Building **R**adio frequency **ID**entification for the **G**lobal **E**nvironment

Trusted Business Interaction

Authors: Oliver Kasten (SAP)

October 2009

This work has been partly funded by the European Commission contract No: IST-2005-033546

About the BRIDGE Project:

BRIDGE (**B**uilding **R**adio frequency **ID**entification for the **G**lobal **E**nvironment) is a 13 million Euro RFID project running over 3 years and partly funded (€7,5 million) by the European Union. The objective of the BRIDGE project is to research, develop and implement tools to enable the deployment of EPCglobal applications in Europe. Thirty interdisciplinary partners from 12 countries (Europe and Asia) are working together on : Hardware development, Serial Look-up Service, Serial-Level Supply Chain Control, Security; Anti-counterfeiting, Drug Pedigree, Supply Chain Management, Manufacturing Process, Reusable Asset Management, Products in Service, Item Level Tagging for non-food items as well as Dissemination tools, Education material and Policy recommendations.

For more information on the BRIDGE project: www.bridge-project.eu

This document results from work being done in the framework of the BRIDGE project. It does not represent an official deliverable formally approved by the European Commission.

This document:

This document presents a model in which the aspects of SC Integrity (including both physical and virtual) can be understood. This model helps (to identify important aspects when) designing an organization-spanning EPC network and to integrate an organizations EPC implementation into an existing EPC network. Based on our model, we can now analyse virtual traces for evidence in both, the physical supply chain as well as the EPC network. To illustrate this, we present examples of integrity violations that can have different causes.

Disclaimer:

This document contains preliminary information and is not subject to any license agreement or any other agreement as between with respect to the above referenced consortium members. This document contains only intended strategies, developments, and/or functionalities and is not intended to be binding on any of the above referenced consortium members (either jointly or severally) with respect to any particular course of business, product strategy, and/or development of the above referenced consortium members. To the maximum extent allowed under applicable law, the above referenced consortium members assume no responsibility for errors or omissions in this document. The above referenced consortium members do not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, satisfactory quality, fitness for a particular purpose, or non-infringement. No licence to any underlying IPR is granted or to be implied from any use or reliance on the information contained within or accessed through this document. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intentional or gross negligence. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you. The statutory liability for personal injury and defective products is not affected. The above referenced consortium members have no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages.

Acknowledgements

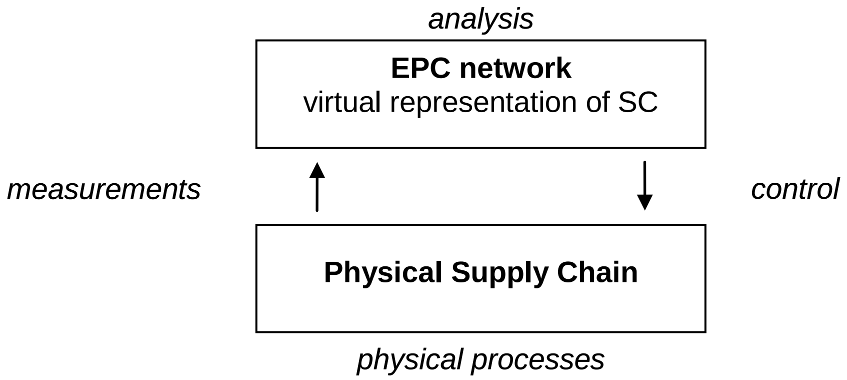
We thank Jeff Farr (BT), Mark Harrison (CAM), and Davide Zanetti (SAP) for their contribution of ideas to this work. Jeff Farr (BT), Alexander Ilic (ETH), Davide Zanetti (SAP) and Mark Harrison (CAM) also contributed to a previous version of this document.

Contents

1 Introduction

Maintaining the integrity of the supply chain is a critical factor for business success. Detecting integrity violations is the first step to maintaining their integrity. In this document we discuss how to maintain supply-chain integrity using the EPC network as a tool for the analysis of virtual product traces. Concretely, we look for evidence of inconsistencies in the trace data. A similar approach has been taken in so-called integrity verification programs, which are used monitor integrity in computer security [NIST-95].

The quality of the integrity analysis of the physical supply-chain now critically depends on how much the EPC network is able to capture a true image of the processes in the physical supply chain. And on how faithful it can reproduce this image at the time of analysis to the analysing party. In this document we use the term EPC network integrity as the ability to measure and reproduce a true image of the physical supply chain for a concrete application.



Moreover, the EPC network is used to control the physical supply chain. False information in the EPC network can directly lead to problems in the physical supply chain. The integrity of the physical supply chain depends on the quality of its analysis, which in turn depends on the integrity of the EPC network.

However, there is no commonly accepted standard of how the EPC network measures and reproduces the physical supply chain. In fact, each organization that contributes a small part to the EPC network, may have different standards. Supply chains consist of multiple partners from different domains (e.g., pharmaceutical industry, logistics providers, wholesalers, hospitals and pharmacies). These have different goals and may be subject to different legislation, service level agreements, and company-internal policies. In fact, each partner in the supply chain may have very different standards on what and how they measure and how much of the captured information they share. Virtual traces may be measured and reproduced quite differently, depending on the organizations that participate in the relevant part of the EPC network. As a result, a virtual trace retrieved from the EPC network may be significantly different from what one may expect, even though each participant’s part of the EPC network functions as designed by *their* organizations.

