InPoSec : Integrated Postal Supply Chain Security

C. Geneste [1], P.Richon[2], O.Tsalpatouros[2], R Guyonneau[3], .H Doduy[3], J.P.Guillet[4], I. Manek-Hönninger[4], L.Canioni[4], P.Mounaix[4*], B. Hellingrath[5], C. Böhle[5]

[1] Groupe La Poste 44 Bld Vaugirard, 75757 Paris Cedex

[2]GeoPost International ,9 Rue Maurice Mallet 92320 Issy-les -Moulineaux

[3]Spikenet Technology 26 Rue Hermes 31520 Ramonville St Agne

[4]LOMA UMR 5798, Université Bordeaux1, 351 cours de la libération 33405 Talence

[5]University of Münster, Leonardo-Campus 3, 48149 Münster, Allemangne

*Porteur p.mounaix@loma.u-bordeaux1.fr

Résumé – **Abstract –** L'augmentation des envois par voie postales et via les douanes constitue l'élément clé qui a initié ce consortium à réfléchir sur des solutions pertinentes et efficaces pour assurer les chaines postales. Les événements de Madrid en 2004, à Londres en 2005 et maintenant en Grèce et au Yémen ont plus que démontré que l'Europe est un territoire accessible face aux attaques terroristes. Même si des mesures ont déjà été prises pour pallier aux dangers, la protection de la chaine postale intégrale reste une menace pour les civils en France et en Europe en général. Le but de ce projet est de développer et d'évaluer un système sécurisant la chaine postale et se nomme InPoSec (Integrated Postal supply chain Security). Les opérateurs postaux transportent environ 1,2 milliard objets par jour dans le monde entier, et chaque objet transporté pourrait contenir une menace telle que bombe, arme chimique ou produits illicites. D'un autre coté, cette chaine postale est vitale pour le développement économique de l'Union Européenne et demande à être sécurisée. Les menaces terroristes augmentent et se sont déjà manifestés récemment comme des explosifs cachés dans des colis démontrant que la chaine postale constitue réellement une cible. L'objectif du projet InPoSec proposé par ce consortium franco-allemand est de renforcer la sécurité de protections des humains ainsi que de l'infrastructure pour assurer une sureté économique en Europe par l'ajout de contrôle par rayons T.

1. Context

The enhancement of daily postal and customs processes was the key driver that guided this consortium to think about securing the postal supply chains. The events of Madrid (2004), London (2005) and now Greece and Yemen have shown that Europe is no longer an uncharted territory for terrorist attacks. A lot of steps have already been taken to counter this growing threat but none have so far been capable of securing the entire postal supply chain. The goal of this project is to develop and evaluate a system to secure the postal supply chain, the project is known as ***InPoSec:*** Integrated Postal Supply Chain Security**. Postal operators transport world-wide approximately 1.2 billion items a day; any one of these items could contain a threat, a bomb, a chemical weapon or worse.** This supply chain is vital for the economic well being of the EU and it needs to be secured. The threat of terrorism is growing and evidenced by recent events concerning the interdiction of an improvised explosive device (IED) secreted in a package, the postal supply chain now being targeted.

– To date a lot of research and development has been focused on securing other types of commerce in particular aviation and marine cargo. These are high value, regulated environments. The goal of InPoSeC is to transition technology designed for aviation screening to more ubiquitous, unregulated environments such as the postal supply chain. **The vulnerability of European postal infrastructure was demonstrated in November 2010 when terrorists tried to bomb aircraft and to attack French president Sarkozy and German chancellor Merkel by hiding explosives in mail packages**. These incidents highlighted the need for risk profiling and security-inspections at the first point of entry into an EU member state are necessary to keep alert to counter possible threats. A description of goods on paper label is NO longer sufficient to target these packages that need further inspection so a combination of risk profiling based on provided electronic data and physical security as targeted in this project, is essential. The objectives of the InPoSec project are to develop, implement, and validate a process-oriented system concept to secure the postal supply chain by using recent development

in Terahertz science. The project includes both a physical security component (Evaluation of a Terahertz detection system of threats, illicit or dangerous shipments) together with a risk-related evaluation of electronically exchanged customs declarations. The goal of InPoSec is to strengthen security to ensure the safety of both personnel and infrastructure thereby protecting European economic security.

2. Project and goals

The InPoSec proposal innovations are:

✓Experiment with MMW and sub mm wave technology: comparison with chemical sensing and X-Ray vision (German project)

✓Image vision processor

✓Data mining procedure

2.1 Terahertz tools

✓A safe, non-contact, high resolution, and potentially on-site NDT tool, easy to integrate in postal chain facilities, allowing the detection of different materials (surface, subsurface and/or in-depth) in a variety of material classes that might be in parcels or letters.

✓Global assessment of THz-NDT capabilities in terms of measurement configuration versus detection and composition of materials in the postal inspection domain, for example drugs or explosives, but even in small quantities, the measurements are not possible on the University campus due to legislation rules.

