European Commission

JRC SCIENTIFIC AND POLICY REPORTS

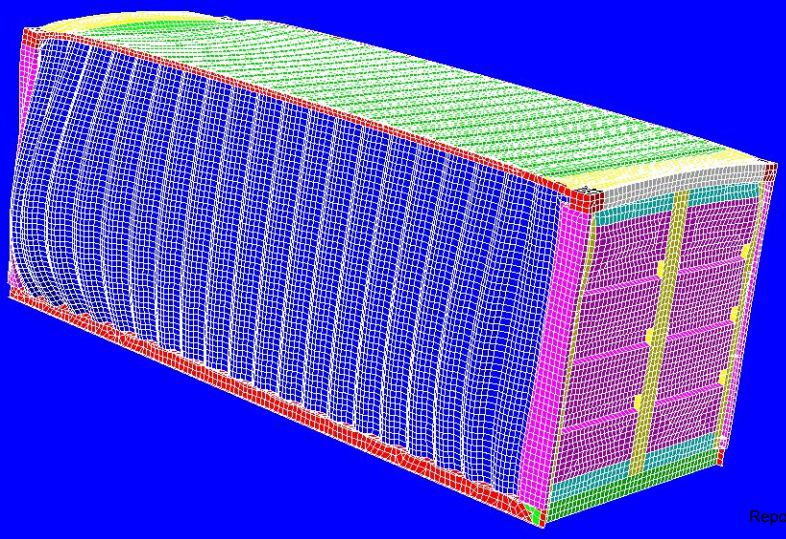
An overview of research programmes and prospective technology in the development of more secure supply chains: The Case of Shipping Containers

E. Gutiérrez (DG-JRC)

W. van Heeswijk (DG-TAXUD)

D. Arrowsmith (Queen Mary, University of London)

2012



Report EUR 25298 EN

Joint Research Centre

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Eugenio Gutiérrez
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 480, 21027 Ispra (VA), Italy
E-mail: eugenio.gutierrez@jrc.ec.europa.eu
Tel.: +39 0332 78 5711
Fax: +39 0332 78 9049

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC70120

EUR 25298 EN

ISBN 978-92-79-24168-0 (pdf)
ISBN 978-92-79-24167-3 (print)

ISSN 1018-5593 (print)
ISSN 1831-9424 (online)

doi:10.2788/23670

Luxembourg: Publications Office of the European Union, 2012

Printed in Italy

COVER FIGURE: FINITE ELEMENT ANALYSIS SHOWING STRAIN DISTRIBUTION OF FIBRE-REINFORCED CCOMPOSITE CONTAINER SUBJECTED TO ISO 1496-TYPE LOADING (T. DYNGELAND ELSA-JRC.EC).

From here on this page is purposely left blank

Contents

1. PREAMBLE

The use of shipping containers over the last five decades has radically changed world shipping and, in tandem with the many technological developments over the same period, has made it possible to transform the balance of world trade in a manner that has not foreseen when the first container shipments —as we know them today— took off in the 1950s.

In its 2009 Review of Maritime Transport, the United Nations Conference on Trade and Development (UNCDT) reported that the world throughput in containers for 2008 was 507 million TEU movements, corresponding to approximately 150 million container shipments (according to Hofstra University the ratio of container traffic over container throughput was around 3.5[1]). Even in spite of the economic crisis, in 2010 UNCDT reported a figure of 465 million container throughput for 2009. The latest figures from the World Shipping council report that the crisis has continued to hit the container traffic sector. They report that in 2010 container traffic stood at approximately 110 million shipments, which would correspond to a throughput of the order of 380-400 million individual container movements: hundreds of millions of opportunities to either defraud customs, introduce illicit cargo, smuggle people, or breach security protocols.

Containers are now considered as a weak link in the supply chain with the potential to be exploited as a major security threat. Within this context, a number of national and international programmes and agreements have been drafted to limit the potential of intermodal containers for the transport of weapons —or illegal substances— that can be used to attack populations or public assets. Beyond this, the mere threat of such attacks and the consequent security backlash, has already perturbed the equilibrium of the container supply chain: shippers, port authorities and other stakeholders –although not purposely obstructive— are wary of how the evolving security agenda will affect their business.

One of the proposed paradigms for secure trade lanes consists in ensuring that a certified stuffed container be transported, from source to receiver, in such a manner that it can be ascertained that at no point during its transport was the container tampered with intent to generate a security threat at its destination.

---

1 http://people.hofstra.edu/geotrans/eng/ch3en/conc3en/worldcontainertraffic.html

The vast number of container throughput makes it impossible to check the contents of every single container without massive disruption to trade. So how is this control to be carried out without disrupting trade?

The ideal scenario for container shipping is one that continues to provide a fast, smooth-running, world supply chain whilst maximising security. Thus, the scope of any analysis of container security performance standards must, not only, consider the technologies available to promote security, but also how these could impact on the smooth flow of goods. To do this we also have to look at the economic technological and logistic constraints that define the container industry.

Although there are a number of types of containers their sizes are standardized according to ISO specifications dating back to 1961; consequently, containers can be handled and transported by a one-size-fits-all supply chain infrastructure that spans the globe.

Shipping containers are a good example of a Network Effect that has led to Lock-In, whereby a chain of events has made containerization so valuable to users that, to all intents and purposes, there is only one vendor product (the ISO shipping container) available to exporters and importers to transport packaged items across the globe. Changing the format of this locked-in 'product' would appear to be very challenging –including proposals of designing new tamper-proof container made from hybrid composite materials. However, we should remember that just as the container completely changed the manner in which goods are transported, it is not impossible to foresee that the introduction of new technology could, in turn, signal the demise of the humble steel box in favour of an advanced transport system. In this respect, the role of the two technological areas of materials science and miniaturised sensors will be fundamental.

The combination of the structural manufacturing and design flexibility of advanced composites, allied to the wide variety of miniaturized sensor technologies opens up the possibility of developing structural components capable of providing more than one functionality in a manner that had, hitherto, not been possible. For example, it is possible of including anti-tamper diagnostics into the structure of the container by exploiting non-structural physical properties of materials; for example, carbon fibre is an excellent conductor and therefore an ideal material for an antenna, which, if broken or damaged by malicious intrusion, will change its transmitting reception properties. In contrast, glass fibre is transparent to radar so that a panel made from hybrid (glass/carbon fibres) could provide a triple function both as a radar-transparent structural component fitted with an antenna. In addition to the material itself, the use of embedded micro sensors fitted with energy-harvesting, or remote energizing capacity, will open up the possibility of introducing hidden networked sensors with extended energy-source autonomy. These are the technical possibilities,

but, one should not forget that containers are, above all, cheap practical vectors for commerce.

The development of new, more secure, container systems should consider the main techno-economic items and devise a solution that, not only provides increased tamper-resistance, but also contains economically beneficial buy-in features that will motivate the adoption of new container models by the shipping trade.

2. SCOPE AND AIMS

The scope of this essay covers, on the one hand the two primary technological considerations (materials technology and production, ad-hoc sensor networks deployment) and, on the other, the economic and trade statistics backdrop of the container industry.

By considering these aspects–in conjunction with the technological developments and policies in container security of the EU's major trading partners– it is intended to set the backdrop to the potential innovative technologies in the area of tamper-proof intermodal containers. The aim is to provide support to European Commission services in their policies of motivating the development, capability testing and evaluation of technologies that could meet the security performance standards in the container shipping industry, and in matters relating to meeting the EU's international cooperation agreements on supply chain security.

The technological scope of the this activity, as carried out at the DG-JRC in collaboration with relevant EC services (but here primarily DG-TAXUD) concerns the development of a multifunctional intermodal shipping container manufactured from hybrid materials –including composites. By multifunctional we mean structures that have the capacity to act both as a structural component and as housing for sensor devices.

Benefitting from the ever-reducing cost of mobile communication systems, it is expected that ad-hoc sensor-equipped containers will, one day, not only advise on the security status of each of the 100's of millions of container movements, but will also provide logistic and economic benefits that will ensure their up-take into the conservative world of container shipping.

Although the general scope is geared towards developing performance levels and standards, in practice, these must be anchored in pre-normative research based on tangible applications of prototypical innovative technological solutions that, not only performs its primary role as a sturdy and commercially viable housing for the transport of goods, but one that also allows the relevant authorities to ascertain the security status of the container and its contents.

