eration WMS software by applying innovative technology to enhance operations in industrial warehouse environments. This includes:

- a set of Java Platform, Enterprise Edition (J2EE) interfaces for interoperability and mobile services, enabling communications between planning components across a network
- a mobility interface, allowing remote users (e.g., truck drivers) to report planning changes
- new interactive modules combining constraint programming and virtual reality, in support of modelling, simulation and optimisation of the packing process
- a set of high-level modelling libraries for the constraint programming system Choco
- extensions to rule programming tools such as constraint handling rules (CHR) and Drools.

Third, on the commercial side, Net-WMS aims at improving European competitiveness in the area of warehouse management by significantly reducing costs related to packing, manpower and transportation.

Net-WMS is a Specific Targeted Research Project co-funded by the European Commission’s ICT for Enterprise Networking D5 Unit. IST in FP6 focuses on future-generation technology in which computers and networks will be integrated into the everyday environment, allowing easy access to a multitude of applications and services through user-friendly human interfaces. Net-WMS places this vision at the heart of its activities and as such contributes to the Ambient Intelligence (AITPL) European cluster.

Net-WMS commenced on 1 September, 2006 and will be active for three years. The consortium has a combined expertise and field knowledge that guarantee the project will reach its objectives. It is composed of ten members representing both academia and industry including the ERCIM members INRIA and SICS.

Link:
http://net-wms.ercim.org/

Please contact:
François Fages
INRIA, France (scientific coordinator)
Tel: +33 1 39 63 57 09
E-mail: francois.fages@inria.fr

Abder Aggoun
KLS OPTIM, France
(technical coordinator)
Tel: +33 1 60 14 66 85
E-mail: abder.aggoun@klsoptim.com

Philippe Rohou
ERCIM office
(administrative contact)
Tel: +33 4 97 15 53 06
E-mail: philippe.rohou@ercim.org

---

The IBM Secure Trade Lane Solution
by François Doliivo

The IBM Secure Trade Lane (STL) is a new comprehensive global logistics information platform. It gives global supply-chain stakeholders access to information on demand, allowing real-time access and response to physical cargo monitoring data as well as the related logistics transaction data. For the first time, shipments can be monitored from the manufacturer to the store and related activities such as port operations optimized.

The international shipping industry plays a key part in the global economy. It is responsible for the carriage of 90% of world trade, with 50,000 merchant ships annually transporting over six billion tons of goods in some twenty million maritime containers. Without shipping, intercontinental trade, the transport of raw materials, manufactured goods and food would simply not be possible.

In this age of ‘just-in-time’ manufacturing and supply, containers are virtual warehouses that move goods from origin to destination via an intricate set of processes. These often involve more than ten different service providers, government representatives or intermediaries. Market and customer pressures demand that these complex operations be optimized, and this has implications for both public and private parties in the trade lane. Governments are therefore under pressure to improve clearance speeds and reduce costs. In addition, security must be drastically improved in this time of increased terrorist threats and security breaches: currently only 2-4% of transported containers are physically inspected. These needs are driving changes in public policy that will affect the entire industry, with new challenges...
arising in terms of security, reliability, liability, visibility, and efficiency of container shipment.

The IBM Secure Trade Lane (STL) is a new comprehensive global logistics information platform that addresses all these challenges by providing unprecedented levels of supply chain efficiency and security. It gives global supply-chain stakeholders access to information on demand, allowing real-time access and response to physical cargo monitoring data, and related logistics transaction data such as order information, invoices, financial data, bills of lading and manifests.

An overall view of the STL architecture is shown in Figure 1. At its heart is the TREC (Tamper-Resistant Embedded Controller), an intelligent wireless monitoring device (see Figure 2) that is mounted on the container. Information provided by TREC is made available to supply chain participants through the Shipment Information System (SIS; see Figure 3). The SIS is a distributed network based on service-oriented architecture (SOA), which enables end-to-end data collection and reporting. It coordinates the sharing of information across authorized parties using proven techniques and tools.

The TREC platform has two primary functions. The first is to create an audit trail of container movements and events from the point of origin to the destination. The second is to make this information available to authorized entities, allowing them to perform risk analyses, to assess the container’s security and integrity and to optimize the efficiency of container shipments. The TREC device automatically collects information on container events, including its physical location (based on GPS) and state (e.g., temperature, humidity, ambient light, acceleration and door status). It can communicate with the backend server via a satellite network, a cellular system (GSM/GPRS), or a Wireless Personal Area Network (WPAN) based on ZigBee/IEEE 802.15.4 radio. A handheld can also be used to communicate with the TREC over a WPAN. The TREC incorporates significant processing power, enabling it to analyze events and take appropriate actions. For example, opening of the door within a predefined geographic zone by an authorized person is an event that is logged; but opening of the door outside of the predefined zone or by an unauthorized person will trigger the sending of an alert to the backend server monitoring the status of the containers.

