Sensor Based Risk Assessment for the Supply of Dangerous Products

Laurent Gomez
SAP Research France
Sophia Antipolis, France
Email:laurent.gomez@sap.com

Omar Gaci
ISEL
Le Havre, France
Email: omar.gaci@gmail.com

Jean Pierre Deutsch
LogPro Conseil
Paris, France
Email: jpdeutsch@logpro.fr

Elie El-Khoury
3Cap Technologies
Stuttgart, Germany
Email: elie.el-khoury@3cap.de

***Abstract*—As a consequence of globalisation, supply chain systems recently evolved toward a dynamic network of firms and industries. This complexification of supply chain processes raises several challenges in particular with respect to compliance to regulations (e.g., safety, security). With the multiplication of intermediate actors, a single non-compliant actor might jeopardize the safety of population and actors involved in supply chain process. There is, therefore, a clear need for risk management in order to mitigate the occurence of potential threats due to non compliance to regulation at the execution of the supply chain process. Traditionnal approaches tend to rely on human operators checks, or collection of contextual information from sensors locally (e.g., warehouse, truck). Therefore, there is risk of a disruption of regulation checks along the process execution. In this paper, we propose the delegation of risk assessment to sensor nodes, attached to the supplied products, for an automatic risk assessment all along the supply chain execution. Empowered with monitoring capabilities, sensor nodes are meant to trigger alert in case of contextual constraint violation along the supply chain. Our goal is to raise the awareness of the supply chain players with an early alerting service to enforce the regulations.**

***Index Terms*—Supply Chain Management, Sensor Networks, Security.**

I. INTRODUCTION

The globalization of trade has been accompanied by a growth of the number of intermediate partners involved in the supply chain. Those intermediate partners are mainly in charge of transportation or storage of products. As a consequence, the risk of disruption of the supply chain increases. For example, the supply of chemical substances raises risks of fire, explosion and environmental pollution. In order to mitigate those risks, and prevent any serious impact on population safety, safety regulations are in place, at international and national levels. Those risks might have a strong impact on population safety, or on the environment. Supply chain players have to be complaint with those regulations which impose them handling, transport and storage constraints on chemicals.

A. Disruption of compliance checks

There is, therefore, a clear need for compliance check at the execution of the supply chain. It is common practice in supply chain that each actor performs local regulation checks, in particular within storage unit, for example for SEVESO [1] classified sites. Measures for risk of fire, gas emission, detection of theft are already put in place locally. But, those measures only concern local checks since tracking and monitoring information are pushed to local supply chain systems only. We have therefore a disruption of regulation checks, as tracking and monitoring information are not forwarded to all the supply chain actors. For example, in the case of ambient temperature reaches chemical flash point during transportation, the storage unit receives the asset, without being informed of the inherent risk of explosion. Depending on the actors, those regulation checks, on temperature for example, are strongly dependent on the certification of the actors. For a site classified SEVESO II, like the K+N's [2] warehouse, strong measures on over heating, gas emission, or chemical leaking monitoring are put in place. But, this is not the case for all the actors involved in the supply chain. Therefore, we observe a disruption of the regulation checks, while each actor is focusing on its own compliance with regulations, with a different degree of implication, depending on their certification. To that extent, non compliance of a single actor might have a direct or indirect impact on the safety of the overall supply chain. For example, for a chemical, we might have a risk of explosion of a product which has been exposed to high temperature during transportation. When stored in the K+N's warehouse, the explosion risk remains for a while, until the temperature of the product goes back to normal. As a conclusion, it is difficult for supply chain management systems to evaluate continuously, without any disruption, the risk of incident occurrence.

B. Delegation of risk assessment to sensor nodes

Any disruption of regulation check might jeopardize the execution of the supply chain process. Therefore continuous risk assessment is critical for supply chain management systems. But, so far, risk assessment have been addressed only locally, within each unit of the supply chain. Meaning that non compliance of previous actor of the process can have a direct or non direct impact of the compliance with regulations. In order to cope with the disruption of risk assessment at the execution of the supply chain process, we propose to delegate risk assessment to sensor nodes attached to the products. Empowered with monitoring capabilities, wireless sensor nodes can evaluate continuously, and at runtime, the compliance with regulations. Sensor nodes are therefore capable of continuous evaluation of any mismatch between product's context and the constraints defined by regulations. To that extend, they support

 ISBN: 978-1-61208-207-3

us with early detection of risks.