These different standards are the reason why the same pattern in virtual trace data may be evidence of an actual violations to the physical SC, why it may be evidence of violations to the EPC network integrity, or why it may be simply an artefact of a peculiar but (formally) correct configuration of the EPC network.

Therefore to analyze data from the EPC network it is absolutely critical to not only understand the physical SC processes but also to understand all aspects of how the supply chain’s concrete partners gather and share information in their part of the EPC network. Failing this understanding results in poor quality of the virtual-traces analysis. It will produce many false alarms and will lead to missing actual integrity violations.

To address this problem, this document contributes by presenting a model in which the aspects of SC Integrity (including both physical and virtual) can be understood. This model helps (to identify important aspects when) designing an organization-spanning EPC network and to integrate an organizations EPC implementation into an existing EPC network. Based on our model, we can now analyse virtual traces for evidence in both, the physical supply chain as well as the EPC network. To illustrate this, we present examples of integrity violations that can have different causes.

The examples illustrates that rules for the analysis of supply-chain traces are so varied as supply-chain participants themselves. Therefore, we argue that standard integrity-analysis methods cannot be applied to arbitrary supply chains. Though there may be much commonality among the integrity-analysis methods among supply-chain participants, participants need a way to adapt the analysis to their concrete environment. To this end, two prototypes have been designed and implement in the context of BRIDGE's Task 6.4. Both prototypes use the rule-based approach to integrity checking. They are software tools that allow to easily adapt and configure their integrity-analysis methods to the supply-chain environment at hand.

The remainder of this document is structured as follows. Section 2 discusses the various aspects of supply-chain integrity. Section 3 discusses how to detect integrity violations by analysing trace data. Finally, Section 4 briefly presents the two prototypes for analysing trace data, which have been developed in the context of this task.

2 Supply-Chain Integrity

The term integrity (besides its meaning in ethics) typically refers to the state of being whole, entire, and undiminished. The concrete meaning of the word then largely depends on the context in which it is used. An appropriate definition of integrity for supply chains is the requirement that *the system performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation* (see, for example, [NIST-95]).

To study this issue further, we first define and distinguish between the two primary elements of the supply-chain system itself:

- the **physical supply chain** and
- the **EPC network** (more generally, the IT infrastructure)

We will define a supply-chain integrity violation to have occurred when *either* of these systems deviate from their intended functions.

The *physical supply chain* is centred on the physical objects being transported (i.e., the actual products, containers, vessels), on the associated work processes (i.e., the processes that eventually distribute those items through the supply chain), and the involved parties. In this category we also want to consider documents that are physically exchanged and/or accompany goods in the supply chain, such as customs forms and delivery orders.

The second element is the *information technology (IT)* used throughout the supply chain in order to gather and analyse information about the physical supply chain. Since the information gathered through IT is often used to make decisions on physical supply-chain processes, the integrity of supply-chain IT directly influences physical supply-chain integrity. With respect to IT, we will focus on the *EPC network* in this document. This is, in its most general sense, the RFID-based system designed to measure, record, analyse, distribute, and model the physical reality of the real-world supply chain (see [EPCnet]). We can say that the data gathered through the EPC network represents a virtual, discrete image of the physical supply chain and the items contained within it.

Before discussing both supply chain elements in detail in Subsections 2.3 and 2.4, respectively, we first discuss two other important aspects. Firstly, we discuss where the concrete conditions of integrity are defined for supply chains and who defines them. And secondly, we discuss the difference between accidental and deliberate integrity violations.

2.1 Regulations and Authorities Defining Integrity

When analysing the EPCIS events in a supply chain, one may come across obvious inconsistencies. However, these inconsistencies may not actually be violations to the EPC network integrity, simply because there is no regulation mandating the absence of the inconsistency. Let us consider a simple example: a product is shipped from one company to another. It would be generally considered an error if the time stamps of the associated events indicate that the products has been received before it has been shipped. However, the EPCIS specification does not mandate that shipping has to occur before receiving. In fact, EPC global specifications typically give their adopters a large degree of freedom regarding their use. This means, however, that many aspects of integrity need to be defined in other regulations.

Supply chains include several organizations, such as manufacturers, distribution centres, logistics providers, and retailers. These organizations typically have different roles and goals, and are subject to different legislations, service level agreements, and partner expectations. Therefore, the intended operation of a supply chain is not set forth in a single consistent document but may be a conglomeration of applicable legislation, specifications, agreements, and policies. Each participating organizations' definition of the intended function and operation of (its part of) the supply chain may vary considerably. In fact, it is not unlikely that an organization has only an implicit notion even of their role in the supply chain.

We classify the different regulations that have a role in writing (and so collectively defining) the purpose and intended operation of the supply chain. Supply-chain integrity can then be classified according to which regulation defines correct operation. It is important to note that this classification applies to regulations in both the physical supply chain as well as the EPC network. The classifications we use are:

- **Intra-organisational specifications**: Specifications internal to an organization or a specific company site, such as company policies and codes of conduct.
- **Inter-organisational contracts**: Contractual commitments and SLAs (service-level agreements) signed between individual collaborating participants, such as, a manufacturer and a retailer, or a supply chain partner and its third-party IT provider.
- **Third-party regulations**: Standards applicable to multiple organizations, typically established by authorities and organizations not directly involved in the physical supply chain. These include international and local regulations, for example, the “Standards for Securing the Drug Supply Chain” by the US Food and Drug Administration [FDA], as well as formal and industry IT standards, for example, EPCIS and EDI specifications.