From the point of view of fostering technology and standards, the JRC is on familiar ground having participated in the past as a node between the EC services, standardization organizations and industrial stakeholders; thus within the context of the JRC's STEC Action (41999) one of the first steps is to analyse the main drivers for technology development with close cooperation with the relevant Commission services. In the first instance, consultations between DG-JRC and DG TAXUD (who motivate the discussion in the following chapters) have served to establish the a basis for prospective collaboration with equivalent programmes with the EU's main trading partners.

3. POLICY STAKEHOLDERS AND TERMS OF REFERENCE

The main driver for the research we propose (other than the economic benefits that may accrue to European industry from the development of cutting edge container industry) are the security measures taken by the Member States (MS) of the European Union with regards to the security threats that could be hidden in any of the millions of containers moving in and out of Europe. Irrespective of the decisions taken by each EU Member State, there is a key role for the EU in various bilateral agreements taken by the EU and its major trading partners. The most significant of these are those between the EU and the *USA* (OJEU L304/34-35 ratified by Council in 2004/634/EC) on intensifying and broadening agreement on customs cooperation (with particularly emphasis on sea-container transport), which is further reinforced by that between the EU and the People's Republic of China (OJEU L375/20-26 ratified by Council in 2004/890/EC).

Whereas these agreements appear to run in parallel, at a first reading, that with the PRC is primarily geared towards intelligence gathering, information exchange and customs protocols. That with the USA, however, appears to have an added technological basis linked to its own *Container Security Initiative* (CSI) programme ; indeed in Article 3 of the EU-USA agreement it is stated that one of the objectives be that of ''supporting the prompt and successful expansion of the CSI''. Now, whereas CSI includes a strong element of intelligence and automated information handling, it also highlights the need of using detection technology to quickly pre-screen containers that pose a security risk, and the development of, so-called, smarter, tamper-evident containers.

More recently, in the summer of 2011, a further agreement between EC services and the DHS proposed, amongst other aspects, reinforcing the role played by technology in ensuring the security and efficiency of the supply chain. Importantly, the document highlighted two main aspects i) the need to ensure that said technologies should be as compatible as possible by way of guidelines and standards ii) encourage continued collaboration in innovation by:

• *"Extend and intensify the bilateral dialogue and cooperation on technology (including R&D, sharing best practices, opportunities for common certification practices, and contribution to setting of international standards"*

• *"Continue to test technologies collaboratively such as currently available radiological/nuclear detection technologies, toward the goal of identifying those that meet internationally recognized standards and explore novel approaches, e.g. in relation to monitoring container itineraries"*

4. RISK MANAGEMENT AND SECURITY FROM THE PERSPECTIVE OF DG TAXUD

The Directorate General Taxation and Customs Union's mission is to develop and manage the Customs Union and to develop and implement tax policy across the EU for the benefit of citizens, businesses and the Member States. Particular attention is given to the Internal Market, by making sure it functions smoothly and efficiently.

The overall aim of EU Customs Policy is to facilitate legitimate trade whilst maintaining a level of controls guaranteeing the safety and security of citizens and protecting the public health, the environment, financial and economic interests of the Community and its Member States. The EU aims to cooperate with its trading partners to ensure the end-to-end security and facilitation of the international supply chain.

The Commission adopted common risk criteria and standards for security and safety risk analysis which are applied from 1 January 2011.

The Decision contains a set of common risk criteria to be applied in the Member States' automated risk analysis systems in order to continuously screen advance electronic cargo information (entry summary declarations) for security and safety purposes.

The Decision[2] represents the foundation for common risk management in the area of security and safety. Its provisions require regular and constant monitoring and evaluation of the criteria principally facilitated by the requirement for the Member States to provide to the Commission on a quarterly basis the results of implementation of the common risk criteria and standards (set of reporting requirements is part of the Commission Decision). The Commission currently closely monitors the implementation of the security and safety risk and will evaluate it on a quarterly basis.

[2] Commission Decision C (2009) 2601 OF 15 April 2009, classified as EU Restraint.

Experts of DG TAXUD (Unit B2) coordinates customs risk management related to international trade with third countries, enhance supply chain security and trade facilitation through management of the EU AEO programme, international mutual recognition thereof and the development and use of **innovative technology** to detect illicit cargo.
Customs control for internal security purposes as well as consumer protection, health and safety purposes has been an integral part of customs control work at Member State level. Since the **2005 'Security Amendment'** of the CCC in particular, the 'security and safety' dimensions of customs control work have also been incorporated into the **customs union policy acquis**, and is fully operational since 1 January 2011. The fact that the customs is constantly present at the border and has a longstanding knowledge of the goods moved within the supply chain, places it as one of the primary authority able to detect and prevent illicit and dangerous goods from entering into and leaving the EU.

In practice, customs activity is that of an enforcement authority, which often means implementing the policy priorities of several policy areas at once. Therefore customs co-operation across the EU takes a range of forms throughout the whole EU external border, whether maritime, air or land border. In addition to respond to multiple types of risks, customs risk-management and control must by nature be holistic. This includes, the use of state of the art data integration and management systems for risk analysis purposes, the application of a variety of equipment and technology tools for the detection of illicit and dangerous goods, sophisticated laboratory testing for security and safety as well as for fiscal purposes. Furthermore, customs carries out control at the most effective place/moment of the supply chain, which also requires use of modern audit approaches (system-based approach) and post-clearance type of controls. Customs thus has to use a variety of co-operation approaches, risk management and control working methods, techniques and equipment.

The EU is convinced that a multi layered risk management approach, in which the use of Non-Intrusive Inspection is based on risk management principles, is the most effective and most efficient tool to enhance the security of the international supply chain without unnecessarily interfering with global trade
Customs' responsibility is no longer limited to protect the financial interests of the public treasury; it is now a service provider with a global mission to protect society and its citizens. More specifically, to ensure that only safe goods enter and leave the territory, that the traded goods comply with legal requirements in general, that they present no danger for the environment and last but not least, that they do not present any security threat.

The use of technology and equipment to enhance effectiveness and efficiency of customs controls is becoming more and more important.

The European Commission is convinced that modern technology is one of the cornerstones to enable Customs to adopt modern risk management working methods. A comprehensive and effective multi-layered approach to risk management will result in increased freight screening, a reduction of physical inspections and a better focus on the risk associated with specific consignments.

In order to attain the above-mentioned objectives, EU Customs aims to develop a wide application of modern technologies in the following areas:

- Techniques for advanced and high speed data analysis;
- Techniques for ensuring cargo and container integrity (e.g. E-seals, Container Security Device (CSD) and smart containers);
- Techniques for supervision and monitoring maritime and air container transport (tracking/tracing);
- Non-intrusive inspection techniques and Radiation and Nuclear detection equipment.

The Joint Research Centre should play an important role to support DG TAXUD's policy towards the use of technology in order to enhance security in the global supply chain and make customs controls more effective and efficient.

DG TAXUD has closely monitored two research projects called “INTEGRITY” and “SMART CM”. These projects tested, amongst other, the use of e-seals and smart box technology under the 7th Framework Programme for Research and Development, funded by the European Commission. Dutch, UK, Belgian and Greek customs participated. More information on the projects "Integrity" and "Smart Container Chain Management" can be found on the websites:

http://www.integrity-supplychain.eu/index.php ,http://www.smart-cm.eu/

The EU-China pilot project on Smart and Secure Trade Lanes (SSTL) has completed its first phase and will continue to test Container Security Devices (CSDs), including e-seals, in the currently ongoing second phase with the participation of seven EU customs administrations (BE, DE, FR, IT, NL,PL,UK) and Chinese customs.

The testing of e-seals during the first phase of the SSTL pilot project has highlighted the need for common customs requirements, procedures and standards to be established globally to ensure interoperability of these security devices and equality of treatment**.**

DG TAXUD believes that these and similar innovative and pilot projects are essential to promote technological innovation to enhance security worldwide.

Furthermore, an EU detection technology project group was created in January 2011, under the Customs 2013 Programme, to support and

facilitate modern customs administrations to tackle the challenges of the rapidly changing 21st century operating environment. This group has an important role to monitor very closely the development of technologies and innovations and evaluate the benefits that customs administrations can extract from its usage.

Supply chain security should not rely on one single technology, but display a combination of different technologies combined with risk management based on reliable and adequate information.

Unilateral security measures alone have a limited impact on security. International supply chains are complex in nature and, as a norm, pass though several countries. It is logical that a risk which is international in nature is addressed not only nationally but multilaterally by combining our resources, sharing the results of innovation and implementing together workable and practical solutions.