C. Outline

The remainder of this paper is organised as follows: in Section II, we describe a supply chain scenario motivating our approach. In Section III, we discuss related work with respect to regulation compliance at the execution of the supply chain. Section IV is dedicated to our approach: delegation of compliance checks to sensor nodes. In Section V, we evaluate our approach. Finally, we conclude in Section VI.

II. Importation of dangerous products from China to Europe

In order to illustrate our approach, we propose to use a supply chain scenario defined in the scope of the RESCUEIT [3] project. Related to the importation of dangerous products from China to Europe, this scenario has been elaborated and validated by end users such as Kuehne and Nagel (K+N) and the group Casino [4].

Chemicals are imported from a Chinese harbour toward the harbour of Le Havre, in France. Shipped products are household and gardening chemicals. These products are meant to be shipped by boat from a Chinese harbour. When received at the Le Havre harbour, the merchandise is checked by customs against REACH [5] regulations.

REACH is the European Community Regulation on chemicals and their safe use (EC 1907/2006) [5]. It deals with the registration, evaluation, authorisation and restriction of chemical substances. The aim of REACH is to provide an additional layer of protection for humans and the environment through the better and earlier identification of the intrinsic properties of chemical substances. To that extend, REACH introduces specific constraints on chemicals along the supply chain. They include the flash point, incompatibilities between products, and humidity conditions for chemicals.

At the Le Havre harbour, French customs with the support of an Approved Economic Operator [6] proceed to a merchandise integrity check. After a check of administrative document describing the content of the cargo, customs verify the quantity and quality of the products received.

Once quality checks have been performed at Le Havre harbour, and customs have verified that the merchandise is compliant with safety regulations, products are shipped by pickup trucks toward the warehouse located close to Savigny le Temple. This K+N warehouse,dedicated to the storage of dangerous products, is classified SEVESO II. This classification defines a set of safety management systems, emergency planning and land-use planning and a reinforcement of the provisions on inspections to be carried out by classified sites. In this case, specific safety measures are implemented on site, such as storage rules (e.g. limited quantity of chemical stored at the same place). Finally, household and gardening products are distributed to retailers (e.g., Casino supermarket).

A. Identified products constraints

In the scope of this scenario, we identify three gardening and household products ICPE-classified. ICPE [7] is a French nomenclature for ”Installation Classee pour la Protection de l’Environnement”. This classification defines a set a measures to be enforced for the handling, storage and transport of dangerous products. Each of the identified products has specific normative ICPE constraints: ICPE 1412, 1432, 1172.

Inflammable liquids are classified under ICPE 1412. In order to manipulate this product, gloves, glasses, a protective clothing, helmet and eye wash are mandatory. Products classified 1412 are a harmful and polluting products. Its flash point is 66 Celsius degrees. The flash point of a volatile liquid is the lowest temperature at which it can vaporize to form an ignitable mixture in air. In addition, this type of product must not be mixed with acids, bases or oxidizing. In addition, it is self flammable in large quantity at high temperatures. Therefore, in addition to risks of pollution along the supply chain, this product represents a significant risk of fire, if exposed to high temperature. In order to mitigate this risk, monitoring of ambient temperature is crucial.

ICPE 1432 products are liquefied gas inflammable. To manipulate this type of product, gloves, classes, protective clothing, wash eye, are mandatory. With respect to transport, they are classified UN 1950 or aerosol, with the mention of the restricted quantity, and a tag code 2.1-5F. Their flash point is between 13 and 13,4 Celsius degrees. It must not be in contact with acids and metal. Same as for ICPE 1412 products, in order to mitigate risk of fire, it is important to monitor ambient temperature.

Products classified as ICPE 1172 are dangerous for environment, extremely toxic for aquatic organisms. Gloves, classes, mask, and eye wash are required for the handling of Ronstar. Ronstar is classified UN 3007. In addition, this is irritant. Packaging of Ronstar is classified type III.

