Contract No. IST 2005-034891

Hydra

Networked Embedded System middleware for
Heterogeneous physical devices in a distributed architecture

D2.1a Scenarios for usage of Hydra in Building Automation

Integrated Project
SO 2.5.3 Embedded systems

Project start date: 1st July 2006 **Duration: 48 months**

Published by the Hydra Consortium **25 January 2007 - version 1.41**
Coordinating Partner: C International Ltd.

Project co-funded by the European Commission
within the Sixth Framework Programme (2002 -2006)

Dissemination Level: Public

IN-JET APS
JEPPE ÅKJÆRSVEJ 15
3460 BIRKERØD
DENMARK

T +45 45 82 13 24
E JTH@IN-JET.DK
W WWW.IN-JET.DK
CVR 19 05 47 80

1. Introduction

The Hydra project develops middleware for networked embedded systems that allows developers to create ambient intelligence applications. System developers are thus provided with tools for easily and securely integrating heterogeneous physical devices into interoperable distributed systems.

The middleware will include support for distributed as well as centralised architectures, cognition and context awareness, security and trust and will be deployable on both new and existing networks of distributed wireless and wired devices that typically are resource constrained in terms of computing power, energy and memory. Hydra middleware will be based on a Service Oriented Architecture (SOA), to which the underlying communication layer is transparent.

Creating scenarios of end-user behaviour and interaction with platform functionality is an extremely useful instrument for identifying key technological, security, socio-economic and business drivers for future end-user requirements. The scenarios will provide the framework for subsequent iterative requirement engineering phase.

From the scenarios and storylines, a systematic formalisation of all relevant user requirements and subsystem functional, security and societal requirements will be derived. Functional user requirements specifications will involve the most important aspects of user expectations in the chosen application domains.

This document describes the work performed with the aim of establishing a set of plausible usage scenarios on 2015 involving the typical use of Hydra in the Building Automation domain.

2. Executive summary

Creating scenarios of end-user behaviour and interaction with platform functionality is an extremely useful instrument for identifying key technological, security, socio-economic and business drivers for future end-user requirements. The scenarios will provide the framework for subsequent iterative requirement engineering phase.

A series of one-day user workshops for each user domain have been organised to bring together appropriate expertise and experience. The activities carried out include identification of uncertainties, grouping and segmenting and flip/flopping (grouping in main directions). At the end of each workshop, scenes, acts and scripts for the scenarios have been defined. The results of these activities have been documented in a set of scenarios for each domain.

2.1 Scenario Thinking – The IDON method

Scenarios are snapshots of possible/alternative futures that help us plumb that uncertainty. Scenarios provide coherent, comprehensive, internally consistent descriptions of plausible futures built on the imagined interaction of key trends. The purpose of Scenario Thinking is to challenge the preconceived notions people have of the future, or their maps, and to afford people the flexibility to change those maps. The IDON method consists of two parts: *Scenario Development* and *Scenario Deployment*.

The scenarios are developed in the *Scenario Development* part using experts and based on knowledge and systematic analysis. The aim is to develop four mind-challenging scenarios for each user domain by mixing inevitable trends with creative fiction.

In the *Scenario Deployment* part, technical experts and project decision makers interpret the scenarios and extract a framework for the functional and trust and security requirement specifications.

The core of the IDON technique is to examine a set of wider environmental factors ambiguities and uncertainties in order to resolve, which role they are likely to play in the unfolding of scenarios. The initial phase of the IDON method involves three steps: Gathering environmental factors grouping them according to their degree of uncertainty and deciding their relative position.

The next phase in IDON deals only with the factors with high uncertainty and direct impact on future trends. The uncertain factors are reformulated as "either / or" questions (flip/flop) and grouped according to connections and associations. Finally they are combined into four distinct possible futures extrapolated from the thinking done by the group.

The outcome of this Scenario Thinking process is 12 equally plausible scenarios for the future use of Hydra middleware in 2015 in three different user domains: Building Automation, healthcare and agriculture.

2.2 The Building Automation scenarios

Four scenarios have been developed to illustrate distinctively different aspects of future user behaviour in the Building Automation domain. The scenarios have been made in response to the question:

How do we develop and deploy intelligent, ubiquitous and secure networked products and services in buildings and facilities in 2015?

We have focused the scenario on the domain of building automation and facility management for commercial and residential buildings and we created the four scenarios from two clusters: "Interconnectivity" (in contrast to interoperability) and "Universal focus" (pointing to either end-users or developer users).

The four scenarios are:

1. Developer-user centric + Connected Systems (*Walking the Dog)*
2. Developer-user centric + Interoperable Systems *(The Beehive)*
3. End-user centric + Interoperable Systems *(Easy does it!)*
4. End-user centric + Connected Systems *(Daredevils)*

The scene shows a typical developer user or end users situation around 2015. The developer user is either employed in a manufacturing company that develops devices, products, embedded and networked systems or services, or he/she is working with system integration, either as a traditional system integrator, an engineering company or as a customer building in-house systems. The developer is faced with the task of creating new or improved embedded systems and applications, which is to be based on a high degree of networking capability of various devices.

The scenes highlights that smart home technologies are widespread and affordable to everyone. Most smart appliances have high value propositions and make the homes more attractive. With people moving frequently, there is a sound market for bundles of products and services. Preventative maintenance is one such service offered, which successfully is used to increase customer loyalty. Generally the manufacturers have a high influence on the way the products are installed and they are able to impose access control and authentication schemes on end-users.

3. The Building Automation domain

3.1 Background of the Building Automation domain

One generally accepted definition of intelligent building technologies are "…integrated technological building systems, communications and controls to create a building and its infrastructure which provides the owner, operator and occupant with an environment which is flexible, effective, comfortable and secure".

The availability of new ICT solutions imposes a dramatic enrichment of the capability of Building Automation components and systems. The expectation among facility owners and managers is that control systems can be integrated and provide a high level of "building intelligence." This concept speaks to managing facilities as assets transforming building data into knowledge and using that to make intelligent business decisions in real time. The driver of building intelligence and many other major trends is economic pressure to increase efficiency and productivity continuously and to do more with less. Another major trend in building is the need for improved security systems, which can be supported by smart and integrated building automation systems. In addition to this, facility management agreements are more and more based on incentives about savings: this implies that facility managers strive to find opportunities for savings in order to share them with the end-users.

The trends affect both major players in the Building Automation market: The *users* (facility managers) and the *suppliers* (components manufacturers and industrial services companies).

3.1.1 Facility managers

The facility managers want plug-and-play interoperability. In fact, the concept of interoperability for facility executives can be traced back to three elements:

- Harmonic coexistence: in this case, what a facility executive wants for his buildings are products from different manufacturers that operate independently without interfering with each other
- Inter-changeability: in this definition of interoperability, all chillers operate so identically, for example, that only the nameplate distinguishes one from another
- Integration that allows for individuality: most facility executives, however, want interoperability somewhere between these two extremes. They want plug-and-play interoperability. They want products that can be integrated easily without using custom hardware or software. But they also want to leave room for supplier differences within product lines.