In the years to come, the Commission and Member States will continue to focus on enhancing the use of modern, non-intrusive control techniques and technologies in close cooperation with the Joint Research Centre of the European Commission, suppliers and the Customs Administrations as the end users.

5. State of Art in Container Security Research

5.1 Recent Container Security Projects in USA

A recent study concerning technological development and research in the field of container security and logistics in the USA was recently published by MIT[3]. The report summarised the state of the art and technological trends in forty-one projects that were either activate or had just been completed in 2007. The report, interestingly, lists the proposals not just in sequence, but in the form of a matrix structure whereby the rows are grouped by stakeholder :

- Regulatory bodies
- Carriers and logistics providers
- Shippers
- Intelligent container Concept providers
- Consortium Study Groups
- Academia and Research

[3] http://dspace.mit.edu/handle/1721.1/38956

On the columns, the projects are grouped by technical initiative or concept:

- Supply chain management (SCM)
- Security and safety
- Technology and level (container pallet etc.) at which the items are tagged

In all, forty-one projects are mentioned spanning a wide range of stakeholders and technologies.

The motivation for their analysis is based on the fact that shipping containers have come under scrutiny for two primary reasons. From the commercial side they are perceived as a key item where technology can be used to provide a competitive edge. From the public sector they are perceived as a growing security threat. The report states its main aim as that of compiling the multitude of technologies and organizations that were dealing with these issues, either for commercial interest or public safety, with a view to providing an overview of the various solutions and their potential benefits. In essence, the analysis consists of a series of taxonomies concerning technology, implementation issues, end users, and relevant initiatives planned or underway in 2007. It is worth highlighting the MIT report as, it would appear, that no such objective analysis has been performed at an EU level. Later on, herein, the authors will suggest by way of example, that using publically available data, it could be beneficial for EU services to conduct such an analysis, at least for EU-funded projects.

The essence of the MIT report is as follows:

The report highlights that ‘’*despite the hype and elegance*” new container technology uptake will only work if it provides added value to the supply chain and, just as importantly, technology vendors should not be perceived as opportunists that seek to find problems for their technologies –implying, perhaps, riding on the security-scare bandwagon. In this sense, the report accentuates the need to highlight the true benefits; i.e., cost-cutting, as perceived by those stakeholders that are most likely to benefit: shippers and carriers.

The report also highlights that there is a wide spectrum of needs between the different supply chain stakeholders and that it is not conceivable that, given the degree of specialisation of each sector, a one-size-fits-all solution can be drawn up from first principles. Indeed the adoption of new technologies could change the landscape of the supply chain, just as the container, itself, dramatically changed the manner of shipping goods for ever.

As regards the proposed benefits, the main claims concern the fact that, given the increasing complexity of the supply chain, substantial benefits could be accrued by adapting containers to handle (i.e. gather and transmit) information concerning multiple handling moves, documentation

(the authors quote that the average container ship generates 40,000 paper documents per trip), customs manifesting, low cost track-and-trace of valuable goods. From the shippers and logistics companies' point of view there would appear to be substantial opportunities for intelligent cargo systems to substantially change the management of the supply chain itself: from container pier management to optimization of container stock distribution (e.g. location and transport of empty containers etc.).

Nevertheless, performance standards for security devices will not be welcome by industry if their cost cannot be recuperated or spread to third parties. Also, just as importantly, the imposition of enforceable standards must also be considered in the light of international agreements with the USA's major trading partners.

Following the short descriptive analysis above, a more conceptual visualization of the projects given in the MIT study are represented in the form of a social network, shown in the following pages. The scope is not to identify and scrutinize all the individual projects, subject areas and parties involved, but rather to highlight the main themes being studied and how they interact between each other. Above all it is interesting to see if there is a structure of interconnectivity linking the actions and research themes. The resulting network structures will then be compared to data concerning EU-funded projects.

In Figure 1 the interaction of projects and project themes is seen to form a connected graph or network. The network is shown by highlighting the importance of the vertices (a project or a subject matter) by calculating its connectivity measure of the remaining graph (see caption Figure 1).

The Graph in Figure 2 provides a quick overview of how the various R&D projects (blue discs) relate to the areas being studied (yellow discs). The size of the disc indicates how many projects are concerned with a certain topic, or, vice versa, how many topics a given project is looking at. A total of 40 projects are represented addressing 33 topics. The most frequent can be read off simply by picking off the biggest yellow discs: hence in the USA, projects have concentrated on the Container itself with special considerations for the conveyance method, the tracking and the verification of custodial aspects. It would appear that, until 2007, the development of embedded sensors or using new materials for the container had not been considered by many projects.

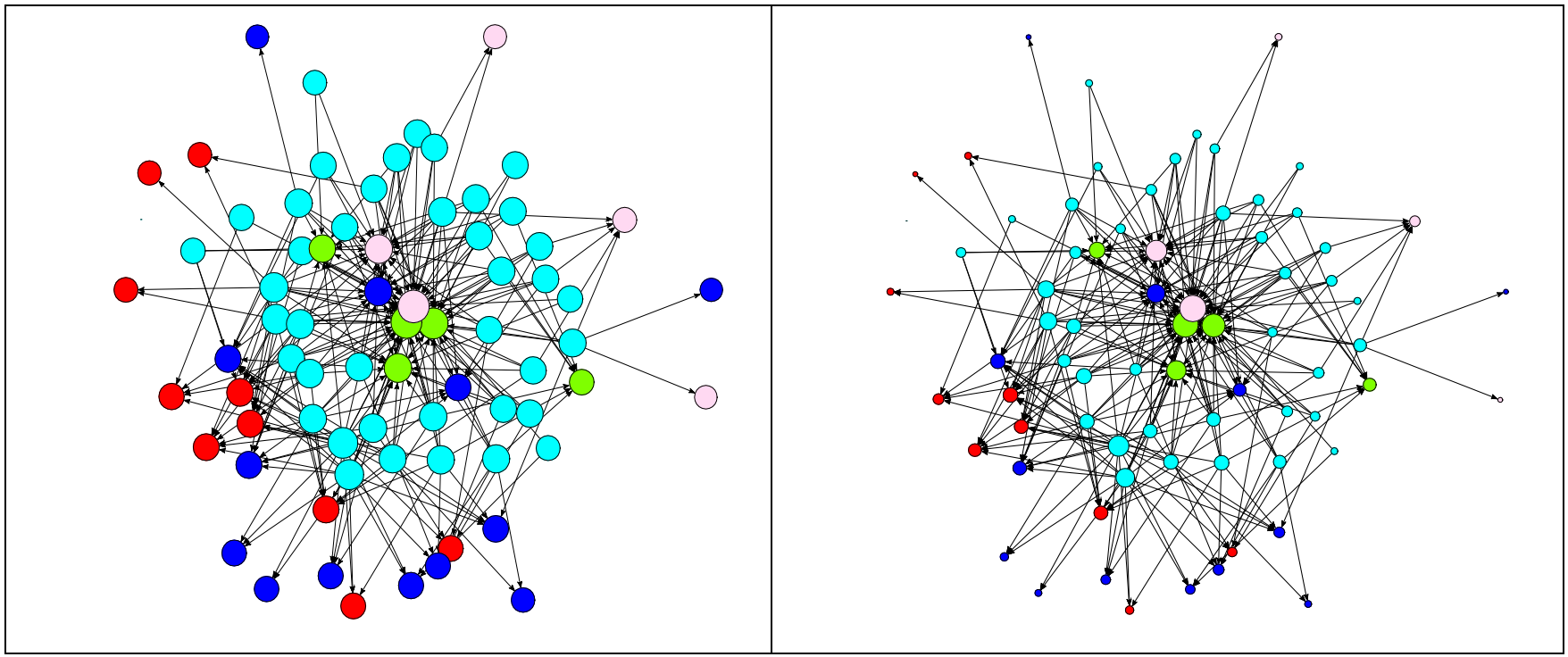


Figure 1. Network view of the project connectivity of the ''intelligent container initiatives'' research and development topics in the USA as reported by P.C Bryn (MIT, 2007). The network view provides a synopsis of the manner in which the projects are interconnected. Left pane: projects are shown as cyan circles the arcs pointing to the four main areas being studied: red circles on security and safety; blue on technology type; green for level of implementation –such as container or pallet; the pink circles concern R&D on communication protocols. Right pane: the same network with node size proportional to number of connections (in and out) assigned to each node. Note how some nodes play a key central role in the network structures (see text).