For transport, those dangerous products are classified UN 3082 [8], meaning dangerous products for the environment. UN code is four digit used for the transport of dangerous products. As this type of products is considered as slightly dangerous, packaging of type III is mandatory, with the mention of the restricted quantity. We therefore identified three additional constraints: shock, falling, opening. Shock and fall deal with any shock, falls occuring to the product, pallet or container, which might damage the product. Regarding opening, it refers to any attempt to product theft with the opening of container or packaging.

Table I summarizes identified constraints per ICPE classification. Those constraints are meant to be monitored by sensor nodes.

B. Impacts

In case of accidents along the supply chain, the impact on population safety, and on the environment can be disastrous. We identified three major impacts: fire, gas emission, dispersion of extinction waters.

 ISBN: 978-1-61208-207-3

Classification	Shock	Falling	Opening	Flash Point
ICPE 1412	X	X	X	13C
ICPE 1432	X	X	X	66C
ICPE 1172	X	X	X	-

TABLE I
IDENTIFIED CONSTRAINTS PER CLASSIFICATION

Depending on its intensity, fire can have more or less serious impact on individual health (e.g., slightly burning to death). In addition, merchandises and their packaging are combustible. They both have a strong calorific potential. In case of fire, the combustion of stored products would cause an important radiation of heating flux through the other storage areas in the warehouse. Toxic gases are also emitted in case of fire. Depending on the quantity of emitted gas, the effects on individuals can be lethal. In addition, under the effect of heat, dangerous products can cause the emission of toxic gas such as hydro-cyanic acid, oxides of sulphur. Fire fighters use specific products in order to extinguish fire. Those products (e.g., water plus chemical, powder, foam) contains chemical which aim at either decreasing the heat, or stifling the fire. Nevertheless those products drain polluting products which must not be thrown into the environment (e.g., river). Such incident may cause pollution of ground, underground or surface waters. It is therefore important to handle properly liquids used for fire extinstion in order to avoid them to be thrown outside of the building.

III. RELATED WORK

Automatic risk evaluation and propagation is currently an active topic in research institutions and industries alike. However, few works have been done over the automation of risk assessment for reasons related to human and technological limitations.

Aagedal et al. [9] introduced the CORAS project, which aims to provide methods and tools for precise, unambiguous, and efficient risk assessment of security critical systems. The focus of this project is on the tight integration of viewpoint-oriented modelling in the risk assessment process. Risk evaluation is done by determining the level of risk, categorize it, determine the interrelationships between risk themes, and prioritize the resulting risks themes. Although the CORAS addresses security-critical systems in general, it is interesting to note the risk assessment methodology used. In fact the authors use a model-based risk assessment.

Ivanov and Sokolov [10] focused their work on assessing and controlling the risks related to container supply chains (CSCs). However, due to the complexity of the risks in the chains, conventional quantitative risk assessment (QRA) methods may not be capable of providing sufficient safety management information, as achieving such a functionality requires enabling the possibility of conducting risk analysis in view of the challenges and uncertainties posed by the unavailability and incompleteness of historical failure data. Combining the fuzzy set theory (FST) and an evidential reasoning (ER) approach, the paper presents a subjective method to deal with the vulnerability-based risks, which are more ubiquitous and uncertain than the traditional hazard-based ones in the chains.

Wagner and Neshat [11] discussed the disruptions that occur more frequently and with more serious consequences. During and after supply chain disruptions, companies may lose revenue and incur high recovery costs. If the capability of measuring and managing supply chain vulnerability existed, they could reduce the number of disruptions and their impact. In this paper the authors developed an approach based on graph theory to quantify and therefore mitigate supply chain vulnerability. Although the approach seems promising, its applicability depends heavily on the availability of quantified data for the drivers of supply chain vulnerability. Without grounded data this method will not work. Additionally, the graph theoretical approach may not fully take into account the dynamic nature of supply chain vulnerability. Graphs are perhaps too static to be able to answer the dynamic changes in the supply chain at runtime.

IV. OUR APPROACH

A. Integration of Wireless Sensor Netwroks into Supply Chain

As depicted in Figure 2, whereas RFID are used for products tracking, sensor nodes can be used at different levels of the supply chain. Depending on the product value, sensor node can be used either at product level, packaging or pallet. In the scope of the RESCUEIT project [3], we have validated this assumption with end users of the project, K+N and the Casino Group. As we are addressing only low valuable products (e.g., household, gardening products), tagging RFID and sensor monitoring is done at pallet level.