Facility managers are pushing Building Automation systems vendors to transform today's closed technologies into Web-enabled applications. Facility managers are driving Building Automation systems by demanding open systems. The open architecture approach means widespread acceptance and sharing of hardware and software designs, standards, and protocols and is seen as being critical to the successful spread of intelligent building technology. It will lead to a greater interoperability of various systems.

3.1.2 Products, components and service suppliers

Most product companies will thus soon realise that device networking isn't only possible, it's essential for their future business. Moreover, in a market where customers continuously ask for more complex and integrated services, it clearly results that these new applications and intelligent solutions can help to reduce the risk that product companies take by assuming a greater and greater management responsibility (from simple installation to global service).

A major challenge for most existing Building Automation systems is that they are not wireless. Consequently they are primarily installed in new buildings. Specialists must do all configurations and systems cannot be remotely controlled. Many users do not find that these systems give sufficient value for money. Consequently, the market today is quite limited, but with a great potential in existing buildings, once the proper products are introduced. By deploying an industry-wide Hydra middleware, all products can be service-enabled and made interoperable with just a few device drivers and supporting models for interoperable functions.

A survey conducted by the Wireless LAN Association and NOP World Technology showed that the average payback for a wireless installation is about nine months. The survey also concluded that the average wireless user is 22% more productive than his or her wired counterparts. Productivity benefits are quantified at 48% of the total return on investment of a wireless network.

3.1.3 Business opportunities

Internet-enabling of industrial products are bringing huge business opportunities, which we are only about to discover now. Everything from a pump, a building, an industrial machine, and an office's thermostat will have the potential to be networked thus creating a huge network of interconnected devices. Product companies can use their devices to enter into a customer service relationship that increases both revenue and customer management. In many ways, the product companies can use the networking technology to reduce the burden of Asset Management and reduce the total cost of ownership for the end-user. But it may not be the end-users that initially have the most to gain from the networking. It can well be the businesses that support them. Product companies can use device networking technologies to reduce costs, reduce installation time, improve effectiveness, neutralise learning differences, bridge knowledge gaps, gain more customers, and pursue new opportunities.

3.2 Organization of workshops

The planning of the workshop took place at a meeting on 10 August 2006 at C-LAB in Paderborn, Germany. At the meeting, the major features of the workshop were decided, the roles were distributed and the participants in the workshop identified. It was decided to conduct the workshops under the label of "smart home", and to invite at least one expert from each of the following areas, in order to have a wide spread in expertise and experience:

Consumer behaviour expert	Security
Facility manager	Smart house expert
Appliance manufacturer	Telecom
Service company	

The scenarios were developed through a one-day workshop held at C-LAB in Paderborn, Germany on 17 October 2006. Moderator of the workshop was Jesper Thestrup (IN-JET). Supporting roles were assigned to Christine Ludwig (C-LAB), Trine F. Sørensen (IN-JET) and Tommaso Foglia (INNOVA).

The users participating in the workshop came from various parts of Europe and were selected because of their personal expertise and their reputation. The participants were:

1. Markus Reichling, Grundfos GmbH, Germany (pump manufacturer)
2. Günther Ohland, Smart Home Initiative Paderborn, Germany (smart home lab)
3. Carsten Thomsen, DELTA, Denmark (technology provider in embedded systems)
4. Simone Moreali, McPerson, Italy (audio and video manufacturer)
5. Walter Schneider, Benq, Germany (device manufacturer and telecom services)
6. Robbie Schäfer, University of Paderborn, Germany (ambient intelligence expert)
7. Gernot Graefe, Siemens Business Services (consumer behaviour and market development)
8. Bert Plonus, Miele AG, Germany (appliance manufacturer)
9. Andres Marin, Universidad Madrid, Spain (security expert)
10. Heinz-Josef Eikerling, Siemens Business Services (device expert and partner)

3.3 Selection of application area and time horizon

As for the time horizon, the experts were concerned about the availability of complementary technologies and infrastructures, if the time horizon was too long. On the other side, a too short horizon would probably lead to less imaginative scenarios. As a compromise, the time horizon of 2015 was chosen. By the end of the Hydra project in 2010 there is plenty of time to deploy the platform and develop the business cases to roll out in time for the scenarios in 2015.

3.4 Trigger question

The "Trigger question" for identification and grouping of environmental factors is:

> How do we develop and deploy intelligent, ubiquitous and secure networked products and services in buildings and facilities in 2015?

3.5 Identification of environmental factors

Factors were identified from among all the possible environments that could influence Building Automation products and applications in 2015:

- Technology trends
- Market trends
- Economic futures
- Social values and life-styles
- Ethical and value questions
- Products, production and logistic systems
- Ecological and environmental issues
- Global political influences

In the following, we present the results of the brainstorming discussion, summarise the items of both certainty and uncertainty identified by the experts as well as the subsequent analysis and clustering performed by the consortium.

The workshop participants defined a total of 75 factors in all areas:

Technology trends (T)
Systemic concepts
One common interface
Information overflow avoided
New connectivity methods
Technical standards
Programming languages
Self-learning capabilities
Transferable personalised settings
Intelligence used proactively
Speech control
Transferability of systems
Firewalls
Security configurability
Interface constraints
Wearable computers
Flexibility
Device interaction
Network complexity
Interoperability standards
Simple touch pads
Predictability
Automatic upgrades
Multimodal interfaces
Prevention of misuse
Interacting systems

Market trends (M)
Structured access required
End-user programming
Warranty period
Business models
Business value creation
Imposed access control
Preventive maintenance
Bundling of services
Device networking required
Simplicity

Economic futures (€)
Energy costs neutrality
Interoperability costs
Smart home affordability
Increased costs for new functions
Energy savings
Affordable devices

Social values and life-styles (L)
PDAs available to all
Mobile phones available to all
End-user acting responsibly
Accepted value propositions
End-user confidence
Attractiveness of homes
High moving rate
eInclusion
Graphical interfaces for the disadvantaged
Trusted domestic environments
Agreed access rules

Ethical and value questions (V)
Third party authorization
Proper functioning
Trust models
Choice of biometrics
End-user configurability
Reputation of manufacturers
Transparency
Automatic updates
Suitability of terminals
System reliability
Clearly defined security responsibilities

Products, production and logistic systems (P)
Certification
Centralized security
Open access for manufacturers
Remote access for manufacturers
Ergonomics

Ecological and environmental issues (E)
Energy efficiency
Energy savings
Renewable energy sources

Global political influences (G)
Warranty coverage
Consumer protections
Data protection
Government access to personal data

A further explanation of each factor is found in Appendix A.