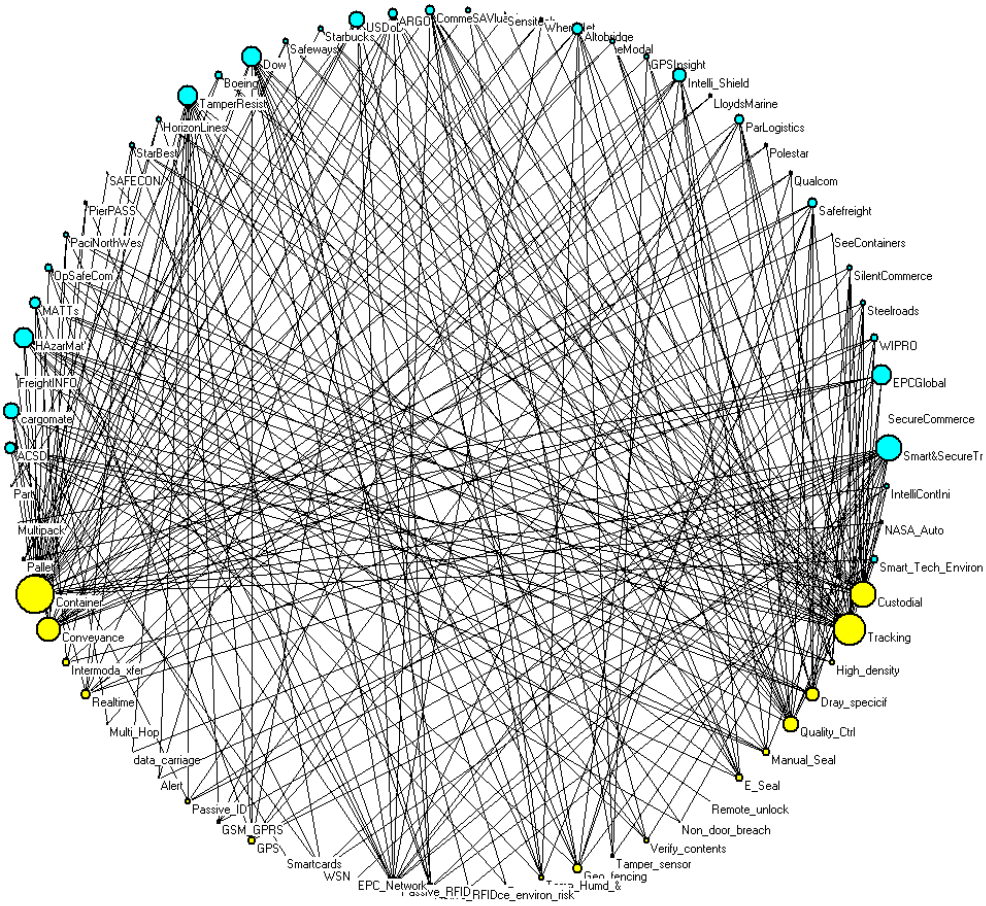


FIGURE 2: a circular network overview of ‘’intelligent container initiatives’’ research and development topics in the USA as reported by from P.C. Bryn (MIT, 2007). The circles are colour-coded as follows: cyan circles correspond to project names; yellow circles correspond to organizations in charge of running them. The size of the circle represents its importance in the overall scheme.

In Figure 3 the network is sorted as two concentric circles: projects (outer circle) and subject matter (inner circle). The figure also bunches the projects in terms their stakeholder or subject matter grouping.

Reading the outer graph clockwise: from 12:00 to 16:00 those projects conducted by –so called–solution providers (of which there are 18); from 16:00 to 18:00 consortium study groups (3 thereof); from 18:00 to 19:00 academic and R& projects (of which 3); from 19:00 to 22:00 are the projects run by regulatory bodies (of which 10) ; from 22:00 to 23:00 carrier's projects (only 2), and finally from 23:00 till 24:00 are found the shippers projects (of which 4). On the inner face on the top left quadrant —in green— projects concerning the location of the level of supply chain management, followed by projects on security and safety (in red), the technology used (in blue) and the level of implementation (i.e., container, pallet) in pink.

The main point to note here is that the most salient topics concern the custodial and tracking aspects of the container itself. Interestingly, the most connected projects, i.e. those that interact most with subject matters are also important to other project teams, specifically Smart and Secure Trade Lanes, Tamper Resist, EPC Global, Dow, ACSD, MATTS and Cargomate and US DoD. What is not clear from the MIT report is how much interaction there is between these project partners, more specifically, the full list of participants, which would allow us to develop the graph of interaction of the participants, is not given.

The overall picture in the USA is that, if one were to distinguish prescriptive (governmental) imposition of security standards from those originating from commercial interest, the intelligent container concept cannot be easily characterised to fit all the needs or commercial interests of the many actors that participate in the container shipping industry. Thus, whereas some companies —especially technology providers—seek to suggest the need for regulation in security performance, others (those that have to bear the brunt of the cost with no clear strategy on how to pass it on) are diffident of implementing new technology unless there is a clear profit margin for them. The disaggregation of the many companies and roles plied by each of them would indicate that trying to impose an all-encompassing performance standard will require considerable collaboration if a successful implementation strategy is to succeed.

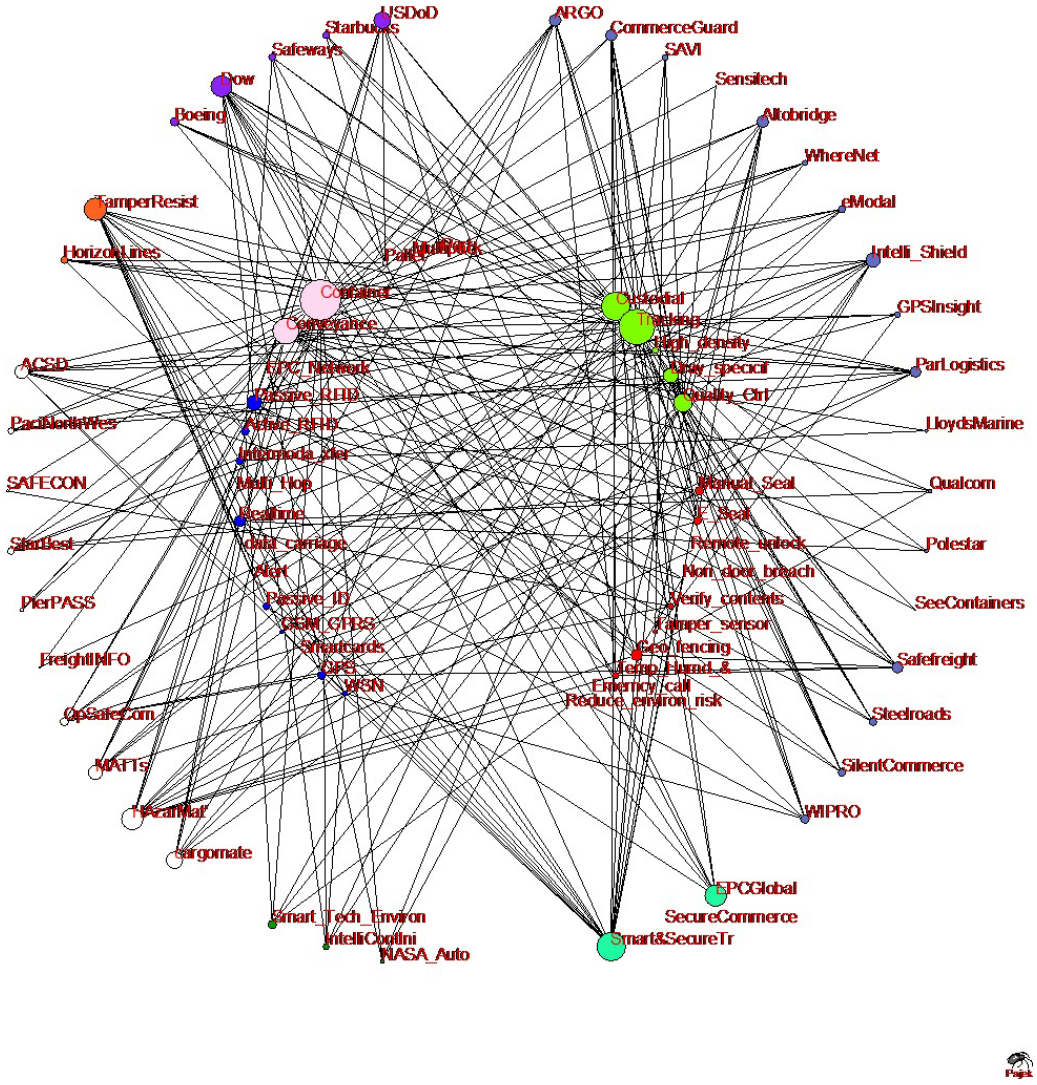


Figure 3 USA's intelligent container initiatives as concentric ring distributions with projects on outer and subject area in inner rings respectively. Size of the vertex corresponds to degree-connectivity.