The NDT-THz tool in this proposal overcomes and completes limitations of the aforementioned technologies by eliminating:

- the safety concerns of X-rays and their need to access two sides of a part
- the requirement of a coupling medium and the moderate resolution of UT
- the non-penetration capacity of IRT
- the moderate resolution of MMW imaging.

Furthermore the InPoSec THz NDT tool will have significant advantages in that it:

- identifies multiple types of objects (surface, subsurface and in-depth objects)
- may be employed at any phase of the inspection process
- does not adversely affect the materials / postal goods
- yields depth and spatial extent location information regarding objects present.

On top of the high resolution and penetration capacity the InPoSec inspection tools allows for an on-site, on-equipment testing as required which might be difficult with other imaging techniques.

Because of the very large variety of dangerous goods in parcels, nearly any branch (civilian and military) can benefit – both in terms of cost savings and security. Among a few potential applications is the non-destructive inspection of drugs hidden in parcels or letters.

This project will use a pulsed THz system also referred to as a time domain (TDS) system, as well as a frequency modulated continuous wave system (FMCW).

Then, we propose to evaluate.

✓Dielectric response of packaging materials from several providers to check the ability and the possibility to realize THz or mm wave imaging. These measurements will be made in reflection and in transmission mode.

✓Dielectric response of specific materials: That could be illicit materials such as different drugs, false explosive etc., these issues will be done in strong collaboration with customs, police department, fight against fraud, counterfeit and pirated items sent through the post.

✓These experiments will be done on the fiber TDS industrial system. The results obtained will light the possibilities and the limitations in terms of material thickness and the trade-off between high speed acquisition, spatial and frequency resolutions.

From those campaigns we will also provide quantitative results of the materials dielectric response between 100GHz to 3THz. This is the first step to the building of a specific database devoted to the security field.

From the typical absorption lines found (they exist mainly for drugs and explosives), we will develop a fast CW imager around these wavelengths with a more powerful source design like the quantum Cascade Laser

MMW imaging

With the state-of-the-art apparatus, we will improve the signal-to-noise ratio, the data analysis in collaboration with the provider to move to a bi-spectral imager. This system will demonstrate in laboratory the ability to see throw one type of parcel. The next step will be the systematically testing of different types of materials, parcels and illegal objects to demonstrate or underline the limit of the actual system, and to propose improvement.

Figure 1: First example of passive imaging techniques.

For this project, we will use an active imaging system working at 100GHz and 300GHz in reflection and transmission mode if samples allow. The second possibility will be devoted to a system that produces good resolution images while being mobile and passive a new 90GHz passive imaging system from 1 to 10 meters. Figure 1 shows first demonstration of passive imaging capabilities to detect metal weapons inside a parcel without the need to open it

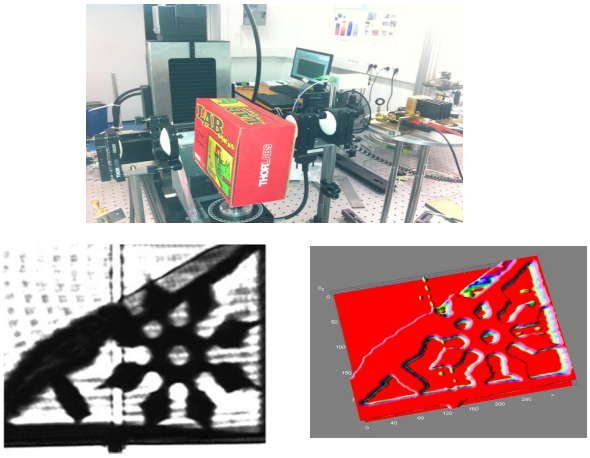


Figure 2 : Visualization of a ceramic knife, a bullet and a skuriken within a parcel imaged with a 300GHz imaging system.

At least, the spectral images and analyses will fill up the database for the datamining approach and also THz-images as an input for a massive collection of models covering the entire set of threats available. Object recognition in this context would be a breakthrough of some importance in the field.

.

2.2 Image vision

For image vision analysis, tthreat detection is a very complex problem which resolution is far from being extensively achieved. Not only are the potentially dangerous objects contained in, say, luggage or mail packages, of a wide variety of shapes, dimensions and sizes, ranging from drug pills to bombs via liquids of unknown origins or weapons, both blades and guns, but they also present themselves at all possible angles in often crowded conditions; and from a strict image analysis angle, picture acquisition is predominantly done at low contrast, since security agents cannot afford to open every potentially threatening containers. As a consequence, part of the solution requires X-Ray imaging as a direct answer to occultation and low-contrast issues. Once acquired, X-Ray pictures can possibly be analyzed through the use of convoluted and multi-headed solutions such as contextual and multispectral image analysis or 3D (re)modeling of the 2D detected objects. Doing so though, one can expect automated systems to produce alarms that eventually have to be confirmed by an expert human agent. To our knowledge, Terahertz vision is not so mature technology but emerging as a future complementary tool. In that sense, multispectral analysis and or 3D modeling will be an innovation that will boost the democratic use of THz radiation in the security field.