When studying integrity violations, it is important to get a complete picture of the regulations and the authorities that influence the intended function of the supply-chain system, both from the physical and IT perspective. We will now discuss the three levels of regulations in the context of EPC network integrity in more detail.

Regulation Category	**Examples**	
	Physical supply chain	***IT/ EPC network***
Intra-organizational specifications	Code of conduct for employees	Company IT policy
Inter-organizational contracts	Contracts with subcontractors (e.g., logistics providers) that handle physical items	Agreements on the sharing and use of RFID data with supply chain partners; SLA with a company’s internet service provider
Third-party regulations	Standards for Securing the Drug Supply Chain by the FDA	ONS and EPCIS specifications by GS1

2.1.1 An Analogy

To clarify this classification for EPC integrity, we might consider the analogy of the World Wide Web. ‘Broken links’ on the Web are a common occurrence, and significantly impede the successful use of the Web. However, they do not actually contravene W3C standards, and so they do not, by that definition, represent a breach of the system’s integrity. On an intranet, however, a particular company might well have an internal policy that prohibits broken links within their network. Within the context of their organisation then, and that small part of ‘the Web’, any broken link there would constitute a breach of the system’s integrity.
In the case of the EPC network, there are two important distinctions from the Web analogy. Firstly, although a prime purpose of the EPC network is to accurately model (some dedicated aspects of) the real world, there is almost nothing in the current formally-defined standards to capture this. Therefore, other forms of documentation, which may capture this, are very important in this context. A second possible distinction is in the significance of such integrity breaches. Whilst the Web is intended for a very wide range of purposes, and an individual ‘broken link’ may prove inconvenient, the EPC network is intended specifically for business purposes and any failures may therefore be of critical business importance. The EPC network may thus demand more thorough attention to its integrity than does, say, the Web.

2.1.2 Intra-organizational Specifications

A first level of regulations at which the intended operation of the EPC network can be specified is within individual organisations. The majority of organisations will themselves have an inherent motivation to ensure that their systems accurately reflect the reality of their physical systems. It is likely that their RFID reader infrastructure, in particular, will have been carefully designed and specified so as to meet the demands for accuracy and dependability placed upon it. Hence local policies, developed internally by individual organisations, play some role in defining the expected operation of the EPC network.

2.1.3 Inter-organizational Contracts

This category captures the intentions of the EPC network as specified in SLAs and contracts agreed between co-operating supply-chain participants, and in legislation used to regulate particular industries. We expect these legal commitments to describe the goal of the EPC network as an accurate reflection of the real world and to require that participating parties truthfully collect and share their information with particular other parties. In many supply-chain environments, each partner may be obliged to record and share certain real-world information, and with a specified accuracy and robustness. Contraventions to such commitments constitute a second form of integrity violation to the integrity of the EPC network. This form of integrity is not a general property of the entire EPC network but is instead highly dependent upon the business context and the agreements between individual business partners.

2.1.4 Third-party Regulations

Some aspects of the intention of the EPC network are well captured by EPCglobal standards. For example, those standards specify who can assign valid EPC numbers, which software components can inject data into an EPCIS, and the data fields that are mandatory in the event records. Non-compliance with any of the requirements specified in these standards constitutes a violation to EPC network integrity.

In this category, we also include breaches in any of the other IT standards that are widely employed within the EPC network. For example, if Discovery Services are finally specified by the IETF (rather than EPCglobal) then that specification too is likely to become a de facto part of the EPC network. Similarly for the global and national standards defined by other industry consortia for different industry sectors.

2.2 Accidental and Deliberate Integrity Violations

When studying integrity violations we also want to consider the cause of failure. Integrity violations can be caused unintentionally (e.g., accidentally, or carelessly) or deliberately (due to selfish, malicious, or possibly altruistic reasons). At the physical supply-chain level, for example, items can be misplaced either consciously to avoid a manual effort to move them around, or inadvertently due to incorrect information about their designated storage location. The EPC-network integrity could be deliberately violated, for example, to hamper the interpretation of trace data for anti-counterfeiting purposes or to cover up contractual failings and compliance violations. Its integrity could be compromised unintentionally due to careless mis-configuration of hardware (such as computer clocks) and software components (such as over-restrictive access-control policies in a shared database).

2.3 Physical Supply-Chain Integrity

Physical supply-chain integrity is the traditional definition of supply-chain integrity and refers to the properties and characteristics of physical entities (such as products, logistic units, organizations, and individuals) as well as of the processes in which those entities interact in the supply chain. A literature and Web search reveals a wide range of meanings associated to the term supply-chain integrity, which largely depend upon the industry sector in which the system operates. In fact, at this physical level there are relatively few processes that are completely generic to all industries, and so the detailed definitions of integrity vary considerably. Definitions of supply chain integrity include:

- food and product safety (e.g., temperature control in the cold-chain)
- regulatory compliance and correct handling of goods, (e.g., cold chain temperatures, quality control, customs)
- absence of tampered products (i.e., unauthorised product manipulations, e.g., re-labelling of Intel Pentium processors)
- absence of tampered containerised cargo (i.e., exchange, removal, and additions of cargo between/ from/ to a container) including cargo theft
- absence of store misplacements and wrong deliveries of products and shipments
- absence of counterfeit products, diversion, parallel trade, and smuggling
- bona fides organizations (e.g., suppliers, distributors, or outsourced service providers such as packagers, forwarders, and advertising agents)
- absence of corruption and fraud

2.4 EPC-network Integrity

As stated previously, the general (although largely implicit) purpose of the EPC network is that it acts as a measurement and recording system to accurately model real-world supply chains. Therefore, supply-chain integrity can also be understood as the integrity of the entire system of hardware, software (including their actual implementation at the supply-chain partners), and data, which, in this document, we will loosely refer to as the EPC network. The EPC network consists of tags, readers, reader management infrastructure (ALE), network infrastructure (typically the Internet), and services (EPC Information Services and Discovery Services). The EPC network is a distributed information system to which the notion of information-system integrity can be applied.