Whereas RFID is rather focusing on identification of products (e.g., identification, classification), WSNs (Wireless Sensor Networks) are meant to monitor and control the supply chain environment. To some extent, RFID are not restricted to unique identification of products along the supply chain, but can be associated to information related to the classification, and dangerousness of products. Based on those classifications, and with regards to the regulations (e.g., safety, quality), the handling, storage, and transport constraints are identified. In this context, WSNs are meant to enforce those constraints (e.g., incompatibilities with other products, flash points). Based on the sensed supply chain context at runtime, sensors tend to evaluate mismatches between the constraints defined by regulations and the current context. Any violation of constraint is therefore reported to the supply chain management system as a risk of incident.

B. Terminology

Supply chain management systems are in charge of the delivery of products, or *assets*, to final customers. Depending on its classification, specific regulations define *constraints* along the supply chain, based on the *activity* on the assets (e.g., storage, transport, transformation). Therefore, regulations vary from one activity to another. A constraint on the stability of

 ISBN: 978-1-61208-207-3

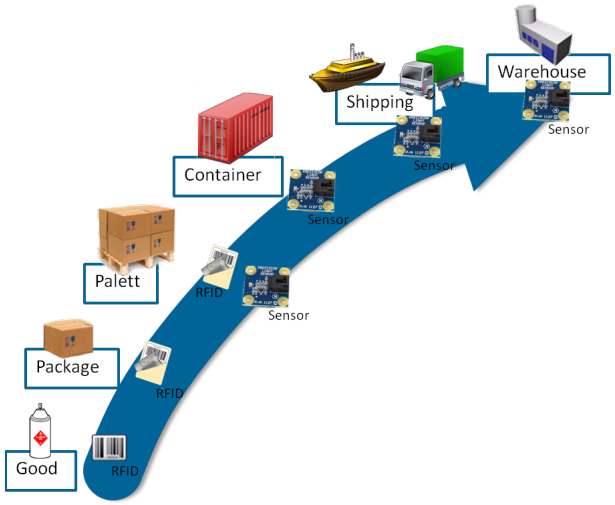

Fig. 2. Integration of RFID and WSN into Supply Chain

rack is only applicable in storage location for example. The non-compliance with regulations might lead to risky situation. For example, considering the flash point of product classified ICPE 1412, the following constraint is defined: *temperature must not exceed 13 Celsius degrees*. Whenever this constraint is fullfilled, then the risk of explosion increases. This example illustrates the relationship between the constraint and the *context*. *Context* is any kind of information which characterizes the environment of the asset. For the sake of clarity, we define the notation of *asset*, *classification*, *constraint*, *activity*, *context*, and *risk* as follows:

- *asset* is any product, or merchandise manipulated along the supply chain toward final customer. Assets are characterised by their classification.
- *constraint* is a representation of regulations over a specific asset, based on its classification.
- An *activity* is any steps in the supply chain, from production to delivery to final customer, including transformation, loading in palett, trucks, or rack.
- context is any type of information characterising the environment of an asset along the supply chain.
- *risk* is the probability that an incident occurs in the supply chain, due to a non compliance with regulations.

In Figure 1, we identify the following relationships: constraints, based on regulation, depend on asset classification and activity along the supply chain execution. For example, constraints on the stability of palett containing chemicals is to be fullfiled during storage activity. In addition, risk is depending on mismatch betwen constraints on products and their context in the supply chain. If a constraint on temperature is defined, the probability of incident occurence is depending on a violation with the context of the asset.

C. Methodology

As depicted in Figure 3, our approach is organised around the four following steps: (i) constraints extraction, (ii) node configuration, (iii) in-node risk evaluation, and (iv) node alerting. At (i) constraint extraction, constraints over product classification and supply chain activity are defined. For that purpose, regulations (e.g., safety, quality) are evaluated in order to extract per asset classification (e.g., chemicals, food), and per supply chain activity (e.g., transportation, storage) a set of constraints. For efficiency reasons, this task is meant to be performed outside of the node. At (ii) node configuration, the identified constraints are therefore pushed to sensor nodes attached to assets. Once pushed on nodes, those constraints are evaluated in real time by the sensor nodes during the (iii) in-node risk evaluation step. Whenever a sensor observes a mismatch between the current context and its set of constraints, it triggers an alert ((iv) node alerting).