5.2 Overview of R&D FP7 Projects Network

The focus of our analysis here is to provide an overview of the structure of the R&D projects in container logistics in Europe by analysing the situation with regards to the FP7 programme.

The data were obtained by searching the CORDIS data base under the 'Find a Project' tool, providing key words such as 'container', 'security', 'logistics', etc. A specific list of projects whose scope was consistent with the themes that either included security research or technical aspects (such as ICT) that could be considered as security-use technology was not explicitly available. We found 26 projects that appeared to deal explicitly with container technology; however, only a small minority dealt directly with container security, the majority being more concerned with logistics. We found that a total of 321 companies or institutions participated in these projects; this implies that, on average, each project was composed of 12 companies. Typically large network-type projects deal more with consolidation of procedures and commercial and corporate networking for implementation of in-house or turn-key technical solutions, rather than analysing and developing research programmes.

The structure and interaction of the projects analysed can be seen in FIGURE 4. From the outset we can see that the interconnectivity graph appears to be composed of one large cluster made up from an ensemble of dendritic, or tree-like, structures. We also have three isolated star-like sub-graphs composed of three projects and their corresponding partners. The Nodes are colour-coded according to the group to which they belong (project or organization) and the role they play in the network (isolated or key-player). The size of the vertex indicates the centrality-closeness of the node within the network and for this reason the three isolated clusters appear to have smaller node sizes. In essence we have the 26 projects (shown in cyan) which are connected to two groups of companies: in the first-case we have what could be called 'single-project' companies/organizations that appear to be appended to the core clique of companies (shown in pink) that link up nearly all the projects. One way of looking at this is that it would appear that FP7 R&D programmes dealing with container technology are highly centred on cliques of organizations with minor-stakeholder companies filling in for secondary roles.

If one examines FIGURE 4 one can see that the single-project organizations (green circles) appear to be appended to the projects (blue) within a very hierarchical structure. This form of connectivity provides limited scope for collaboration between participants; it is not conducive to transfer of information or shared procedures such as the development of common standards.

Although the projects, in themselves, may be of high quality, they will not be of much use to the ambitious theme of developing common, transnational inter-sector security performance standards. The research

efforts will, at best, spread slowly and at worst could remain as compartmentalised proprietary technology limited strictly to commercial, rather than societal, exploitation.

6. THE CONTAINER SECURITY INITIATIVE IN USA.

The Science and Technology Directorate (S&T) of the Department of Homeland Security (DHO), via the Space and Naval Warfare Systems Center has, in the period 2004-2009, allocated a number of grants to finance research in the area of supply chain security specifically dedicated to improvements in container security technology. According to the United States Government Accountability Office (GAO report-10-887) *"The DHS has conducted research and development for four container security technology projects, but has not yet developed performance standards for them"* .

In view of the collaboration agreements between EU and USA for cooperation on supply-chain security mentioned above, and particularly the Joint Statement issued by the Secretary of the DHS and three EC Commissioners of June 2011 where attention is brought to ''*exploring and deploying new technologies''*, it is worthwhile to pause and analyse the —apparent—status of the various R&D programmes associated to CSI.

6.1 THE CSI INITIATIVE

The CSI initiative includes a host of programmes concerned with border controls, intelligence-gathering of shipping data, pre-screening and other information that may be used by border controls to identify and target suspect containers. This programme has been active since 2002.

In 2004, the DHS initiated an R&D effort to develop container security technologies; and here the emphasis is in deploying electronic systems and/or using new materials to reduce the possibility of introducing illicit items into the container itself. In August 2009 Commission services were invited and reported —Note for the file TAXUD/C6/WVH D(2009)— on the Cargo Security Technology Demonstration. The meeting was organised by the DHS at the Sandia National Laboratory in Albuquerque. The Commission report makes a point that , on the basis of the information presented to the EC services delegation, the following points can be highlighted:

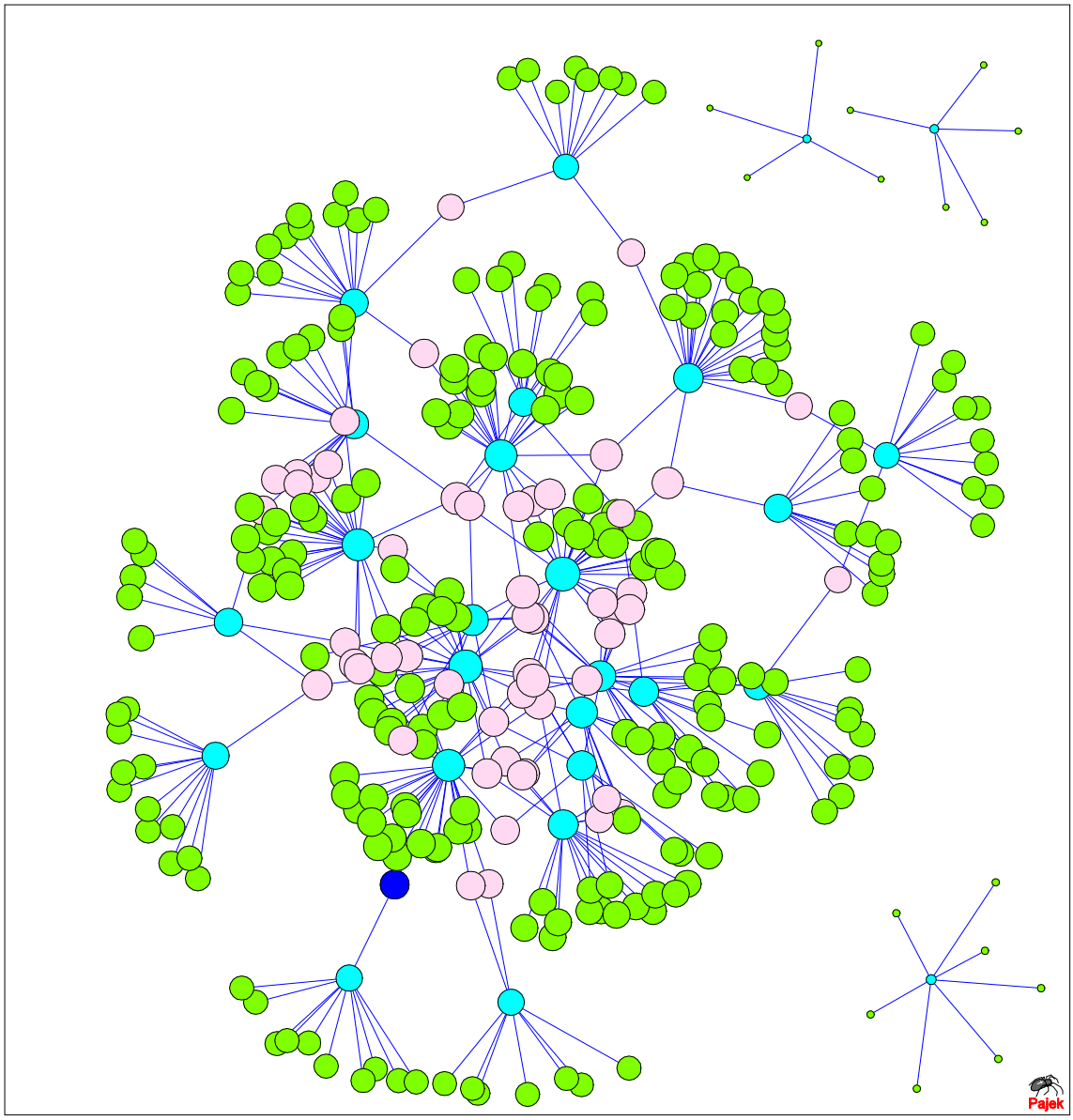


Figure 4 The structure of FP7-funded projects closely related on container research. It can be seen that most participants are single-project, low interaction, members attached to the various projects (coloured cyan). There is a group of participants (shown in light pink) that appear to gel most of the fp7 proposals and interact with each other to form cliques. This structure does not accelerate inter-sectorial knowledge-spreading throughout the programme: more interconnections between green circles could benefit the spread of knowledge and development of common performance standards.