The environmental factors were then group according to the certainty and impact criteria, which yielded the following matrix:

High UNCERTAINTY

Joker

V Clearly defined security responsibilities

M Structured access required

T Systemic concepts

M End-user programming

T One common interface

T Information overflow avoided

€ Energy costs neutrality

Indirect Impact

€ Interoperability costs | M Warranty period | € Energy savings

G Warranty coverage | T New connectivity methods

L PDAs available to all | T Technical standards | V Automatic updates

Either/or

T Programming languages | V Third party authorization | V Proper functioning

M Business models | P Centralized security | M Business value creation | G Data protection

L End-user acting responsibly | V Trust models | V End-user configurability

E Energy efficiency | V Choice of biometrics | V Reputation of manufacturers | P Certification

T Self-learning capabilities | T Transferable personalised settings | V Transparency

T Intelligence used proactively | L Accepted value propositions | T Speech control

L End-user confidence | T Transferability of systems | G Consumer protections

Direct Impact

M Imposed access control | P Open access for manufacturers | T Firewalls

€ Smart home affordability | T Security configurability | V Suitability of terminals

E Renewable energy sources | L Attractiveness of homes

G Government access to personal data | T Preventive maintenance

T Interface constraints | L Mobile phones available to all

Scene

M Bundling of services | L High moving rate

T Wearable computers | € Increased costs for new functions | L eInclusion

T Device interaction | T Flexibility | V System reliability | T Network complexity

M Device networking required | T Interoperability standards | M Simplicity

T Simple touch pads | T Predictability | P Remote access for manufacturers

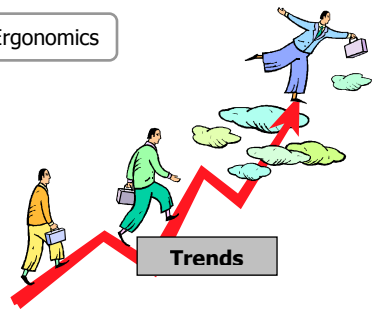
T Automatic upgrades | T Multimodal interfaces | E Energy savings

T Prevention of misuse | € Affordable devices | P Ergonomics

L Graphical interfaces for the disadvantaged

L Trusted domestic environments

L Agreed access rules | T Interacting systems



Trends

High CERTAINTY

3.6 Flip-flopping the pivotal uncertainties

Looking at the factors in the "Either / or" quadrant marked we now turn to grouping them in clusters. Each of the clusters will form different scripts in our scenarios.

We now think of each of the uncertainties as a question, for which there are two possible outcomes: The "flip" (+) and the "flop" (-) outcome. When the factor in question has either "flipped" or "flopped", the uncertainty is resolved.

The following table presents all uncertainties in the Either/or quadrant and there related flip-flow questions.

Interoperability costs What are the additional costs for producers to make their devices interoperable?	+	The additional costs of providing interconnectivity are insignificant compared to the system price
	-	The costs of interconnectivity with other systems are prohibitive to most manufacturers
Warranty period Will the warranty period for products be decreased in the future?	+	The warranty period will increase due to market demand
	-	The warranty period will decrease due to lack of market demand and fast obsolescence
Warranty coverage Will the issue of warranty coverage for interconnected products be a regulatory issue?	+	Warranty coverage is a regulatory issue and is not related to specific products or services
	-	Warranty coverage is determined by the market forces for the products or services in question
New connectivity methods Will new technologies be introduced for interconnecting devices?	+	New technologies (e.g. the human body) will be introduced for interconnecting devices
	-	Only traditional technologies (i.e. wired and wireless) are used for interconnecting devices
PDAs available to all Will entire population use PDAs?	+	Most end-users own and wants to use PDAs
	-	Only few end-users own and use PDAs
Technical standards Will there be technical standards introduced and dominating?	+	Technical standards for interoperability of systems are introduced and globally accepted
	-	There are few or no technical standards for interoperability of Building Automation systems
Programming languages Will there be sufficient programming languages available?	+	There are common programming languages available for developing interoperable applications
	-	There are only traditional programming languages for embedded systems available
Certification Will device drivers, interfaces and applications need a third party certification?	+	Device drivers, interfaces and applications can obtain third party certification of interoperability
	-	Device drivers, interfaces and applications are solely based on manufacturers own descriptions
Third party authorization Will authorization be handled by third party authorization bodies?	+	Authorization will be provided by a mix of separated trust entities and third party
	-	Authorization will be provided only by third party authorization bodies
Proper functioning How well do systems function in their operating environments?	+	Interconnected systems generally function well in their operating environments
	-	End-users experience frequent problems with the functionality of interconnected systems

Business models Will it be necessary to introduce new business models?	+	Manufacturers will routinely introduce new business models that improve the value proposition
	-	Manufacturers will generally stay with the existing and well proven business models
Centralized security Will the security model be centralised across the network?	+	The security model will be distributed across the network and individualised for each application
	-	The security model will be centralised and all systems will use the same model
Business value creation Will manufactures introduce new products and services with sound value propositions?	+	Manufacturers will launch new offerings with sound value propositions based on interconnectivity
	-	Manufacturers are not able to introduce new products and services based on interconnectivity
End-users acting responsibly Will end-users feel responsible for using the devices/products correctly?	+	End-users expect manufacturers are responsible for correct use of connected devices/products
	-	End-user will accept responsibility for correct use of connected devices/products
Trust models Will manufacturers be able to impose trust models?	+	End users will demand to choose their own trust models
	-	Manufacturers will be able to impose their trust models on end-users
Energy efficiency Will smart homes provide more efficient use of energy resources?	+	Intelligent building concepts will be able to use overall energy resources more efficiently
	-	Intelligent building concepts will lead to an overall increase in the of use energy
Energy savings Will end-users focus on systems to save energy?	+	End-users will prefer systems that have the ability to save energy
	-	End-users will not always be able to choose energy saving system, but must accept what is offered
Choice of biometrics Do end-users want freedom to select the most suited biometric device?	+	End-users wants the freedom to select the most suited biometric device for security
	-	End-users cannot chose specific security devices beyond what is offered by the manufacturer
End-user configurability Do end-users want to be able to configure their system?	+	End-users will be able to fully configure their systems
	-	End-users do not want to and cannot configure their own system
Reputation of manufacturers Will reputation of manufacturers have any influence?	+	End-users choice of trust model is only marginally influenced by individual manufacturers' reputation
	-	Each manufacturers' reputation will dominate the end-users' choice of trust model
Self-learning capabilities Will systems have self-learning capabilities?	+	The systems will have self-learning capabilities
	-	The systems will not have self-learning capabilities
Transferable personal settings Will houses, hotels etc. be able to adjust to individual computing and ambient preferences?	+	New environments (e.g. hotel rooms) will be able to adjust to individual ambient preferences
	-	Every environment will have to be separately adjusted to individual ambient preferences
Transparency Do end-users want full insight into the functionality provided by the system?	+	End-users want full insight into the functionality provided by the system
	-	End-users are not concerned about the details of the functionality provided by the system