D. Constraint definition

In Section II-A, we identify a set of constraints to be monitored depending on products' classification. Those constraints can be related to temperature, shock and container opening as depicted in Table I. While extracted from regulation, there are represented in an XML format. That XML representation is mapped product's classification, extracted from the regulations. In that context, we distinguish two types of constraints: monitoring and alerting ones. Monitoring constraint deals with regular monitoring of a given type of information, such as temperature.

```
<event>
  <name>Monitoring</name>
  <description>Monitoring Temperature every second</description>
  <monitoring>
  <sensorType>TEMPERATURE</sensorType>
  <sampleRate>00:00:01</sampleRate>
  </monitoring>
</event>
```

Alerting constraints define threshold over given sensor data type. Whenever that threshold is reached, an alert is triggered by the node. In addition, we define a notion of temporality on alert. An alert is triggered by the node only if the constraint is violated for a given time, for example light above threshold for 15 seconds in a raw.

```
<event>
  <name>CO</name>
  <description>Container opened.</description>
  <alert>
    <delayBetweenNotifications>00:00:30</delayBetweenNotifications>
    <constraintType>TEMPORAL</constraintType>
    <timePeriod>00:00:15</timePeriod>
    <expression>
      <constraint>
        <sensorType>LIGHT</sensorType>
        <compareOperator>GREATERTHAN</compareOperator>
        <value>1900</value>
      </constraint>
    </expression>
  </alert>
</event>
```

Finally, we enable combination of constraints. Combination of simple constraints enables an abstract of a constraint on the node. In the following example, we define a constraint, that if it is violated, trigger an alert for container overturn. This abstract constraint is based on acceleration monitoring.

```
<event>
  <name>PO</name>
  <description>Container has overturned.</description>
  <alert>
    <delayBetweenNotifications>00:00:30</delayBetweenNotifications>
    <constraintType>NONTEMPORAL</constraintType>
    <expression>
      <expression>
        <expression>
          <constraint>
            <sensorType>ACCELX</sensorType>
            <compareOperator>GREATERTHAN</compareOperator>
            <value>1000</value>
          </constraint>
        </expression>
        <binaryOperator>OR</binaryOperator>
        <expression>
```

 ISBN: 978-1-61208-207-3

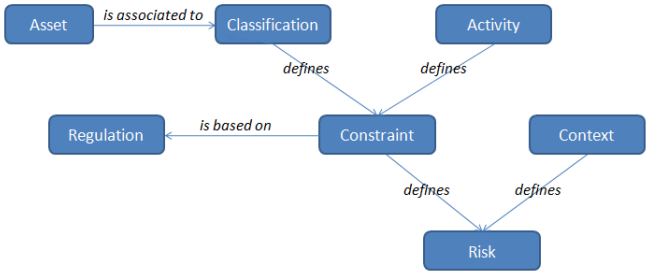

Fig. 1. Terminology

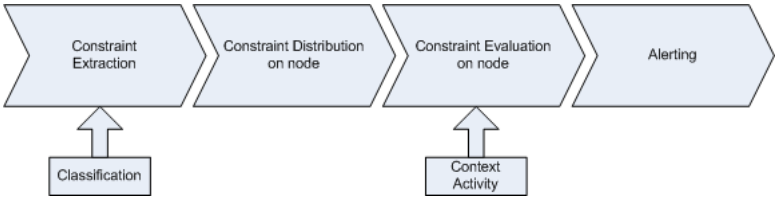

Fig. 3. In-node risk evaluation process

```
        <constraint>
          <sensorType>ACCELX</sensorType>
          <compareOperator>LOWERTHAN</compareOperator>
          <value>-1000</value>
        </constraint>
      </expression>
    </expression>
  ...
  </alert>
</event>
```

E. Constraint evaluation

Sensor nodes have restricted resources available. XML processing is barely performed on such devices. For that reason, we need a specific representation of an constraint on the node. On the one hand, the representation must have a low memory cost and, on the other hand, its representation must be easily executable on an embedded device. A set of constraints is therefore represented on the node with:

- a set of simple constraint: Each constraint follows the template

  ```
  [SensorType]
  [Operator]
  [Value]
  [TypeofConstrainst]
  [<TemporalValue>]
  ```

  (e.g., A = ”Alert if Temperature GreaterThan 20”,Alert if Alert if Temperature GreaterThan 20”,Alert if Temperature GreaterThan 20”, B = ”Alert if Tilt LowerThan 50 for more than 5 seconds”).
- bytecode: that describe the execution of simple constraints.