All these capabilities of THz imaging make this technique an ideal candidate for an on-site tool in postal security inspection.

2.3 Survey of data mining methods.

The rapid emergence of electronic data management methods has led to something that is often referred to as the "Information Age" in recent times. Powerful database systems for collecting and managing are in use in virtually all large and mid-range companies. There is hardly a transaction that does not generate a computer record somewhere. Today’s databases contain so much data that it becomes almost impossible to manually analyze them for valuable decision-making information.

This need for automated extraction of useful knowledge from huge amounts of data is widely recognized now and leads to a rapidly developing market of automated analysis and discovery tools. Knowledge discovery and data mining are techniques to find strategic information hidden in very large databases.

Data mining, which is also known as knowledge discovery in databases (KDD), is the area of attention in recent years. It is a set of techniques that exhaustively automated to uncover potentially interesting patterns from a large amount of data in any kind of data repositories.

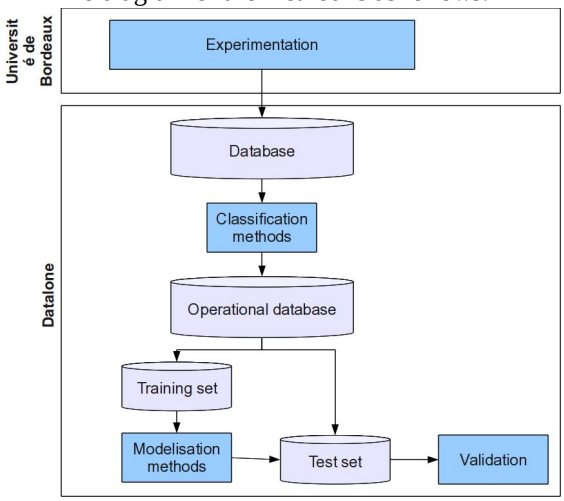
Usually, the data mining project involves a combination of different types of problems, which together solve the scientific or business problem.

Initially, it is important to use classification methods to determine the variables most discriminating of a suspicious package from another package. In this step, the data provided by the University of Bordeaux will be analyzed requiring cross-collaboration between the team and Datalone Bordeaux.

- In a second step, after selecting the most discriminate variables, several prediction models will be tested. According to the performance and practicality of each

model, several tests will be conducted on representative samples of each category of fraud. An indicator performance will be proposed.

The diagram of the method is as follows:



3. German project and collaborative links

This Franco –German project relies on a need to increase the security level of postal supply chains. The InPoSec project will be designed to work out solutions. The project's link to the government-subsidy goals of the German-French program "Research for Civilian Security" is created in the following areas.

On the one hand, the threats to citizens, economies and the infrastructure that the project is designed to reduce the threat that terrorists could mail parcels containing explosives or biological or chemical agents. On the other hand, the criminal misuse of the postal network by circumventing bans and restrictions, including the import of drugs, the smuggling of counterfeit products and medications, the violation of food laws or the shipment of radioactive materials, should be reduced.

At today's security level, the provision of basic postal services is not completely assured in crisis situations. As a result, the desired improvement of security in postal supply chains promotes the protection of critical infrastructure and assures essential product flows during crises, e.g., during an increased terrorist threat.

The project will generate a process-oriented overall concept that will increase the security of postal supply chains. Such a protected infrastructure forms the foundation for economic and social stability.

The German part of the project will largely be concerned with analyzing and closing existing or future security gaps in transnational postal traffic. The focus will be on novel concepts which have not previously been used, e.g. the electronic advance information for goods and the data exchange between Posts and Customs.

The current postal system is analyzed towards threat scenarios, which outline the focus of the following security measures. Such scenarios define the vulnerabilities in the supply chain along with the type of misuse and the objective.

Current process modeling languages will be extended to consider these threats in postal processes. According evaluation procedures will be developed..

Findings from the analysis will be used to develop a security management concept for the postal sector. The resulting framework will be used to define procedures for a continuous risk and improvement identification.

For the risk assessment, an integrated IT-system will be devised, which consolidates the electronic data sets of the parcel and the results gathered from the physical inspections. The resulting risk rating identifies malicious mailings and controls the subsequent operations.

The project is carried out with strict adherence to French, German, and European laws. As a key asset, "privacy by design" principles are applied to guarantee that national and personal rights remain unharmed throughout the project.

In combination with the French project, the German project will give a comprehensive overview of all aspects along the supply chain, to create a seamlessly integrated solution which sets the standard for postal services.

The framework depicts all aspects of the InPoSec project assigned to the national groups.

The project is funded by Bundesministerium für Bildung und Forschung (BMBF) within the framework of the program „Research for Civilian Security" of the German government and the Agence Nationale de la Recherche (ANR) within the framework of the program "Concepts, Systèmes et Outils pour la Sécurité Globale".