Intelligence used pro-actively Will system intelligence assumed responsibility?	+	Embedded AmI intelligence will often assume responsibility for part of the system's functionality
	-	There will be no network based functionalities outside the individual components and systems
Accepted value propositions Will the value propositions be clear and acceptable?	+	Value propositions for intelligent buildings will generally be clear and demanded by end-users
	-	Value propositions for intelligent buildings are often not so evident for the end-users
End-user confidence Are end-users confident that products work properly?	+	End-users needs continually to be made confident that products and systems work properly
	-	End-users are generally not informed and involved when products and systems work properly
Speech control Will the system be based on speech recognition and natural language premises?	+	End End-user interaction is based on new modalities (e.g. speech recognition and natural language)
	-	End-user interaction is based on traditional modalities i.e. with no speech control
Transferability of systems Will the system follow the end-user?	+	End-users can move the system when moving to new premises or homes
	-	The system is location specific and cannot follow the end-user to new locations
Consumer protections Are there laws and regulations to protect consumer interests?	+	Consumer interests are the sole responsibility of the consumers themselves
	-	There are strong laws and regulations in place to protect consumer interests
Data protection Are there laws and regulations to protect private data?	+	It is up to the end-user to make his own provisions to protect his private data
	-	There are strong laws and regulations in place to protect the privacy of end-users' data
Automatic updates Will automatic update require approval from end-users?	+	Automatic updates require approval from end-users and procedures for this are built into the system
	-	Automatic updates do not require approval from end-users but are immediately implemented

3.7 Clustering the uncertainties

We will now group the pivotal uncertainties in two groups by searching for connections and associations between the various uncertainties.

When inspecting all 31 uncertainties it becomes obvious that about half of them are related to the identity of *the Universal Focus* that drives breakthrough changes in Building Automation technologies. Such breakthrough changes can be driven by a strong focus on user demands is called "Market Pull" and is characterised by technology development that is driven by end-user needs, rather than by ideas or capabilities created by technology developers and researchers.

Conversely, "Technology push" is characterised by technology development that is driven by ideas or capabilities created by the technological advances with manufacturer and their developer-users in the absence of any specific customers needs. In "Technology Push", innovations are created and then appropriate end-user applications are sought that fit the innovation or the ambitions of the manufacturer.

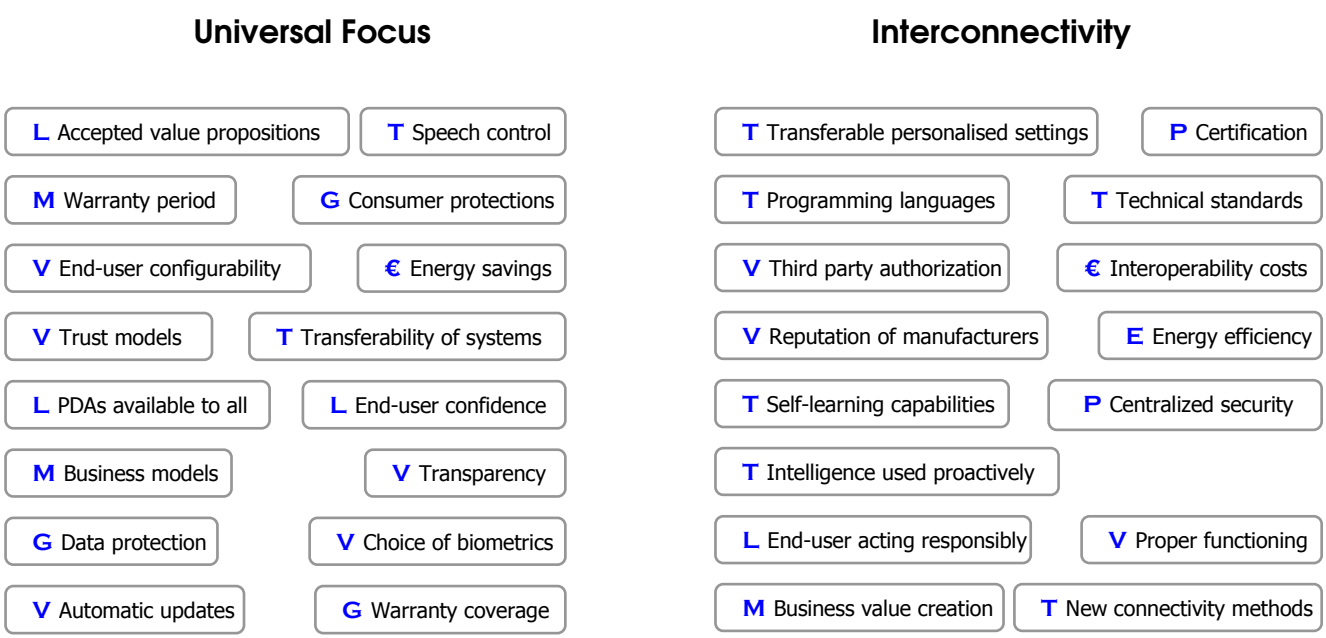
A specific cluster of uncertainties related to future technologies in Building Automation is related to end-user configurability and transferability of ambient settings between locations, specific modalities

for end-user interaction, end-user's attitudes towards security, trust and privacy and regulatory actions to protect consumers.

Clustering of uncertainties of this kind can be termed **"Universal Focus"** as shown in the figure below. Within the cluster, uncertainties tend to counter align in flip-flop questions so that if one flips, the other will flop (e.g. technology pushed or market pulled innovation).

The other cluster of uncertainties is related to the extent that Building Automation products are able to interconnect and create interoperable, intelligent networked systems. In this cluster, the uncertainties relate to how the products interconnect, the types of intelligent applications that can be supported, the security issues related to distributed and networked systems, and the way business models can be developed to create sustainable values.

The uncertainties in this cluster also tend to align in flip-flop questions, i.e. they will all flip or all flop simultaneously, like a domino effect. This cluster has been termed **"Interconnectivity"**.



3.8 Naming the sub plots

Having identified all the flip-flop questions and grouped the uncertainties in two clusters, we are now ready to perform the last step before scenario write-up, i.e. naming the different subplots that will define the scripts.

In the clusters we now deploy the flip-flop questions from above. We analyse and group the responses thus resolving the entire cluster as a large-scale flip or a large-scale flop. We do this for each cluster at the time.