The bytecode is inspired from the RPN (Reverted Polish Notation). Each operator follows their operands. (e.g., if A and B are simple constraint, the evaluation of ”A AND B” will be written as ”A B AND”). The interpretation is stack-based; that is, operands are pushed onto a stack, and when an operation is performed, its operands are popped from a stack and its result pushed back on. In the bytecode, we support three operands: AND, OR, and NOT.

On regular basis, the monitoring node collects all available ambient information (e.g., noise, temperature). It evaluates each simple constraint, and afterwards executes the loaded bytecode. If a violation in the combination of simple constraint is identified, an alert is sent to the SCM system.

F. Architecture

Figure 4 depicts our overall architecture. It is organised around three layers: supply chain management, mediation layer, and wireless sensor networks.

Supply chain management systems aim at monitoring assets along the execution of the supply chain. They have to be alerted in case of any incident which might disrupt the supply chain process. In our case, we use the container tracking system from SOGET [12].

As described previously, a WSN hosts a set of wireless nodes, attached to specific assets.

A mediation layer finally eases the integration of sensor nodes with supply chain. Within the mediation layer, we distinguish two services: the *sensor broker* and the *crossbow agent*. The sensor broker serves as a dispatcher for the subscription coming from the SCM system. The crossbow agent is in charge of the interface with the crossbow nodes [13] used for our evaluation.

As mediation layer, we use a mediation layer called the Middleware for Device Integration (MDI). MDI is a mediation layer developed by SAP Research for the integration of smart items (e.g., WSNs, RFID) into business applications. Based on an OSGi Service Platform, MDI is an agent-based middleware which enables both monitoring and controlling of smart items.

G. Message flow

In Figure 5, we depict the subscription to asset monitoring. Therefore, SCM systems have to subscribe to MDI for any

 ISBN: 978-1-61208-207-3

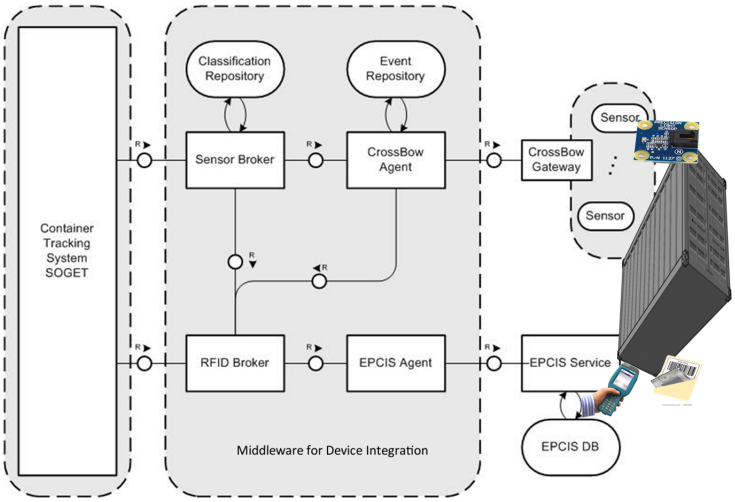

Fig. 4. Architecture

asset monitoring or occuring alerts (e.g., temperature exceeds flash point, shocks on the pallets).

As depicted in Figure 5, the SCM subscribes to monitoring or alerting for a given product, uniquely identified with its *productid*. In addition, the SCM provides the ICPE classification of the product to be monitored.

This classification is mapped to a set of contraints to be programmed on the nodes. This mapping is done at sensor broker level, with a dedicated database. The XML representation is pushed to the crossbow agent which generates a dedicated set of simple constraints and a bytecode to be executed on the crossbow node. The set of constraints and bytecode is specific to the type of sensor nodes used. Finally, the node is programmed over the air, with new constraints mapping monitored product's classification.

