfc/rfc1738

25. Engels, D.W., *On the Design of Globally Unique Identification Schemes*. 2002, Auto-ID Centre white papers. p. MIT-AUTOID-TM-007.pdf. http://www.autoidlabs.org/whitepapers/MIT-AUTOID-TM-007.pdf

26. *CAGE - Commercial and Government Entity*. http://www.dlis.dla.mil/cage_welcome.asp

27. *FAA Form 8130-3, Airworthiness Approval Tag*, Federal Aviation Administration. http://forms.faa.gov/forms/faa8130-3.pdf

28. Vanalstyne, M., E. Brynjolfsson, and S. Madnick, *Why not one big database? - Principles for data ownership.* Decision Support Systems, 1995. **15**(4): p. 267-284.

29. *Domain Name System (DNS)*. http://www.bind9.net/rfc

30. *EPCglobal Object Name Service (ONS) v1.0*. http://www.epcglobalinc.org/standards_technology/ratifiedStandards.html

31. *Web Services Security*, OASIS - Organization for the Advancement of Structured Information Standards. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

32. Androutsellis-Theotokis, S. and D. Spinellis, *A Survey of Peer-to-Peer Content Distribution Technologies.* Computing Surveys, 2004. **36**: p. 335-371.

33. *EPCglobal UHF Class 1 Generation 2 air protocol*, EPCglobal Inc. http://www.epcglobalinc.org/standards_technology/ratifiedStandards.html

34. Rivest, R., *The MD5 Message-Digest Algorithm - RFC 1321*. 1992, IETF - Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3174

35. Eastlake, D. and P. Jones, *US Secure Hash Algorithm 1 (SHA1) - RFC3174*. 2001, IETF - Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3174

36. *IETF/W3C XML-DSig Working Group*. http://www.w3.org/Signature/