The definition of integrity has been, and continues to be, the subject of much debate among computer security experts [NIST-95]. In computer security, integrity is often discussed as having two facets: data integrity and system integrity. “Data integrity is a requirement that information and programs are changed only in a specified and authorized manner" [NRC-92]. System integrity is a requirement that a system "performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system" [NRC-88].

Other qualities of computer systems are availability and confidentiality, which together with integrity comprise computer security. In the scope of this document we will also be looking at availability inasmuch it may affect the intended use of the system. Availability is a "requirement intended to assure that systems work promptly and service is not denied to authorized users."

While all previously discussed aspects of integrity have been intensively studied for computer systems in general, and for the EPC network in particular (for example, in BRIDGE WP4), in this document we want to focus on those aspects relevant for supply-chain integrity and the detection of its violations. Concretely, we consider the following aspects, which we discuss below:

1. System and Data Integrity

2. Availability, Reliability and Robustness
3. Information Sharing
4. Data-Model Quality and Data Quality
5. Use of EPC numbers

2.4.1.1 Data and System Integrity

Examples for this category are:

- unauthorized injection of events (i.e., insertion into EPCISes and DSes by unauthorized parties, even if these events are true observations, e.g., cloning and replay of trace data)
- unauthorized modification and deletion of events, in EPCISes, DSes, as well as in transit during network communication
- unauthorized modification of system configurations

These properties largely depend on the definition of who is authorized to create, modify, and delete events. To protect their part of the EPC network, companies can use standard security mechanisms, such as access control. However, fraudulent partners in the supply chain may deliberately inject false events into the EPC network, for example, to cover up counterfeit injections.

2.4.1.2 Availability, Reliability, and Robustness

Since the EPC network inherently depends on such components, failure in hardware and software components also affects its operation and potentially its integrity. Although in computer science these issues are typically related to the notion of robustness and availability (rather then integrity), we also want to consider:

- hardware failures in the EPC network (including tags, readers, server hardware, the network, etc.).
- availability of the EPC network components, such as the ONS, DS, and the EPCISes of the relevant supply-chain partners
- anomalies in the RFID reads, such as bit-flips, missed reads, over ranges
- malformed query replies, (e.g., missing mandatory fields in observations and incompatible data formats)

2.4.1.3 Information Sharing

The EPC network can only perform its intended function, if all required parties (truthfully) collect and share their information with partners that depend upon them. In some supply-chain environments, for example, each partner may be obliged (by law or by contract) to record and share certain events. In general we expect that supply-chain partners mutually engage in (service level) agreements that mandate which information is to be shared. Violations to such agreements constitute a violation to the integrity of the EPC network. This form of integrity is not a general property of the entire EPC network but instead is highly dependent on the business context and the agreements between business partners. Missing trace information from a business partner may clearly hamper the supply-chain integrity analysis and may lead to incorrect control decisions or false alarms.

2.4.1.4 Data-Model Quality and Data Quality

In this document we defined the term EPC network integrity as the ability to measure and reproduce a true image of the physical supply chain for a concrete application. Part of that definition then is the integrity of the data model, that is, the requirement that the data model actually *can* represent the reality sufficiently well for the task at hand. In other words, do the semantics of the data model allow to draw the conclusions we want. This requires a common standard among supply-chain participants, which aspects of a given physical process must be recorded, what the recorded information actually means, and how this information is represented (i.e., the data format).

This type of integrity condition is typically related to the design of data structures used throughout the supply chain's EPC infrastructure, and particularly the fields of EPCIS events that an organization records and makes available through the EPC network. EPC global specifications provide guidelines on the meaning of data fields which can be used as a starting point for such standards. However, they are not binding.

Another aspect closely related to the quality of the data model is the quality of the data itself. (We deliberately avoid the term data integrity since this term has a different meaning in the filed of computer security.) Data quality is the requirement that the data (values) in the EPC network actually do represent the reality well enough for their intended use. This is closely related to the quality and configuration of the "sensor" equipment used to record data. Examples are:

- absence of incorrect event attributes, such as time stamps generated by a clock that is incorrectly set, defective, or does not provide the required precision (resulting in errors in the eventTime of EPCIS events)
- the values of event fields have the required granularity for a specific application, for example, they are not unduly discretised (e.g., by stripping of hours, minutes, or seconds from a time stamp)

More generally we require the absence of false events, that is, events implying that the reality was different than it actually was (regardless if the party generating the false events is actually authorised to generate events in the first place). It is worth noting that while a system may have integrity from an system's perspective, it may not at all truly represent the (and be consistent with) the real world, in our case, the actual flow of products in the physical supply chain. EPC global specifications do not mandate that EPCIS events reflect the observed reality.

We expect that companies will sometimes create EPCIS events for EPCs without actually having observed the physical products, that is, by reading the RFID tags. For example, the reception of a tagged pallet (e.g., an SSCC) may be used to infer that a particular item has arrived with the pallet based on an advanced shipment notice (ASN), subsequently generating a receiving event for the item. We call these events synthesized. The synthesis of new events from existing events and other information may be a particularly error-prone process. Synthesized events always bear the risk of being false, either because the inference algorithm proves to be flawed, or because the original information the synthesized event was based on was incorrect in the first place.