On regular basis, constraints and the bytecode are evaluated. If a constraint violation occurs, the sensor node triggers an alert. The MDI then notifies the subscriber.

V. Evaluation

In order to validate our approach, we propose an implementation of risk assessment on Crossbow sensor nodes [13]. Our goal is to evaluate the overhead on battery and memory introduced by our mechanism.

For the evaluation of our in node risk assessment approach, we used MICAz (MPR2400) processing unit equipped to a MTS310CAsensor board. Energy has been provided by two 1.2V rechargeable batteries with a capacity of 2200mAh. Each battery has been charged to a voltage of 2.65V before test start.

For the evaluation we propose four scenarios :

- Continuous packet sending every 30 seconds
- Monitoring of sensor data and continuous transmission every 30 seconds
- Monitoring of sensor data, evaluation of constraints violation and continuous transmission every 30 seconds
- Monitoring of sensor data, evaluation of constraints and Alerting only in case of constraint violation.

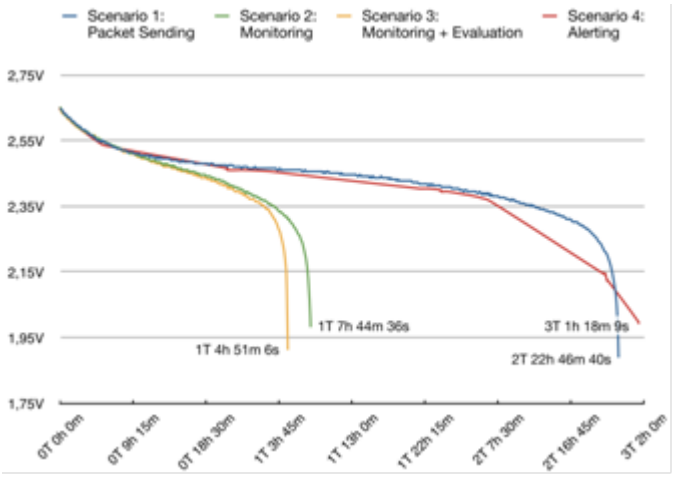

Fig. 6. Battery Evaluation

A. Battery overhead

Figure 6 depicts the consumption of energy for the four scenarios identified previously. We can observe three majors facts from that figure:

- Comparing Monitoring and Monitoring+Evaluation, we clearly demonstrated that the negligible overhead of evaluation of constraint violation.
- Comparing Packet Sending and Alerting, we observe that constraint evaluation do have a negligible overhead on energy consumption.
- Comparing Monitoring+Evaluation and Alerting, we confirm the fact that packet sending is main source of energy consumption. Following alerting strategies, we observe a gain in energy consumption of almost 60%.

B. Memory overhead

The sensors memory is limited. The used MICAz processing unit is equipped with an Atmel ATmega128L processor (8 bit

 ISBN: 978-1-61208-207-3

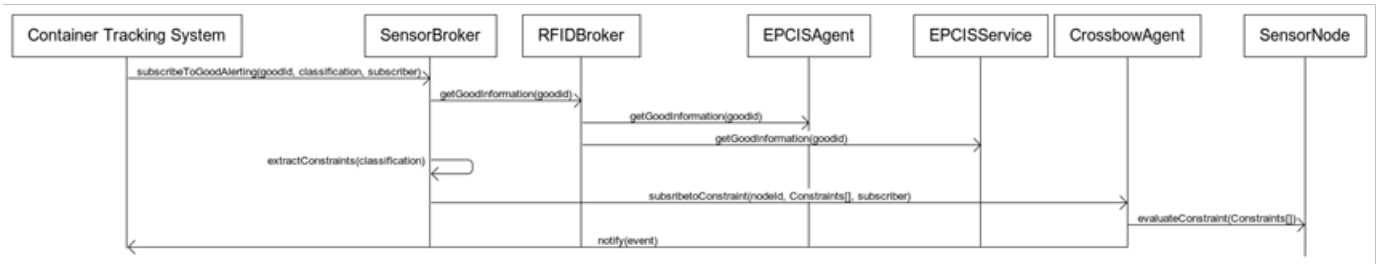

Fig. 5. Message Flow

architecture), 128 K bytes of program is available in memory (ROM) and 4 K bytes for the runtime (RAM). The code in charge of constraint evaluation occupies 50.868 bytes in the ROM over 496.758 bytes available (10%), while using 3.737 bytes of RAM over 36.494 bytes available (10%). Those measurements are provided by the NesC, after source code compilation. Overall the memory consumption of our approach is relative limited.