In the **Universal Focus** cluster we arrive at the following large-scale flips and flops:

Big Flip Cluster "Universal focus"	**Big Flop Cluster "Universal focus"**
• End-users will be able to fully configure their systems • End-users want full insight into the functionality provided by the system • End-users can move the system when moving to new premises or homes • End-users needs continually to be made confident that products and systems work properly • Automatic updates require approval from end-users and procedures for this are built into the system • End-user interaction is based on new modalities (e.g. speech recognition and natural language) • Most end-users own and wants to use PDAs • End-users wants the freedom to select the most suited biometric device for security • End users will demand to choose their own trust models • Value propositions for intelligent buildings will generally be clear and demanded by end-users • Manufacturers will routinely introduce new business models that improve the value proposition • End-users will prefer systems that have the ability to save energy • It is up to the end-user to make his own provisions to protect his private data • Consumer interests are the sole responsibility of the consumers themselves • Warranty coverage is a regulatory issue and is not related to specific products or services • The warranty period will increase due to market demand	• End-users do not want to and cannot configure their own system • End-users are not concerned about the details of the functionality provided by the system • The system is location specific and cannot follow the end-user to new locations • End-users are generally not informed and involved when products and systems work properly • Automatic updates do not require approval from end-users but are immediately implemented • End-user interaction is based on traditional modalities i.e. with no speech control • Only few end-users own and use PDAs • End-users cannot chose specific security devices beyond what is offered by the manufacturer • Manufacturers will be able to impose their trust models on end-users • Value propositions for intelligent buildings are often not so evident for the end-users • Manufacturers will generally stay with the existing and well proven business models • End-users will not always be able to choose energy saving system, but must accept what is offered • There are strong laws and regulations in place to protect consumer interests • There are strong laws and regulations in place to protect the privacy of end-users' data • Warranty coverage is determined by the market forces for the products or services in question • The warranty period will decrease due to lack of market demand and fast obsolescence
which leads to the name: **END-USER CENTRIC**	*which leads to the name:* **DEVELOPER-USER CENTRIC**

The "big-flip" of the **Universal Focus** cluster sets out very *end-user centric* scenarios where end-users have a considerable freedom to configure the systems to their own desire and generally be in control of the systems in most situations. Combined with many of the environmental factors with high certainty, it points in the direction of scenarios with very strong end-user participation.

The "big-flop" situation is similarly dominated by *developer-user orientation* and the view of manufactures of systems, components, devices and services for Building Automation. The system view often takes over from the end-user view.

In a similar way we can group the "Interconnectivity" cluster:

Big Flip Cluster "Interconnectivity"	**Big Flop Cluster "Interconnectivity"**
• Technical standards for interoperability of systems are introduced and globally accepted • New environments (e.g. hotel rooms) will be able to adjust to individual ambient preferences • There are common programming languages available for developing interoperable applications • Device drivers, interfaces and applications can obtain third party certification of interoperability • Embedded AmI intelligence will often assume responsibility for part of the system's functionality • The systems will have self-learning capabilities • The additional costs of providing interconnectivity are insignificant compared to the system price • New technologies (e.g. the human body) will be introduced for interconnecting devices • The security model will be distributed across the network and individualised for each application • Authorization will be provided by a mix of separated trust entities and third party • End-users choice of trust model is only marginally influenced by individual manufacturers' reputation • Interconnected systems generally function well in their operating environments • End-users expect manufacturers are responsible for correct use of connected devices/products • Intelligent building concepts will be able to use overall energy resources more efficiently • Manufacturers will launch new offerings with sound value propositions based on interconnectivity	• There are few or no technical standards for interoperability of Building Automation systems • Every environment will have to be separately adjusted to individual ambient preferences • There are only traditional programming languages for embedded systems available • Device drivers, interfaces and applications are solely based on manufacturers own descriptions • There will be no network based functionalities outside the individual components and systems • The systems will not have self-learning capabilities • The costs of interconnectivity with other systems are prohibitive to most manufacturers • Only traditional technologies (i.e. wired and wireless) are used for interconnecting devices • The security model will be centralised and all systems will use the same model • Authorization will be provided only by third party authorization bodies • Each manufacturers' reputation will dominate the end-users' choice of trust model • End-users experience frequent problems with the functionality of interconnected systems • End-user will accept responsibility for correct use of connected devices/products • Intelligent building concepts will lead to an overall increase in the of use energy • Manufacturers are not able to introduce new products and services based on interconnectivity
which leads to the name: **INTEROPERABLE SYSTEMS**	*which leads to the name:* **CONNECTED SYSTEMS**

The "big-flip" of the Interconnectivity cluster we have well developed frameworks for interconnecting and interoperable systems, components and devices. Not only is the technical foundation for interoperability present (standards, open drivers, network applications, etc.) but also the market demand and the business framework. This version of the cluster facilitates scenarios with *interoperable systems* featuring systems that work together to achieve a common goal and produce more value added services.

In the "big-flop" situation the technological advances do not support interoperability in the same sense. Focus is here on systems and components that are *connected to each other*, but are actually not operating together. Such scenarios are likely to involve a high degree of end-user participation.

3.9 Multiple images of how Building Automation systems are being developed in 2015

We are now able to define the structure of the scenarios for the Building Automation domain.

3.9.1 Developing the scene

In this process, we start with the scene, which is common for all scenarios. The elements for defining the scenes are found in the lower left "Scene" quadrant of the original grid of environmental factors. These factors are deemed to be rather certain by the experts and thus serve at the reference point for all four scenarios. The "Scene" factors are mostly related to end-user's attitudes to Building Automation in the future.

Smart home technologies are widespread and affordable to everyone. Most smart appliances have high value propositions and make the homes more attractive. With people moving frequently, there is a sound market for bundles of products and services. Preventative maintenance is one such service offered, which successfully is used to increase customer loyalty.

Since the large number of new devices increase energy consumption, local energy generating devices like solar cells and fuel cells connected to a local network have become increasingly popular.

Generally the manufacturers have a high influence on the way the products are installed and they are able to impose access control models and authentication schemes on end-users. In particular, all manufacturers have exclusive access to their own systems on the end-users' premises. Also various governments have introduced special anti-terrorist legislation which allows the government to access personal data information. Besides these cases, end-users are generally free to configure and manage the security issues themselves. Obviously, all systems have built-in firewalls for basic perimeter protection.

User interaction is performed using a wide variety of interfaces. Graphical interfaces are widespread, because traditional interfaces like keypads are too limited for serious interaction. Whereas all end-users will have and be able to use mobile phones, these terminals, as well as PDAs, are not regarded as suitable for all end-users.

3.9.2 Building the sets

The environmental factors in the lower right "Trend" quadrant constitute the changing sets that are built on the scene for each scenario. The experts have identified several trends. They do not necessarily form a cohesive, single targeted trend for the future. Rather, the trends point in different directions for different sorts of applications and different target groups. The trend corresponds to one of the four scenarios defined later (identified in [square brackets]).

One trend [1] concerns the increasing complexity of system integration, which puts a large pressure on developers, installers and system integrators. Since the complexity of networks increase rapidly with increasing number of devices there will be focus on using various interoperability standards. It must be possible for the manufacturers own system to interact and communicate with many different devices. Conversely, the system itself must be open to other systems.

Another trend [2] influences issues relating to facility management and the development of building and industrial automation infrastructures. Since end-users increasing will rely on a large number of services that are available in electronic form, e.g. service contracts and preventative measures, which can predict and thus prevent malfunctions of installations, they need their systems to have the capabilities to interact with users, with each other and with other manufacturers. A special challenge is that additional functionalities in appliances and device will lead to higher cost.