As shown in Figure 3, the TREC devices are wirelessly connected to a Logistics Service Provider (LSP) through a secure, fully integrated network that links to the SIS. This system enables manufacturers, customers and any authorized member in the logistics network to check cargo integrity and location. Participants manage their own data through decentralized databases, ensuring full customer control over data access and privacy.

The IBM Secure Trade Lane solution will be composed of four service packages:

- Monitoring services enable complete real-time monitoring of any container, anywhere in the world. Collected data can be used to offer services to other trading partners who seek to better manage on-time deliveries, quickly identify bottlenecks, take advantage of green-lane customs treatment and realize additional supply chain efficiencies.

- Information-sharing services allow trading parties within and across industries to exchange data more easily, helping them in meeting their security and efficiency objectives.
• Efficiency services help exporters and importers to optimize their supply chains.
• Security services help any trading party to balance efficiency and security challenges in the context of their specific industry.

The STL concept and the first TREC prototypes were developed at the IBM Zurich Research Laboratory with the support of IBM Business Consulting Services. In September 2005, IBM and Maersk Logistics, of the A.P. Moller-Maersk Group, announced a partnership for pursuing the development of STL. Several hundred

TREC prototypes have now been built by the IBM Engineering and Technology Services in Mainz. The SIS prototype is in development at the IBM European Business Solution Centre (EBSC), La Gaude, France, and the IBM Global Business Solution Center, Bangalore, India. IBM is participating in a large-scale international research project sponsored by the European Union, known as Information Technology for Analysis and Intelligent Design for e-Government (ITAIDE). The intent of the project is to define and, using STL, pilot ways to make international trade safer while reducing the administrative burden.

Clipped RFID Tags Protect Consumer Privacy

by Günter Karjoth and Paul Moskowitz

Existing methods designed to protect consumer privacy in RFID either put the burden on the consumer or suffer from the very limited capabilities of today’s RFID tags. By using ‘clipped’ tags, consumers are able to physically separate a part of the antenna from the tag in an intuitive way. Such a separation provides visual confirmation that the tag has been turned into a proximity tag. Deliberate action on the part of the owner is then required to permit the RFID tag to be read. This mechanism enables controlled reuse after purchase, making the clipped tag a viable addition to the privacy mechanisms proposed for the use of RFID by consumers.

Radio Frequency Identification (RFID) tags typically are small devices that can be embedded in or attached to objects for the purpose of identifying the object over a radio channel. Objects tagged with RFID technology can be read more easily and more frequently, thus improving the quality of information on objects in a supply chain or in the inventory of a warehouse. RFID tags can be read if they are within range (typically up to a few metres) of a reader, which communicates with tags over a radio channel without requiring a line of sight. However, these characteristics of RFID tags have raised privacy concerns.

Retailers are constrained in the technology they use to protect consumer privacy. Stringent cost requirements limit the computational power of RFID tags, which in turn limits the mechanisms that could give users control over the use of their data in back-end systems. Existing solutions either put the burden on the consumer, which may include the risk of illegal behaviour, or are hampered by the very limited capabilities of inexpensive tags. Until now the ‘kill’ command seems to be the solution with the greatest potential. However, it is still necessary to overcome its three major weaknesses: complex key management, no (controlled) reuse after purchase, and no (visual) confirmation of successful disablement. In response to these limitations, we propose an RFID tag structure that permits consumers to disable a tag by mechanically altering it. We call such structures ‘clipped tags’ since a portion of the antenna is separated from the tag.

The mechanical alteration inhibits the ability of a base station or reader to interrogate the RFID tag or transponder by wireless means, and provides visual confirmation that the tag has been deactivated. Once a tag has been disabled (or ‘clipped’), the distance over which it can be read is drastically reduced. Later use would require deliberate actions on the part of the owner of the RFID tag to permit the tag to be read, and thus could not be undertaken without the owner’s knowledge unless the item were either stolen or left unattended. This makes it an appropriate mechanism to implement consumer consent.

Clipped tags are a simple and practical privacy-enhancing technique for RFID retail. Disabling can be performed in an easy, reliable and verifiable way. Even if the RFID tag is ‘printed’ onto a prod-

Figure 1: Schematic scheme.