In our example, the inference that the item has arrived with the pallet is wrong if the item had in fact been surreptitiously unloaded from the pallet or if the ASN proved to be incorrect. For this reason we think it is likely that the storage of synthesised events in EPCISs should be minimised and their use reserved for application-level analytical track & trace services (see BRIDGE Work Package 3).

2.4.1.5 Use of EPCs

A integrity property specific to the EPC network concerns the use of EPC numbers.

- using invalid EPC numbers (a malicious party may hijack EPC numbers assigned to an authorized party and use them for its own products, potentially to mask counterfeiting or diversion)

- using the same EPC number for multiple products at the same time, which could be a consequence of tags cloning, that is, creating a new tag using the EPC number (and possibly the tag id--a supposedly unique hardware number) of an existing tag

Interestingly, very few of the integrity properties we discussed throughout this subsection above actually depend on EPC global specifications. The majority of integrity properties need to be defined by companies bilaterally.

2.5 A General Model of Supply-Chain Integrity

This section attempts to provide a fairly simple but broad-ranging model in which all the issues relating to supply-chain integrity can be more clearly understood. The intention is to produce a simple description that can be used by the EPCglobal community and EPC practitioners alike, inside and outside of the BRIDGE consortium.

The table below summarises the key classifications and concepts described in this section in a comprehensive model of supply-chain integrity. The categories of regulations that define integrity are, however, omitted to improve readability. The table cells present a variety of example integrity violation in each of the identified categories.

Finally, it is worth noting that our model of supply chain integrity clearly omits some other important, related systems, such as Electronic Data Exchange (EDI) [EDI] exchanges and the Global Data Synchronisation Network (GDSN) [GDSN]. It is possible that failures in those systems might have consequences on our domain of interest, and so, ultimately, they might need to be considered in a yet more comprehensive analysis of integrity.

2.6 Summary

This section has described a comprehensive model of supply-chain integrity, and has shown how the integrity of the EPC network (as defined by various sets of regulations and authorities) can be compromised. We anticipate that the model will be particularly useful in scoping the types of faults that a particular integrity mechanism is designed to manage, and in helping to ensure that (ultimately) adequate mechanisms are in place to handle the entire set of threats. Whilst there is clearly scope for some innovation in these mechanisms, it will also be apparent that we should easily be able to re-use many of the established integrity-supporting mechanisms already developed for other types of information system.

It should now also be clear that some of the work on the EPCIS-specific access-control framework (in the Network Confidentiality task of this work package) plays a strong role in preventing the injection of false information into the network by unauthorised parties, and so contributes to the maintenance of EPC-network integrity.

Supply Chain Integrity Categories	***Examples of Integrity Violations***	
	accidental, unintentional	*intentional*
Physical Integrity	misplacements/ misdirection/ mislabelling of products, delivery delays	theft, introduction of counterfeit products into the supply chain, sabotage
EPC-Network Integrity		
Data and system integrity	accidental deletion of EPCIS events (e.g., during database maintenance)	generating fake commissioning events in the genuine manufacturer's EPCIS to conceal counterfeiting
Availability, reliability,	EPCIS downtimes due to	

robustness	network failure, broken RFID tags	
Information sharing	misconfiguration of access-control policies of DS and EPCIS	intentionally denying access to certain data
Data-model quality and Data quality	events contain incorrect time stamps (due to broken or incorrectly set computer clock); incorrectly synthesized EPCIS events	injecting false events, e.g., to cover up contractual failings
Use of EPCs	accidental reuse of EPC number for multiple products	use of unauthorized EPC numbers; “tag cloning”, i.e., intentional reuse of EPC number for multiple products

3 Detecting Integrity Violations

In the previous section we have presented our model of supply-chain integrity. In this section we try to answer the question of how to detect integrity violations. One approach for detecting violations to supply-chain integrity is to look for evidence in the EPC trace data. We will explore this approach by giving examples of what evidence can be extracted. The overall goal of this section is to understand how far we can get using this approach and to learn the requirements and general structure of rules so they can be specified for use in automated integrity tools.

3.1 Example: Finding Evidence for Theft

In the following we will discuss in detail a specific violation to physical supply-chain integrity, namely the theft of goods in-transit, that is, during transportation from one supply-chain partner to the next. In particular, we will preset approaches to detect evidence of this kind of integrity violation from EPC-network trace data and other information sources.

A simple (but possibly over-simplistic) approach for detecting theft of goods in-transit is to count the number of products (more precisely, the number of distinct EPC numbers) within a certain shipping unit both at the shipper and the receiver, and matching the numbers. A smaller count at the receiving end compared to the shipping end of the transportation link may indicate theft. However, such an approach could be easily deceived by replacing the stolen goods with other (cheaper) RFID-tagged products or just RFID tags. (Unauthorised goods replacement constitutes another integrity violation in itself.)

A more sophisticated approach would be to match the (received versus shipped) identities. The rule could be formulated as: *All identities associated with a shipping unit at the sender must arrive with that shipping unit at the receiver.* This approach could also detect replaced products in a shipping unit. However, it would be still susceptible to replacing the original products with cloned tags carrying the genuine products' identity.