A third trend [3] points in direction of the emergence of highly integrated systems with extremely simple user interfaces. Target groups for such systems are the non-technical end-user requiring very complex functionality or assisted living support for elderly or chronically ill citizens. For this group of end-users, the systems must be easy and simple to use and system reliability is a particularly concern. The domestic environment must be trusted and secure. Devices and interfaces must also be designed according to ergonomic principles and will be equipped with graphical displays or

perhaps familiar touch pads, which most end-users can use. Wearable computing devices, e.g. for healthcare application, supporting mobility is an essential feature.

The last trend [4] points in the direction of increased demand for affordable, networked devices, from which the adventurous end-user expects a high degree of flexibility. These end-users expect to be able to build their functionality and thus require all systems to be flexible, adaptable, configurable, scalable and modifiable. Devices will be upgraded automatically and will have preventative measures installed to prevent misuse by end-user. User interaction will take place using multimodal interfaces and access rules to devices and applications will be commonly understood and accepted.

3.9.3 Defining the script

In the final step, the four scenarios come to life as imaginative plays defined by scripts. In writing the scripts, the environmental factors enter according to a simple grouping: What is happening, how is it happening and why is it happening?

What is happening?

The scene shows a typical developer user situation around 2015. The developer user is either employed in a manufacturing company that develops devices, products, embedded and networked systems or services, or he/she is working with system integration, either as a traditional system integrator, an engineering company or as a customer building in-house systems. The developer is faced with the task of creating new or improved embedded systems and applications, which is to be based on a high degree of networking capability of various devices.

Some of the people involved are definitively employees of the manufacturer, either in the developing departments or on-site, but also personnel from the system integrator may participate. The skills of the people involved vary between the scenarios.

How is it happening?

The developer user will constantly rely on visualisation and analysis of imaginative end-user behaviour. The target groups are, on one side, end-users that do not have interest, ability or skills to be concerned with the operation and interior functioning of the systems. They just want secure, reliable and functional environments. Another target group is the technically competent end-users, who have strong desire to work with the system and build new functionality and applications. The aims and needs of the target groups thus have different priority and the script differs correspondingly.

In some cases, the end-users have strong and clearly defined requirements thus requiring the developer user to fulfil a specific set of market requirements in an optimum way (market pull). In other cases, the end-user requirements are more vaguely defined in terms of technology content and functionality, thus leaving more room for the developer user in the design (technology push).

Why is it happening?

The main thrust for the developer users script are the commercial benefits to be derived from the under laying business case. Developer users must develop products and services that satisfy the needs and expectations of the customers. By using the Hydra middleware, the developer users are capable of developing secure, interoperable solutions with high degree of functionality and precisely targeted the end-user group in question.

Writing the scenarios

The four scenarios have been written on the basis of the scenario thinking process with the group of international experts in smart homes, Building Automation and embedded systems. The scenarios have been illustrated with pictures and drawings to stimulate the reader's imagination.

3.10 Writing up the scenarios

We are now going to define four scenario structures generated from the two clusters "Inter-connectivity" and "Universal Focus" each of which has two states or sub-plots. The possible combinations are as follows:

1. Developer-user centric + Connected Systems
2. Developer-user centric + Interoperable Systems
3. End-user centric + Interoperable Systems
4. End-user centric + Connected Systems

From these four combinations we can write-up four scenarios in the following way:

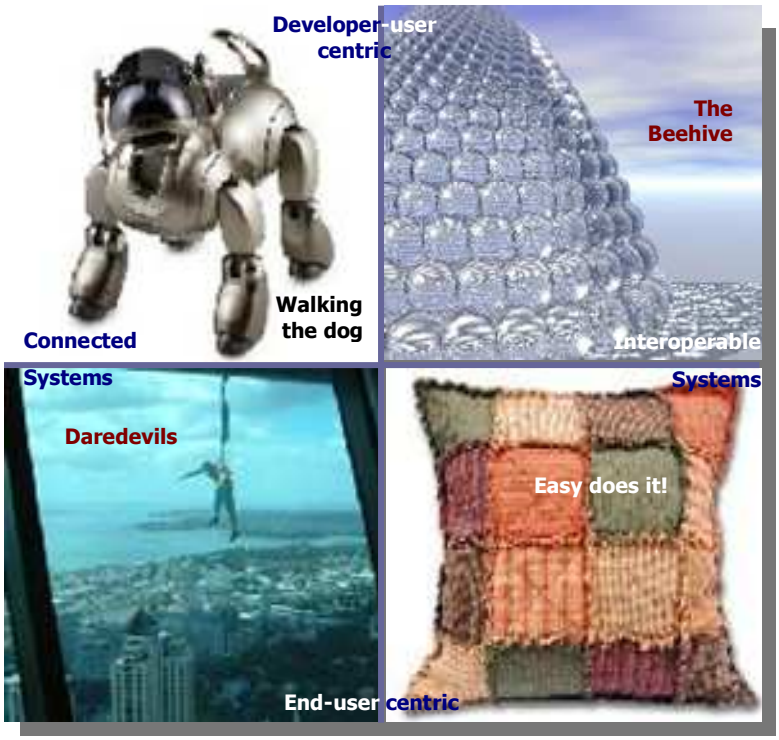
1. Walking the Dog

This scenario addresses the complexity of networks and the increasing number of devices to be networked, which poses a range of special problems for the developers. The scenario is set in public utility services, where a large number of proprietary commercial systems are deployed and controlled from a single control centre. The manufacturers must open parts of their systems for interconnectivity and at the same time maintain exclusive control over other parts in light of product liability, warranty issues, property rights and for the purpose of product differentiation.

2. The Beehive

The second scenario is dealing with the development of interoperable building and industrial infra-structures. In facility and plant management, the main focus is on automatic interoperability of various manufacturers' systems and configurability and accessibility by the management company's staff. Systems must be self configurable, fault tolerant and provide the functions needed for facility management, e.g. energy control, while at the same time supporting a trouble free transfer of responsibilities from facility owner to facility manager, including service level monitoring and accountability. The actors in this scenario are manufacturers and system integrators developing interoperable systems for facility management based on Hydra middleware.

3. Easy does it!



Highly interoperable systems capable of delivering intelligent ad-hoc applications relying on extremely simple user inter-faces is the theme for the third scenario. The end-users are technology illiterate, elderly and chronically ill citizens. The scenario is set in an integrated social institution where apartments for senior citizens are integrated with homes for assisted living and full scale nursing homes. Actors in this scenario are the employees of a system developer and a facility manager responsible for the maintenance of technical installations.

4. Daredevils

This scenario focuses on end-users, who want to have affordable, networked devices, from which they can set up integrated applications. The actors are the typical manufacturers of home control systems for private homes, e.g. alarm systems, heat control, media and information networks and similar systems. The challenge for the developer-user is to make the systems configurable and modifiable by the end-user, while still maintaining product integrity.