- The US was advanced enough to develop an international standard that, in view of the lack of funding at the EC/MS level, would require the EU to motivate the development of equivalent standards.
- The MS delegates were concerned that no comparable funding for an equivalent project was available at Community level.
- That although the security research call (FP-SEC-2010-1) had been launched, and included a topic on supply chain security, it feared it would *'take several years to have concrete deliverables*'.

In view of this —evolving— state of affairs as perceived by the DG TAXUD note, it is interesting to examine the report drafted by the US Government Accountability Office (GAO) regarding the progress made by the DHS-funded programme on container security technology. The report –dated September 2010—provides an alternative portrayal to that given to the EC delegation in August 2009. The DHS has funded four projects (see appendix A2 for further details) in the period 2004-2009 these are:

- ACSD: to develop a system to monitor and report intrusion on any of the six sides of (presumably standard) containers.
- CSD: to develop a device to detect and report on opening or removal of container doors.
- To develop a Hybrid Composite Container with embedded security sensors.
- MATTS: to establish a system to track containers.

The plan is that each of these systems is put through Phase I (laboratory testing) and then, if successful, Phase II (trade lane or environmental testing). Only if the systems pass both stages do they then move on to be proposed for the end deliverable; that is, Performance Standards to DHS Office of Policy Development for Customs and Border Protection (CBP).

Although the listed items do not constitute performance Standards *per se*, the project requirements give a good indication of what is expected of the technology. It is important to examine these proposals as they represent the first basis for a discussion on technology-sharing and development between Commission services (DG TAXUD and JRC) and their corresponding interlocutors (DHS and Scientific and Technology Directorate). In or order to ascertain if these projects constitute a viable common basis for discussion it is important to consider what the DHS considers to be the level of maturity of such projects and whether indeed the intention is to pursue further, abort or take some other action.

At the time of publishing of the GAO report, the state of progress in September 2010 appeared to be as follows:

- The CSD and MATTS systems had passed Phase I and were moving to Phase II.

- The ACSD (i.e., the 360° counter-intrusion system) and the Hybrid Composite Container appeared to have stalled. In the first case, the ACSD system had failed a number of tests in Phase I. The case for the Hybrid Container appeared to come against some technical and managerial difficulties and had not yet proceeded to Phase II.

It would appear, that since then, progress concerning both the composite container and the sensors has taken place (see, http://www.gtri.gatech.edu/media/726). Field testing on a sensor-equipped composite system have taken place between Asian (Singapore) and US ports in 2011. For a more detailed description of telemetry and sensor performance standards see Annex2.

6.2 USA National Strategy for Global Supply Chain Security

On 23rd January 2012 President Obama adopted the National Strategy for Global Supply Chain. Subsequently, on 25th of January the Secretary of Homeland Security, Janet Napolitano, announced the Strategy at the Davos World Economic Forum.

Although entitled as a '*National*' strategy, it is evident that any policy decisions adopted by USA at this level, will ultimately have repercussions world-wide. However, upon reading the announcement, it is made evident from the beginning that because the USA depends inherently on a global supply chain, it considers that any threats (natural or anthropogenic) must be considered within the context of cooperation not only with customs and border agencies of the USA's major trading partners, but also with international organizations that will collaborate in the development of a more robust global supply chain.

The strategy, which considers the supply chain as one of the major Critical Infrastructures essential for the USA's economy and a critical global asset, presents two goals

- Promote the Efficient and Secure Movement of Goods
- Foster a Resilient Supply Chain.

The first item, in essence, is geared towards increasing the security of the supply chain, whereas the second aims to develop methods that will increase the capacity of the system to return to normal functioning as soon as possible after a significant event has happened. The strategy clearly underlines that security should not undermine the efficiency and the smooth running of the supply chain.

It is stated that, to accomplish this, the US government will, amongst other things: eliminate potential threats as early as possible, improve verification of suspect goods, upgrade the infrastructure conveyances (and here there

is a case for improving on current container technology), and, all in all, maximise legitimate trade flow.

For the second goal, the Strategy will increase resilience by mitigating systemic risk, identify special-protection assets (or critical supply chain nodes), introduce system redundancy–where possible– and promote trade resumption policies and practices in order to return system to a normal performance level as soon as possible.

All the above must be set within a global context, so that international programs are expected to evolve in logistic, technological and policy fields in collaboration with stakeholders involved in supply chain running. Special emphasis is given to information-sharing and the setting of common performance standards.

In order to do this, the document provides a *'Path Forward'* which highlights a number of priority areas. One of these concerns the use of advanced technology and research to develop and test secure cargo systems for all modes of transport. Another key aspect is that the targeted priority areas be developed ''*in concert with industry and foreign governments*'' .

In view of these recent announcements, it would seem appropriate that - within the context of technological developments of more advanced supply chain conveyance systems (of which shipping containers are central), both policy-making and research services from EC institutions should seek to develop collaboration programs with their US counterparts.

It is of interest that whereas the announcement still maintains as a key target the illegal use of the supply chain as a source of insecurity for society at large, there seems to be a new emphasis in pointing out that the supply chain itself be considered as a target, and not just as a vehicle to deliver threats to others. Because of this, the announcement makes special reference to natural events that could also drastically affect the supply chain; for example, there is mention of two natural events that considerably affected the world-wide supply to the automobile manufacturing sector in 2011 (the Japanese Tsunami and Monsoon flooding in Thailand).

For these and other reasons, it would seem appropriate that, as well as evaluating and developing new technologies to improve the anti-tamper security of conveyance systems of the supply chain, it would be beneficial to study the vulnerability of the supply chain itself as a highly complex interconnected network. Thus, adding *network vulnerability research* to that on engineering development would prove to be consistent with the scope of the proposed strategy; one that could fit well within the scope of the JRC's activities and, hopefully, prove to be a useful tool for EC policy in supply-chain critical infrastructure protection.

7. SPOTLIGHT ON TECHNOLOGIES TO BE EXAMINED BY EU PROGRAMMES

Two key technologies stand to have a significant impact on the container manufacturing and logistics industry.

1. Innovative materials
2. Pervasive sensor technology

However, perhaps the most important aspect for future development is not so much the use of these two specific technologies in isolation, but rather the possibilities offered by composite materials –allied to their processing technologies– to be adapted to directly incorporate sensors as part of the fabric of the structural material itself: a, so-called, 'smart' or 'intelligent' structural element. A smart material or component is one that, not only is capable of carrying a desired structural load, but one that can collect and process data from its environment and relay diagnostic information –via a network of similarly smart structures—to a central control unit where decisions can be made as to safety, security or logistics of container traffic flows.

7.3 COMPOSITE MATERIALS TECHNOLOGY

In a separate STEC Action document (deliverable D02.01 of the STEC project 2011) a guideline has been provided of the market costs and production capacity —at European and global levels—of the composites manufacturing industry. Although there is a very wide range of costs which depend on the materials and processing techniques used, it can be said that a reasonable cost for the manufacture of composite material components that could used in the container industry is if the order of 4 €/kg

It can be shown that, to a first approximation, fibre-reinforced composite containers could weigh of the order of 50% that of a steel one; however, given that the production costs would be of the order of 4 times that for steel , it was shown that the net cost of composite containers would be of the order of 4000€, compared to the 2000€ for steel. Composite containers have to make up this loss in a number of ways. In the first place by reducing on the running costs associated with road haulage and any other process where the weight of the container itself has a significant bearing on cost: this implies that a thorough analysis must be made of the potential cost both in cash and CO2-emission savings that could be achieved for every kilo of dead weight saved. The second aspect concerns the fact that, in view of the development of the aim of connecting containers into the, much-touted, Internet Of Things, the materials advantages of composites manufacturing technology (especially their low processing temperature etc) would suggest that the cost of rendering a container 'intelligent' would

probably be reduced for a design based on soft-embedded sensors rather than protruding systems attached to a hard, steel-based, structural system.

Aside from their higher cost, fibre-reinforced composite materials, have one main drawback: the environmental impact of their manufacture and recycling. An analysis is required of the environmental cost that arises due to the fact that composites are, by their nature, not easily bio-degradable. In the first instance it would appear that the typical thermoset resins used for the manufacture of composites are not easily recyclable. Although there are now companies that claim to recycle waste from glass-fibre composite systems, most waste appears to end up in unsustainable land-fill sites.