VI. Conclusion and Outlook

With the shift towards a global open market in the recent decade, optimising production life-cycle of products is key to gaining the maximum profit. Ensuring safety of the products throughout the supply chain is a main aspect of the optimisation. The supply chain is typically made up of multiple companies who coordinate activities to set themselves apart from the competition.

Risk analysis techniques have emerged as a way to evaluate the potential risk inherent along the supply chain, and the identification of several different options in how to proceed. Often, these options are designed to minimize the risk while obtaining the most benefit, or at least finding ways to protect the product while taking the risk.

We discussed the current techniques for risk analysis. We show that current techniques lack the autonomy at execution time therefore, whenever an error occurred, a human intervention was always required to locate the problem and trigger a mitigation plan to prevent further propagation. we showed that this technique is not portable and scalable.

In this paper, we proposed to go a step further, with the delegation of risk assessment to sensor node attached to the supplied products. We identified a set of constraints mapped to the products classification. Those constraints represent the risk conditions of the item in question.

In addition, we propose the implementation and evaluation of our approach in the scope of the RESCUEIT [3] project. As future work we foresee the improving of the calculation of the risk value, to take into account the values from previous executions of the same supply chain. In addition, the issue related to the confidentiality of the generated alerts is still opened.

Acknowledgement

The research was partially funded by the German Federal Ministry of Education and Research under the promotional reference 01ISO7009 and by the French Ministry of Research within the RESCUE-IT project [3]. The authors take the responsibility for the content.

References

[1] ECD, “European council directive - control of major-accident hazards involving dangerous substances,” 1996. [Online]. Available: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0082

[2] Kuehne and Nagel, 2012. [Online]. Available: http://www.kn-portal.com/

[3] L. Gomez, M. Khalfaoui, E. El-Khoury, C. Ulmer, J. Deutsch, O. Chettouh, O. Gaci, H. Mathieu, E. El-Moustaine, M. Laurent, H. Schneider, C. Daras, and A. Schaad, “Rescueit : securisation de la chaine logistique orientee service depuis le monde des objets jusqu’a l’univers informatique,” *Workshop Interdisciplinaire sur la Securite Globale*, 2011.

[4] Casino, 2012. [Online]. Available: http://www.groupe-casino.fr/

[5] {European {Chemicals {Agency, “Guidance for identification and naming of substances under reach,” 2007.

[6] DGDDI, “Direction des douanes et droits indirects, approved economic operator,” 2005. [Online]. Available: http://www.douane.gouv.fr/page.asp?id=3421

[7] IPCE, “Installation classifiee pour la protection de l’environnement,” 2010. [Online]. Available: http://www.installationsclassees.developpement-durable.gouv.fr/

[8] UNECE, “United nations economic commission for europe, recommendations on the transport of dangerous goods - model regulations,” 2005. [Online]. Available: http://www.unece.org/trans/danger/publi/unrec/12e.html

[9] J. Aagedal, F. den Braber, T. Dimitrakos, B. Gran, D. Raptis, and K. Stolen, “Model-based risk assessment to improve enterprise security,” in *Enterprise Distributed Object Computing Conference, 2002. EDOC ’02. Proceedings. Sixth International*, 2002.

[10] D. Ivanov and B. Sokolov, “Handling uncertainty in supply chains,” in *Adaptive Supply Chain Management*. Springer London, 2010, pp. 81–91.

[11] S. M. Wagner and N. Neshat, “Assessing the vulnerability of supply chains using graph theory,” *International Journal of Production Economics*, vol. 126, no. 1, pp. 121–129, July 2010. [Online]. Available: http://dx.doi.org/10.1016/j.ijpe.2009.10.007

[12] SOGET, 2012. [Online]. Available: http://www.soget.fr/

[13] Crossbow, 2012. [Online]. Available: http://www.xbow.com/

 ISBN: 978-1-61208-207-3