4. Building Automation scenarios

Walking the dog

4.1 Walking the dog

The increasing number of devices and the complexity of system integration put a great deal of pressure on developers, installers and system integrators to bring about open, secure and reliable solutions. It must be possible for the manufacturers own product to interact and communicate with many different products. Conversely, the product itself must be open to other products. Since the complexity of networks increase rapidly with increasing number of attached devices there will be focus on open interfacing standards, at the expense of true interoperability and dynamic development of intelligent applications.

Such applications are developed by manufacturers and system integrators, literally driving the application from one system to another through the network. We call this scenario "Walking the dog".

Forty per cent of The Netherlands' surface lies below main sea level. Since the late Middle Ages the Dutch have been making mud flats and sections of the ocean habitable by draining the water, but at a high cost. Countless people have lost homes and lives to the sea. Nearly everyone in the Netherlands knows that every square meter of soil came at a high cost, yet giving up is not an option.

It comes as no surprise that one of the most valued and prestigious institution in this country is the Rijkswaterstaat, the national organisation responsible for coastal monitoring in all sectors of the Netherlands. Working with and for RWS is highly attractive, but also extremely challenging.

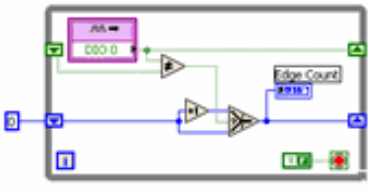
Jaap Van Beyl knows this. Jaap is a software engineer working for Redenbeek b.v. a leading international supplier of speciality pumps and water treatment equipment. Jaap got a degree in software engineering at the TU Delft and for the first six years of his career, he developed embedded systems for a company making heating and cooling equipment.

One of Redenbeek's biggest customers is RWS. Redenbeek has more than 9.800 submersible pumps deployed in the Delta Works in the province of Zeeland and participates in several projects on water protection and warning systems together with other manufacturers and institutes under the RWS.

Four years ago, Jaap was offered a newly created position as technology manager of Redenbeek. His responsibility would be to head the technology department and act as external scout and gatekeeper for new, emerging technologies, which could impact Redenbeek's product programme and market. Jaap gladly accepted this challenging position.

The pumps have over the years become increasingly intelligent. Embedded systems are used to reduce energy costs and increase the product life time by optimising operating conditions to actual load. Other systems are logging operating data and handles error conditions. Even before Jaap joined Redenbeek, several product lines had been equipped with various kinds of remote interfaces. Due to increased demands from customers like RWS, Redenbeek is now considering how additional, intelligent functionalities can be made remotely available for external services, customers and other manufactures, without compromising the core product.

Lately, a new middleware tool has been attracting a great amount of attention from the community. The Hydra middleware, as it is called, will allow Redenbeek to communicate with other systems in an open, intelligent and secure way and allow customers and other manufacturers to fully access and utilise the Redenbeek core functionalities using new and emerging interface standards.



Jaap has proposed to management, that his group should undertake a pilot project together with the RWS with the aim of

investigating how the Hydra middleware can be used to enhance their products. Since he graduated, Jaap has been a dedicated user of NI LabVIEW and last year he was named chair of the Dutch LabVIEW User Group. Logically, Jaap now wants to use the Hydra SDK module for LabVIEW to develop the Hydra middleware.

One project that Jaap has in mind is the "Hoogwaterinformatie Systeem" (HIS), High Tide Information and Early Warning System. In this project, RWS and their partners are developing an advanced system for early warning and prepared readiness for high tides. The HIS system interfaces with a large number of local and national measuring systems, widespread sensor networks, low altitude aerial and satellite based meteorological and oceanographic surveillance systems as well as several large-scale computer modelling systems. Applications are being developed that automatically collects data and information from these systems, cross-correlate the information using models and historic data and performs real time predictions of tide levels in each sector under RWS authority. Further, the HIS information will be used to investigate actual de-watering conditions in the affected areas in light of the predicted needs and to eventually fuse data for automatic operational control of unmanned sluices and water levels in dams and polders. The challenge here is to develop applications that can interface in real time with networked, heterogeneous systems, to make them fault tolerant, even under extreme conditions, and to provide the necessary security for the systems to avoid terrorist and similar malign attacks on a life saving infrastructure of national importance.

The RWS has posed a series of requirements on the Redenbeek pumping systems. The HIS application requires first of all that external applications will know and be allowed to read data from the pumps and pumping systems. The external requestor must present the necessary credentials before obtaining the information and there must be a trust model for how these credentials are evoked and maintained. Secondly, the flow rate must be remotely adjustable, which requires careful monitoring to protect the pump from physical damage. To minimize overload and the so called downthrust problem (due to lack of sufficient cooling flow), the pump must be run within its specified maximum and minimum flow range, which is a function of the actual head (groundwater height) and temperature. External applications should be closely monitored as to how the pump is affected by the imposed controls.

Jaap is also conceptualising a comprehensive logging and authorisation systems. His idea is that every external service must not only be authorised to access the pump, but he will also log every access for tractability and accountability. Redenbeek management thinks that remote access and controllability of their products carries a value in itself, which should be compensated by the beneficiary owner and have requested that Jaap considers these aspects also in his product design.

Finally, Jaap has to consider how he shields off the core of the embedded control system from external services, while still allowing his own organisation (including independent service organisations) to enter these sacred parts. Another issue is that the embedded applications are becoming so large, that the developers have serious problems with computing power and especially the burden of constrained memory space. To overcome this, Jaap is considering distributing the applications across the pump network and automatically performing system optimisation using the GRID network support in Hydra. There is also a need for automatic discovery and configuration of new pumps being deployed by the local RWS sector authorities, so that they instantaneously enters the HIS warning network. Jaap is thinking of using web services frameworks and in particular, the standardised description languages available.

The LabVIEW Hydra SDK module has been installed and they are currently building the security platform, which shall form the core of the pilot project. The management of Redenbeek gives the project top priority because they see this as a great opportunity to develop new business models, in which Redenbeek can deliver e-Business services directly to new customers. Jaap is definitively looking forward to very interesting and challenging development tasks in the coming year.

4.2 The Beehive

Development of interoperable building and industrial infrastructures impose serious challenges to the participating manufacturers' products. The products must provide all the functions needed for automatic, interoperable performance like self- properties, fault tolerance, trust and security frameworks, ambient intelligence, etc. and at the same time offer ease of use and support trouble free transfer of responsibilities from one end-user to another, including accountability and activity monitoring.*

Such system will need to have build-in capabilities to monitor and proactively manage the application, to learn from previous situations and be able to interoperate a large amount of devices, networks and embedded functions in a secure and standardised way. We call this scenario "The Beehive".

