Smart networked objects: towards a civilization shift

Paris, October 22\textsuperscript{nd} 2013 - Networked smart objects perform a growing share of control and monitoring in industrial plants and buildings and increasingly in our homes.

Securely connecting these smart objects to networks and managing related data therefore stands as a tremendous challenge for the time to come. "Building France of communicating objects" is listed as one of the 34 plans for New Industrial France, recently defined by the French government.

The 2013 edition of CARTES, Secure Connections Event, which runs from November 19 to 21, will focus on the strategic area of the Internet of Things. The conference on Thursday, November 21, "Smart Cities: embedded connectivity and intelligence" will point to the existing technologies and future challenges, with leading companies such as Gemalto M2M, Giesecke & Devrient, Oberthur Technologies and Wincor Nixdorf.

For years, industrial control systems have relied on smart objects like sensors and actuators to interact with factory processes. Formerly, a typical system consisted of smart objects that sent information to a control device. Today, smart objects and devices are tiny, rather inexpensive to manufacture and don't need a lot of power - an essential characteristic since many smart objects are expected to operate long-term without access to networked electrical power.

In the meantime, the advent of low cost wireless broadband connectivity for new embedded devices and handhelds has made Internet more and more pervasive. Not only an "Internet of People" but also an "Internet of Things" where the web provides a medium for physical world objects to interact. The Internet of Things (IoT) is a worldwide network of intercommunicating devices integrating ubiquitous communications, pervasive computing, and ambient intelligence.

A multitude of everyday life applications

Virtually any manufactured object either already is or has the potential to be a smart object. Nearly all home appliances but also furniture, clothes, vehicles, roads and smart materials are readable, recognizable, locatable, addressable and/or Power Source Location controllable.

Smart objects have a triple role in most networks; they act as data collectors, data processors and traffic forwarders for other objects in the network. Some of the most strategic applications of smart object technology include:

- Health & Medical applications, including disabled assistance platforms, remote patient monitoring, portable diagnosis, automated drug delivery, real-time tracking and monitoring of
doctors and patients

- Environmental applications, including the monitoring of crops and livestock
- “Smart grid” electricity monitoring and response capabilities
- Vehicle theft and location systems
- Home networking and home automation
- “Smart cities”, where parts of infrastructure and government services are digitally connected and optimized
- Industrial applications like monitoring material and product quality, environmental control of the office buildings, factory process control and automation
- Military applications, including monitoring of forces and equipment and detection of nuclear and/or biological attacks

The strategic impact of these applications resides in that they all require some combination of data confidentiality, high systems availability and/or strong authentication of users and information.

80 billion smart objects – connected anywhere, anytime to the cloud

IDATE Institute estimates that there were 15 billion smart connected devices in 2012, and this figure is expected to reach 80 billion by 2020. Smart objects are becoming a huge phenomenon, causing a profound shift in user behavior and expectations, and placing huge demands on communications infrastructure.

They are a driving force behind bandwidth explosion and create greater demand for applications and entertainment content delivered in an optimized way anywhere and anytime. Content Service Providers therefore have to build inherent capacity, flexibility and adaptability into their operations so that they can rapidly respond to completely new services driven by new smart objects and devices. This evolution will greatly rely on Cloud computing, an Internet-based computing where shared resources, software, and information are provided to computers and other objects on demand.

Security and reliability challenges

At a time when electronic devices were simpler and unconnected, securing them was unnecessary as they weren’t networked to anything and so could neither be attacked remotely nor cause harm to anything else. Today smart objects - devices that are essentially small computers with communications capability - perform a wide range of functions, interact with each other and even more critically communicate with the world at large. The proliferation of smart objects therefore creates new opportunities for hackers to disrupt services and steal sensitive information, just as they do on conventional computer networks. The New York Times’ IT system is reported to have been recently hacked via an Internet-connected thermostat. This has triggered some anxiety about industrial and other forms of espionage.

It’s important to realize that smart objects often play critical roles in information gathering, management and control, sometimes in life-and-death applications – yet they are vulnerable. Upwards of 120,000 new pieces of malware and attacks on embedded systems (the
building blocks of smart objects) are identified every week. In the past, this type of device was rarely attacked, often because there simply weren’t a lot of them around, or because their architecture was strange and unfamiliar when compared to PCs. The fallout is that today’s smart objects are significantly more vulnerable to attack than desktop systems are.

“It is not yet routine to secure smart objects and networks and everyone agrees that security is required going forward. Since smart-object networking is still in its infancy, there is tremendous technical and market opportunity in this arena, especially for the smart security industry” comments Isabelle Alfano, CARTES Secure Connexions Event Director.

A quick glance at the future

The so-called connected life will have a major socio-economic impact worldwide. According to Michael O’Hara, Chief Marketing Officer, GSMA, Asia is expected to be the most connected region of the world both in terms of the number of networked devices and in terms of revenues.

Generally speaking, every city in the world is exploring the smart city concept as a way to make themselves better places to live, work, and grow. They implement and experiment with solutions based on smart networked objects for promoting e-government initiatives, integrating public transport with Intelligent Transportation Systems or developing ways to cut carbon footprints.

At home or at work, at any time and in any place, a growing part of our lives will depend on smart networked objects.

<table>
<thead>
<tr>
<th>Did you know it?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>In China</strong>, traffic telematics could help commuters reclaim nearly two hours each of their time every week</td>
</tr>
<tr>
<td><strong>In India</strong>, reducing power theft and increasing usage efficiency via smart meters could save enough electricity to power more than 10 million homes</td>
</tr>
<tr>
<td><strong>In Japan</strong>, the adoption of mHealth for elderly care could result in savings equivalent to the medical expenses of 1 million senior citizens each year</td>
</tr>
<tr>
<td><strong>In South Korea</strong>, technology enhanced learning could save families between 8,000 to 12,000 USD on private tuition for their children</td>
</tr>
</tbody>
</table>

Source: Report from PwC and GSMA on the socioeconomic impact of the connected life in Asia by 2017
Figure: The "Internet of Things", an ever-growing list of connected devices (source: the IPSO Alliance)

Isabelle Alfano, Director of the Cartes Secure Connexions Event 2013, will be happy to answer any questions. Please do not hesitate to contact us.

Stay in touch in real-time and get the latest news on the trade show:
- visit the Internet site: www.cartes.com
- follow us on Twitter «@_cartes » and use #cartes2013
- join the CARTES Events group on LinkedIn [link]
- download the MyCARTES mobile application
- join the CARTES Facebook Community

Press Contacts - Actifin

Jennifer Jullia
+33 (0)1 56 88 11 19

Marie-Caroline Cardi
+33 (0)1 56 88 11 13
cartes@actifin.fr

About CARTES Secure Connexions Event 2013:
CARTES Secure Connexions Event 2013 will be held from 19 to 21 November 2013 at the Paris-Nord-Vilelpinte exhibition centre. It is the world leading event dedicated to secure payment, identification and mobility solutions.
With 137 countries represented, 435 exhibitors and 140 conferences attended by international experts, CARTES Secure Connexions is the key trade show for all players in this fast-moving market. In 2013, at the 28th CARTES show Brazil will take centre stage.