We could also think of a situation where there is a distributor between the sender of goods and their receiver. If that distributor does not take part in the EPC network or does not share events with either side, the above approach would produce false alarms if the distributor (permissibly but unexpectedly) exchanges products between shipping units, for example, in order to optimize transportation. In this case one of the following two adapted approaches may be more suitable:

- *All items of a delivery must arrive before the next delivery*. This approach assumes a FIFO (first-in, first-out) ordering, that is, all items of a shipment are received before any item of a later shipment is received. In the face of priority shipments, this may not always be that case.
- *No item that belongs to a certain shipment does arrive later than* n *units of time after any other item of the same shipment.* This approach assumes that there is a deadline after which all items should have arrived. Only if the deadline is passed, an alarm indicating the potential theft is raised. This deadline depends on several factors, such as the transportation means and the processes at the distributor.

3.2 Same Evidence, Different Causes

An interesting observation is that a missing event could also be caused by violations to the EPC network integrity. Reasons (different from theft) why events could be missing are:

1. the event has been accidentally deleted during database maintenance

2. reading the RFID tag failed (e.g., due to a defective reader or non-optimal read rates from collisions, shadowing, etc.)
3. the remote EPCIS was offline when the event in question was to be retrieved (thus the event is only missing for the analysis but otherwise available)
4. the remote EPCIS is (accidentally or deliberately) configured to withhold the events in question

According to our model of integrity, the above reasons fall into the following subcategories of EPC-network integrity:

1. Data and system integrity
2. Availability, reliability, robustness
3. Availability, reliability, robustness (again)
4. Information sharing

In an honest world without theft, the approaches described previously could be used verbatim to detect these violations of the EPC-network integrity. This little example illustrates that EPC trace data cannot only be used to find evidence for physical supply-chain violations, but also for integrity violations of the EPC network.

3.3 False Alarms

In the previous section we pointed out that we must be careful not to interpret failed RFID reads as theft. Even in the case of an excellent RFID read rate of 99.999% (i.e., a miss rate of 0.001%) there is still one missing RFID read in 100,000 reads. If large volumes of items are processed, this could lead to a high number of false alarms.

In order to fix our previous example on theft in the face of failed RFID reads, we could include read events from multiple readers in the same company. More readers may be installed on the company site to observe other processes, such as shipping to the next partner in the supply chain.

3.4 Summary

In this section we have shown that it is indeed possible to detect integrity violations based on EPC traces (although there are situations where deciding which kind of violation exactly caused the evidence is ambiguous). Concretely we can formulate rules that evaluate this data in order to detect evidence of integrity violations. We have illustrated such rules using a concrete example, namely detecting theft during transportation of goods.

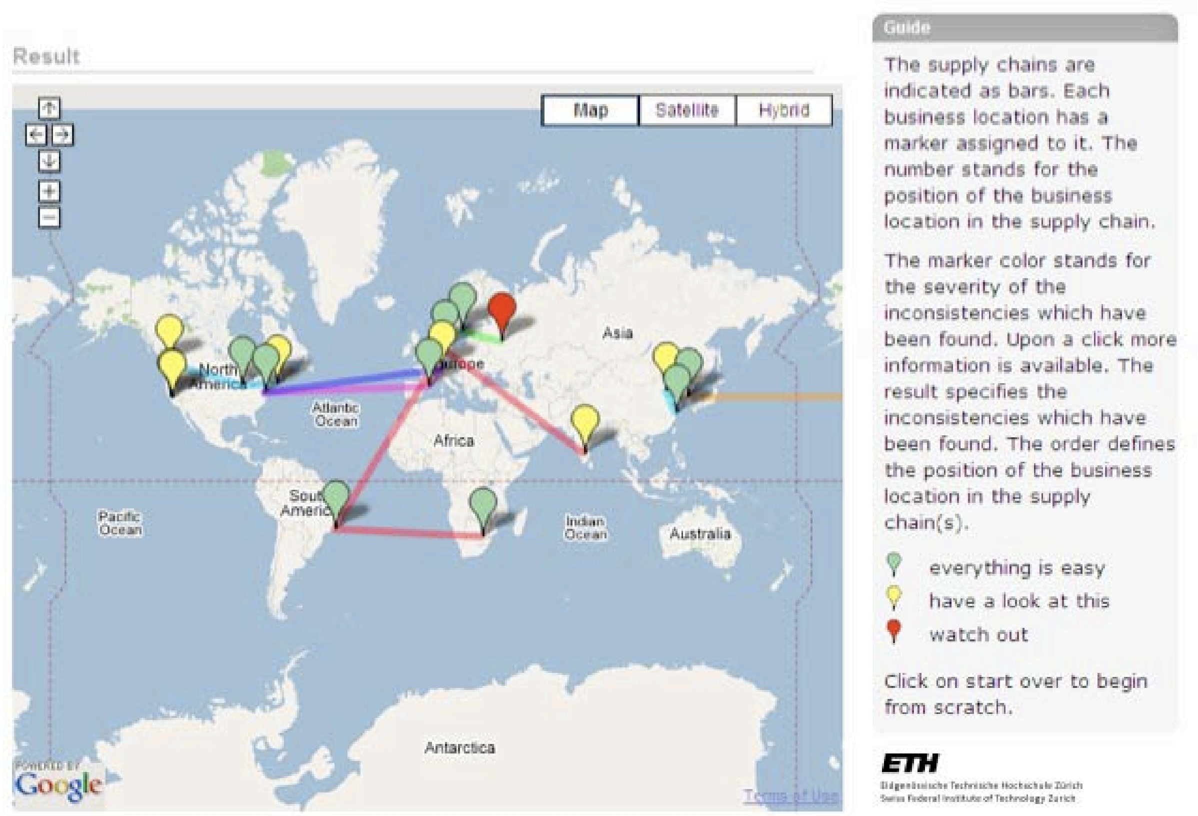
Our examples suggest that there is no single best rule for detecting integrity violations. Clearly the concrete rule chosen should be carefully adapted to the situation or otherwise many false alarms can be expected, or, even worse, actual theft is not detected. As a consequence, a tool supporting the detection of evidence must be flexible enough to cover a wide range of situations and should allow to dynamically modify integrity-checking rules.