Having identified the technical aspects that must be revised vis-à-vis the development of the second generation of container structures, and having identified the cost analyses of weight-saving and embedded technology compared to the development of 'smart' container systems based on metallic containers, we come to the second main theme proposed above: ad-hoc sensor network development.

7.4 AD-HOC SENSOR NETWORK ARCHITECTURE

Currently there is no paradigm for the 'smart' container, but at its most basic one can consider a system made up of a sensing device (i.e. one used to detect some physical effect) connected to some sort of radio-transmitter/receiver that allows the system to communicate with the outside world. If every actively-used container were to be fitted with such a system then, potentially, there would be of the order of twenty million such containers circulating around the globe. How they are expected to communicate between each other –if at all— plays a key aspect in the actual physical design of the system. Likewise, there is currently no paradigm for the communication protocol that said systems must have with their control basis; thus, for example, the system may or may not have the capacity to communicate with the control base at any time from any location on the globe with minimum time latency.

The manner in which these systems communicate with the outside world defines the nature of a network, and the ties among the elements that constitute the network confer certain –topological-- characteristics that play a critical role in the vulnerability (conversely, robustness) of the network to keep functioning as efficiently as possible.

Because containers are constantly moving, and because we have no way of predicting a container's future trips, the ensemble of such sensor-equipped containers constitutes an ad-hoc network. If containers were to rely on their neighbours to hop information from one to the other until the message reaches some final destination, then the topology of connectivity is also in a state of flux. In a large port, container bays can extent for hundreds of metres and house thousands of units. In some of the mega -

ports, extending over tens of kilometres, hundreds of thousands of containers are either in transit or waiting for cargo. What will happen to the communication channels if all these 'smart' containers start 'chatting' between themselves, or even, perhaps, over the internet?

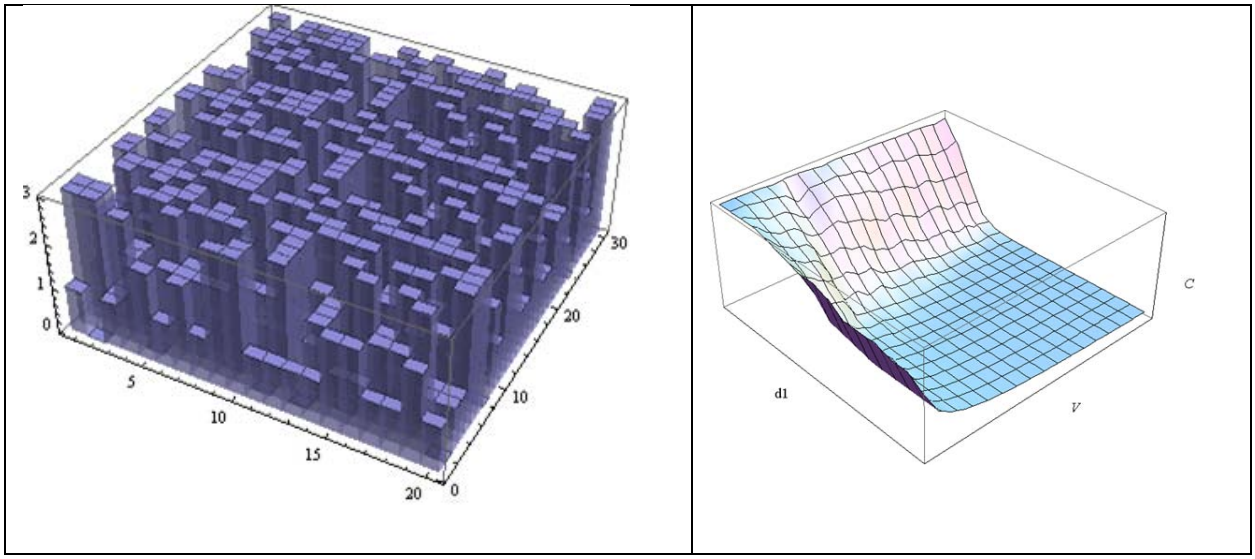


Figure 5 Synthetic container-bay stacking profiles and sensor network connectivity topography. On the left frame: random stacking distribution of 'container' bay profile. Right frame: transceiver connectivity topography for sensor-equipped container bay as a function of transceiver strength and percentage of containers equipped with transceivers (the flat valley floor of lower right-hand corners implies full connectivity between sensors).

These ever-changing topological configurations will place severe constraints on how we choose to design a communication protocol and the nature of the physical system (i.e. batteries, data logging etc).

For example, we could consider the following question: How many randomly dispersed sensors does a bay of stacked containers have to have before we are assured that a single communication path to the central control station is established? The type of scenario is shown conceptually in **FIG**URE 5.

Before considering the physical characteristics of the sensor and transceiver system capacities, or the communication protocol it is required to ensure optimum communication levels, this type of problem can be studied in a synthetic manner using basic mathematical tools.

FIGURE 5 (right) shows the kind of results that may be produced, even with a simple analysis[4] based on graph connectivity measurements. As it turns out, it is possible to establish a single connected-component network that can communicate (by hoping from one container to another) a signal, such as an intrusion-alarm, to a base station, by awakening and nudging information by using only a small percentage of the available containers. These strategies can be used to dimension the lifetime of the batteries and communication protocol of the containers. Hence, these basic mathematical models can provide very useful information to help dimension the physical components (and hence cost) of the sensors and their communication systems.

In order to realise the concept of interconnected smart containers there is still a need to undertake research in the development of ad-hoc sensor networks that could conceivably make an in-road in the container market. The following issues will have to be investigated at length:

- Development of low-cost sensors and transceivers.
- Energy conservation in Ad-Hoc sensor Networks.
- Methods and protocols for node-tracking in mobile container networks.
- Control algorithms for geographically constrained (e.g. port, ship, etc) topologies.
- Development of indefinite battery life or energy-harvesting systems.
- Robustness of sensor equipment to environmental loading.
- Evaluation of acceptable false-alarm propagation models.
- Robustness of the network of interconnected sensors to natural and manmade hazards.
- Performance and design communication protocols adaptable for variable-topology interconnected networks.

There are no technological reasons why, even today, all containers could not be fitted with on-board sensing systems and connected to the outside world. Moreover, millions of such systems exist in the form of modern mobile telephony. The problem for a container-based ad-hoc sensor network would appear to boil down to cost: if the end-users are willing to pay for such systems there is no technical reason why hundreds of millions –never mind tens of millions– of containers could not be connected within a short time-frame. Unfortunately, whereas hundreds of millions of individuals are prepared to pay for mobile telephony networks, the same cannot be said about containers. Which mathematical tools are needed to model such a techno-economic paradigms.

[4] D.K Arrowsmith (London University) and E. Gutierrez (JRC) from ''Ad-hoc sensors networks for secure container bays'' preprint in preparation as JRC Report expected 2012.

Apart from the technology/cost ratios mentioned above, it is important that we not only understand the business model of container shipments, but also develop models of how to introduce the proposed new technologies into the existing container shipping infrastructure. In order to model the effects of such evolving techno-economic systems, it is required to implement complex systems models that can cater for the discrete non-linear nature of container logistics.

These mathematical approaches are essential to develop the underlying sensor-based technology required for the next generation of container technology. Applications of mathematical fields such as complex systems theory, non-linear time-series analysis and network analysis can deal with complex systems composed of discrete packages, of which the dynamics and logistics of shipping containers is a good example.

8. CONCLUSIONS AND RECOMMENDATIONS

In this report we have given a brief overview of the status of container security research along two lines:

- The policy framework in the EU and USA
- The current technologies being considered for improving container security.

It would appear that whereas the EU and USA have a concerted effort to collaborate on the area of supply chain security, their respective research programs in this area are markedly different in the manner in which they are run. Although a number of links have been established (joint workshops, conferences etc.) there appear to be no major joint basic research projects geared towards developing common performance standards suitable for the main parties concerned.

From our analysis it would seem that most of the research, even those few projects that are 'transatlantic' in scope, is geared towards demonstration projects of –usually— proprietary technology, which, even if technically very advanced, leaves little scope for extension to all potential stakeholders (i.e. policy-makers, customs agencies and the container shipping industry)

More specifically, it would appear that both the policy and technological communities have not yet tackled the wide variety of needs and economic constraints imposed, in no small part, by the fragmented nature of the container shipping industry.

In terms of the type and aspect of the research projects, there appears to be a major effort relating to the developing of 'devices' and 'solutions kits' , whereas few projects have examined abstract issues such as network

connectivity and communication protocol concepts, operational research of container movements and sensor deployment, and, perhaps just as importantly, the security threats introduced by the potential to connect the world's container stock to the, so-called, Internet of Things.

Another fundamental issue is Standardisation. In such a developing industry, where no widely accepted standards exist, the temptation is to borrow formats from communications systems that appear to have similar constraints and working environments. The fact that many applications will rely on radio technology certainly makes it reasonable (sometimes enforced) to accept standards (e.g. regarding the use of permitted spectrum). However, given that containers have to travel all over the world, how are these systems supposed to function if they contravene national standards?

These and many other questions motivate the need for international research and standardisation cooperation agreements between the EU and its major trading partners.

9. ANNEXES

A. ANNEX 1: SECURITY AMMENDMENTS of EU CUSTOMS LEGISLATION

The so-called "Security amendments" of the EU Customs legislation were adopted in 2005[5] and in 2006[6]. These amendments introduced the **EU Risk Management framework**, **advance cargo information** as well as a trusted trader program referred to as the **Authorised economic operator Program (AEO).** Since 1st January 2011, these amendments are fully implemented.

These amendments introduced:

- **EU Customs Risk Management framework:** sets out a mechanism aimed at reaching an EU level of protection against commercial or safety and security risks through common control priorities based on common risk analysis criteria. Real time information exchange between operational customs border points and the sending of alerts is ensured through the Customs Risk Management System (CRMS). The EU Risk management framework is the backbone of the EU multilayered risk-based approach aimed at focusing controls on high risk cargo whilst facilitating low risk consignments and managing huge volumes of goods.
- **Advance cargo information:** Since 1.1.2011 advance cargo information must be provided to Customs for all goods entering or leaving the EU Customs territory. This enables Customs to carry out risk analysis for security and safety purposes, to detect serious risks prior to the arrival of the goods in the EU and to take immediate action, where necessary. Advance cargo information is provided by electronic means and should be linked in the risk targeting systems.
- **Authorised economic operators (AEO):** operational since 1.1.2008, the EU AEO program sets out a general trusted trader program providing customs simplifications and benefits as regards security and safety measures. The AEO program constitutes a major component of the multilayered risk based approach focusing Customs' main attention on high risk consignments whilst expediting low risk consignments.

---

[5] Regulation (EC) No 648/2005 of the European Parliament and of the Council amending Council Regulation (EEC) No 2913/92 establishing the Community Customs Code.

[6] Commission Regulation (EC) No 1875/2006 amending Commission Regulation (EEC) No 2454/93 on implementing provisions to the Community Customs Code.

B. ANNEX 2: Performance criteria and standards for the wireless communication systems for the CSI programmes

The four in the CSI projects and their goals are outlined in Table 1.

TABLE 1 CONTAINER SECURITY TECHNOLOGY PROJECTS FUNDED BY DHS S&T DIRECTORATE (SOURCE US GOVERNMENT ACCOUNTABILITY OFFICE REPORT GAO-10-887 SEPTEMBER 2010)

Project name	Key project requirements
Advanced Container Security Device (ACSD)	• Detect container door opening, door closing, and door removal. • Detect a 3-inch diameter hole in the container on any six sides. • Detect human presence within the container. • Cost less than $175 per container trip.
Container Security Device (CSD)	• Detect container door opening, door closing, and door removal. • Monitor the status of any seals or locks.
Hybrid Composite Container	• Composite container • Meet or exceed ISO requirements. • Sensor grid • Detect a 3-inch diameter hole in any six sides of a container.
Marine Asset Tag Tracking System (MATTS)	• Communicate a container intrusion alarm within 5 minutes of the alarm occurring. • Provide operational availability at least 95 percent of the time. • Possess a power source to operate for 30,000 hours. • Cost less than $175 per container trip.
General	• Provide a 95 percent probability of intrusion detection. • Provide a combined probability of false alarm and critical failure of 0.2 percent. • Possess a power source to operate for one trip (1,680 hours). • Time to detect and report a hole in the container ≤ 1 second • Alarm Detection Latency ≤ 1 minute • Lifetime Power Source Duration ≥ 3,600 hours • Continuous enabled time ≥ 1,680 hours

For the purposes of clarification, the following terms in the table are given[7] as follows:

- *"Hole in the Container is an opening that was not part of the original container design or construction, that was created during container monitoring, and that provides access to the interior volume of the container.*

- *Alarm Detection Latency is the elapsed time between occurrence of an alarm event and communication relay of alarm status.*

    - *E.g., time from detection of a breach by a subsystem of the BSD to successfully communicating the breach to the CSD.*

- *Lifetime Power Source Duration is defined as the length of time during which no maintenance of the power source is required and only includes time in the armed state. This includes enabled time and time from testing of the container to stuffing in a disabled but powered state"*

The following list of technical specifications (again, provided by G. Bennett from Georgia Tech) are defined for the CSD programme for the electronic equipment used for the wireless sensor intrusion detection and communication systems.

- *Temperature:*
    - *Operate: -40^{o}C to +70^{o}C (IEC 60721-3-2 Table 1)*
    - *Survive: -50^{o}C to -40^{o}C and +70^{o}C to +85^{o}C (IEC 60721-3-2 as above, and IEC 60721-3-2 Class 2K5 (modified low end to -50^{o}C)*
- *Thermal Shock*
    - *As listed in IEC 60721-3-2, Table 1, Class 2K4:*
        - *from 20^{o}C to -40^{o}C in 4 minutes maximum*
        - *from -40^{o}C to 20^{o}C in 4 minutes maximum*
        - *from 20^{o}C to 70^{o}C in 4 minutes maximum*
        - *from 70^{o}C to 20^{o}C in 4 minutes maximum*
- *Humidity:*
    - *95% humidity over the temperature range from -40^{o}C to +70^{o}C (from IEC 60721-3-2, Table 1)*
- *Structural Vibration and Mechanical Shock Environments*

[7] Source: G. Bennett from Georgia Tech , at Proc. of 4th European Conference on Transport Logistics, 13-14 October 2011, Thessaloniki Greece

- *Shock: 10-inch empty container drop & 5-inch fully-loaded container drop (from IEC 60721-1, Table 1, Item No. 6.1.3)*
- *Vibration (from IEC 60721-3-2, Table 5):*
  - *3 m^2/s^3 from 10-200 Hz*
  - *1 m^2/s^3 from 250-2000 Hz*

- *Precipitation*
  - *Salt Mist, Rain, Impacting Water/Water from sources other than rain, Frost/Ice, Sand & Dust, Fungus (From IEC 60721-1 and IEC 60721-3-6)*
- *Radiation and Electromagnetic Environments*
  - *Radiated emissions shall not exceed the limits given in 47 CFR Part 15 (UC FCC Rules on radio frequency devices).*
  - *Radiated emissions shall not exceed the emission limits for enclosure port type (please see Appendix B for specifics on enclosure ports) equipment installed in the bridge and deck zone of a ship or in the general power distribution zone of a ship, from IEC 60533, Tables 2 and 3, consolidated in the table* Table 2 *below.*

TABLE 2 POWER CONSTRAINTS ON WIRELESS COMMUNICATION SYSTEMS

Frequency Range	**Limits**
150 kHz to 300 kHz	80 dBµV/m to 52 dBµV/m
300 kHz to 30 MHz	52 dBµV/m to 34 dBµV/m
30 MHz to 2 GHz	54 dBµV/m
Except 156 MHz to 165 MHz	• BµV/m

European Commission
EUR 25298 – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: An overview of research programmes and prospective technology in the development of more secure supply chains: The Case of Shipping Containers

Authors: E. Gutiérrez (DG-JRC), W. van Heeswijk (DG-TAXUD), D. Arrowsmith (Queen Mary, University of London)

Luxembourg: Publications Office of the European Union

2012 – 32 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1018-5593 (print), ISSN 1831-9424 (online)

ISBN 978-92-79-24168-0 (pdf)
ISBN 978-92-79-24167-3 (print)

doi:10.2788/23670

Abstract

The development of new, more secure, container systems should consider the main techno-economic items and devise a solution that, not only provides increased tamper-resistance, but also contains economically beneficial buy-in features that will motivate the adoption of new container models by the shipping trade. This report provides an overview of these aspects within the context of EU policy and R&D programmes in this area.

LB-NA-25298-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.

Publications Office

ISBN 978-92-79-24168-0

9 789279 241680