4 Rule-based Integrity Checking

In the previous section we have shown how to detect evidence of integrity violations using rules over EPC trace data (and possibly other data, such as advanced shipment notices). In the context of BRIDGE two prototypes using the rule-based approach to integrity checking have been designed and built as configurable software tools.

4.1 Supply Chain Visualizer

The first prototype has been designed and built by ETH Zurich. It is targeted at a managerial audience and entitled “Supply Chain Visualizer”, as its primary goal is to make supply-chain integrity violations visible to the supply-chain manager. The Supply Chain Visualizer displays “hot spots” to indicate weak links and integrity violations in the supply chain. It provides bottom-up supply-chain consistency and performance analysis based on EPC-trace data. Below is a screenshot of the prototype.



Guide

The supply chains are indicated as bars. Each business location has a marker assigned to it. The number stands for the position of the business location in the supply chain.

The marker color stands for the severity of the inconsistencies which have been found. Upon a click more information is available. The result specifies the inconsistencies which have been found. The order defines the position of the business location in the supply chain(s).

🟢 everything is easy
🟡 have a look at this
🔴 watch out

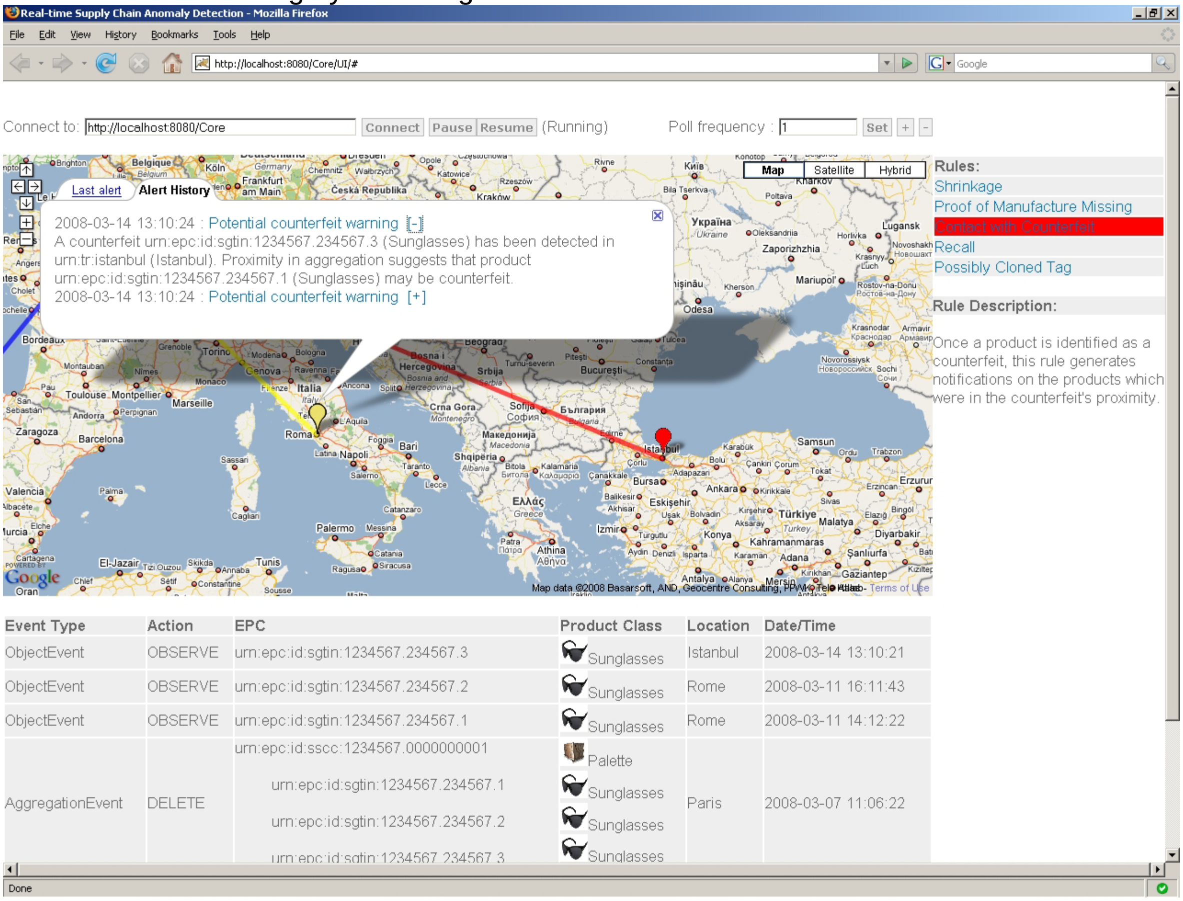
Click on start over to begin from scratch.

A previous version of the Supply Chain Visualizer has been described in the previous version of this document [BRIDGE-461]. For a recent description see [Ilic-09a, Ilic-09b]. The tool has also been presented at the Internet of Things Conference 2008 in Zurich, Switzerland, in 2008 and at the Auto-ID Labs Research Meeting, in Hong Kong, China, in 2007.

4.2 Rule-based Integrity Checking Framework

The second prototype, the Rule-based Integrity Checking Framework, has been designed and built by SAP. Its main goals are its general applicability and configurability for all kinds of integrity applications. To prove the point, the framework has been configured to specifically analyse trace data regarding evidence of counterfeits in BRIDGE’s Anti-counterfeiting workpackage (WP5).
The tool provides a general language in which rules can be expressed in first-order logic over trace data. The language allows to formulate application specific rules, which can be added

and modified during the tool’s runtime. Rules that fire trigger alerts, which can be displayed in a graphical user interface or delivered via email and text messages. Below is a screenshot of the Rule-based Integrity Checking Framework.



Connect to: http://localhost:8080/Core (Running)

Poll frequency : 1

2008-03-14 13:10:24 : Potential counterfeit warning [-]
A counterfeit urn:epc:id:sgtin:1234567.234567.3 (Sunglasses) has been detected in urn:tr:istanbul (Istanbul). Proximity in aggregation suggests that product urn:epc:id:sgtin:1234567.234567.1 (Sunglasses) may be counterfeit.
2008-03-14 13:10:24 : Potential counterfeit warning [+]

Rules:
- Shrinkage
- Proof of Manufacture Missing
- Contact with Counterfeit
- Recall
- Possibly Cloned Tag

Rule Description:

Once a product is identified as a counterfeit, this rule generates notifications on the products which were in the counterfeit's proximity.

Event Type	Action	EPC	Product Class	Location	Date/Time
ObjectEvent	OBSERVE	urn:epc:id:sgtin:1234567.234567.3	Sunglasses	Istanbul	2008-03-14 13:10:21
ObjectEvent	OBSERVE	urn:epc:id:sgtin:1234567.234567.2	Sunglasses	Rome	2008-03-11 16:11:43
ObjectEvent	OBSERVE	urn:epc:id:sgtin:1234567.234567.1	Sunglasses	Rome	2008-03-11 14:12:22
AggregationEvent	DELETE	urn:epc:id:sscc:1234567.0000000001 urn:epc:id:sgtin:1234567.234567.1 urn:epc:id:sgtin:1234567.234567.2 urn:epc:id:sgtin:1234567.234567.3	Palette Sunglasses Sunglasses Sunglasses	Paris	2008-03-07 11:06:22

For a in depth description of the Rule-based Integrity Checking Framework please refer to [BRIDGE-54]. The framework has also been presented at the Internet of Things Conference 2008 in Zurich, Switzerland.

5 Bibliography

[BRIDGE-41] EU FP6 IP Project “BRIDGE: Building RFID Solutions for the Global Environment”. Deliverable D-4.1.2 *A Threat Model Analysis of EPC-based Information Sharing Networks, 2007*

[BRIDGE-54] EU FP6 IP Project “BRIDGE: Building RFID Solutions for the Global Environment”. Deliverable D-5.4*, Anti-counterfeiting Prototype Report, 2008*

[BRIDGE-61] EU FP6 IP Project “BRIDGE: Building RFID Solutions for the Global Environment”. Deliverable D-4.6.1 Interim report on *Dynamic Supply Chain Operations and Integrity*, 2007

[EDI] *Electronic Data Interchange*, Wikipedia, The Free Encyclopedia, 18 December 2007, 13:25 UTC, Available at: http://en.wikipedia.org/w/index.php?title=Electronic_Data_Interchange&oldid=178713359, accessed December 21, 2007

[Eurich-09] M. Eurich and N. Oertel, *Interorganisationales Teilen von Ereignisdaten auf Stückebene: Gegenwärtige Barrieren und Möglichkeiten zu deren Überwindung*," SAP Research. To be published.

[FDA] U.S. Food and Drug Administration, Standards for Securing the Drug Supply Chain - Standardized Numerical Identification for Prescription Drug Packages, Guidance for Industry, available at http://www.fda.gov/RegulatoryInformation/Guidances/ucm125505.htm, accessed May 22, 2009

[Fearne-00] Andrew Fearne and David Hughes, *Success factors in the fresh produce supply chain - Insights from the UK*, British Food Journal, Vol. 102 No. 10, 2000, pp. 760-772. Available at http://www.wye.imperial.ac.uk/CFCR/pdfdoc/fresh-produce.pdf

[GDSN] GS1 GDSN (Global Data Synchronisation Network). Available at http://www.gs1.org/productssolutions/gdsn/, accessed December 21, 2007

[Ilic-09a] A. Ilic, T. Andersen, F. Michahelles, *Increasing Supply Chain Visibility with Rule-Based RFID Data Analysis*, IEEE Internet Computing, vol. 13, no. 1, pp. 31-38, Jan./Feb. 2009

[Ilic-09b] A. Ilic, T. Andersen, F. Michahelles, *EPCIS-based Supply Chain Visualization Tool*, Auto-ID Labs White Paper, 2009

[NIST-95] National Institute of Standards and Technology, An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, Oct 1995. Available at http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

[NRC-92] National Research Council, *Computers at Risk*, Washington, DC: National Academy Press, 1991.

[NRC-a] Department of Defense, *Glossary of Computer Security Terms*, Pub. NCSC-TG-004, National Computer Security Center, Ft. Meade, MD 20755 (Oct. 1988). Also known as the "Teal Green Book." Available at http://packetstormsecurity.org/docs/rainbow-books/NCSC-TG-004.txt