NCC is one of the largest building companies in Denmark. They operate globally, but have large contracts with the Danish government for building housing projects. One such project is the "Krøyers Plads" housing complex in centre of Copenhagen. This project consists of 5 apartment blocks with at total of 120 apartments. In addition, the project contains a medium sized shopping mall with a fitness complex and two social service centres e.g. a kindergarten and an activity centre for the old people. The project was designed by the Dutch architect Erik Van Egeraat and is renowned for its highly unusual architecture. The first apartments were ready in late 2014 and the rest are being finished in the coming few months.

The management of the housing complex is in the hands of ISS, Europe's largest facility management company. ISS manages buildings and facilities all over the world. The technical control centre in "Krøyers Plads" was originally planned as a central facility located in one of the blocks from where, a team of six caretakers could monitor all the technical installations. With the emergence of many new control systems based on Hydra middleware, it is foreseen that most systems will be able to work together and perform intelligent, interoperable tasks so that no human intervention is required. Consequently, the central control centre has been abandoned and the rooms transformed into a community day care centre.

Being responsible for the technical and building maintenance, ISS will undertake to specify the advanced monitoring systems for control and maintenance of technical installations such as electrical distribution, heating and cooling systems, water supply and wastewater. The actual applications for controlling the building and the installations will be designed by TAC Danmark, a market leader in system integration and Building Automation. As facility manager, ISS has clearly stated that they are not interested in how the system works, as long as it lives up to the requirements specification. This is a proven business model, which both ISS and TAC are comfortable with.

Klaus Jensen is the lead engineer in TAC's system integration unit and responsible for the "Krøyers Plads" project and is a very experienced in all aspects of system integration. Today, system integration is mostly performed through dedicated TAC networking applications that connect various subsystems through a central control platform. With the emergence of the Hydra middleware and a common, open interface standard, Klaus expects to be able to develop effective applications operating directly on the network itself, utilising the interoperability of the connected systems. Last year the International Device Interoperability Verification (IDIC) body was inaugurated, so in the future, Klaus and his colleagues will probably only use systems and devices certified by IDIC.

TAC applications must have extensive provisions for all sorts of services, such as meter reading, so that the consumption of electricity, water and heating can be remotely read from each apartment and automatically transferred to the administrative system. TAC applications need further to be capable of learning from the individual user's behaviour and to create suitable user profiles for monitoring of adverse consumption patterns, which may indicate faulty installations. This kind of embedded intelligence is one of the reasons that Klaus has selected the Hydra middleware, because he sees great potential in letting the large constituency of manufacturers develop a wide range of useful and interoperable solutions, and letting TAC develop only the customer oriented application.

TAC applications should also have extensive end-user features allowing residents to remotely access and control things, when away from their homes e.g.: in-house lighting, burglar alarms, camera surveillance, booking of laundry room, control of heating, supervision of windows, doors, stove, etc.

A major concern here is how the user will be authenticated, which credentials to use and how the trust model should be developed.

The newest service to be requested by ISS is a vendor access system that requires all authorised vendors, subcontractors and service organisation to access the building management system through a new authentication procedure. The purpose of this is to have a better security in the maintenance process, including the integrity of logged data, e.g. water temperature, which is required by law. There has been an example of data being lost during service, which is not very welcomed by the Danish Building Inspections Bureau. ISS also wants to use the system to check accuracy of the service costs they are being billed under the current service contract.

John Hansen is a senior service technician with Siemens Denmark, the main vendor of the electrical power automation and climate control installations. Since ISS is not prepared to accept responsibility for the correct use of interconnected devices and products, John has a full time job looking after the service contract that Siemens has entered into with ISS. When John starts his day, all service and maintenance jobs are automatically distributed on available service technicians and downloaded to their mobile devices in their cars. All the building systems automatically locates the manufacturers central maintenance systems and reports faults and corrective actions taken, so John can immediately get updated information from the Siemens system.

Today John needs to perform maintenance on the "Krøyers Plads" heating system. When John arrives at the apartment building, he is automatically recognised and cleared by the security clearance system to enter and move around freely in the building complex. The standard TAC system comes with access control based on identity card authorisation, but ISS have chosen to utilise a more intelligent system based on a distributed security model and individualised authentication provided by a mix of trust entities and third party authorisation. Although the basic trust model is an integral part of the TAC system, the choice of security model can be completely independent.

All systems in the building interoperate, not only in respect of access control, but it also to provide John with a specific personalised environment in terms of access to equipment and data sources.

John has now received all data on his mobile web tablet about history and service records for the heating system. From Siemens' own database, he has also downloaded the product information and tutorials he needs, so he can go directly ahead and perform the maintenance. Every device is available to him and he has the possibility to perform different kinds of tests, check the current status and to upgrade software components, if needed.

As he goes through the procedures, one heat exchanger does not perform as he expects it to. He can see in his service record that the Siemens support centre in Germany remotely updated the software 2 weeks ago, so he assumes that there might have been some problem with the operating conditions of this device. Instead of trying a range of different approaches, he decides to buy technical support directly from the Siemens support centre in Germany. The support is ordered and within 3 minutes, a service support person from Siemens is online with John and the device.

After the successful completion of his work, John checks his web tablet again and heads off for another job. He finds life much easier now, because the intensive decision support provided by all the systems gives him time to think through the really important and critical elements in his job. He finds this very un-stressing.

4.3 Easy does it!

Highly interoperable, self configurable, fault tolerant and secure embedded systems capable relying on extremely simple user interfaces is the need for non-technical target groups such as elderly or chronically ill citizens.

Developers need to build self-configuring systems that automatically can take part in and deliver ambient intelligence applications with semantic and leaning

capabilities. Mobility is an essential design feature and trust, security and reliability are of particularly concern. The systems must be extremely easy to use and special requirements are put on design of terminals and their interfaces.

Such requirements force developers to think strictly user centric. We call this scenario "Easy does it!"

"Park View Homes" is a large building complex located 50 miles north of London. It comprises individual apartments and semi-detached houses for elderly or people with long-term conditions needing assisted living as well as a full scale nursing home. The individual apartments are designed for the residents to live as independently as possible while at the same time having assistance near at hand if necessary. The entire building is fitted with a large number of embedded systems which supports both residents and healthcare and social workers in their daily work. Each apartment or house can have any number of devices helping to care for the individual residents' needs and desires. Healthcare applications are automatically created or launched according to needs and are fully interoperable with the residents' networked devices, the building infrastructure, the healthcare staff's monitoring and administrative systems as well as the county's healthcare provisioning and guidance systems.

Mr. and Mrs. Klein are both in their early 70's. They have lived in Park View Homes for 2 years now. Mr. Klein was diagnosed with diabetes II nearly 15 years ago but it is only recently that he has learnt to control his condition properly thanks to new self management programs. However, because of inefficient control in the past, there have been several incidents where his blood glucose level was too high sending him into hypoglycaemic shock. He has also had serious problems with his feet and now requires frequent treatment from the podiatrist. Mrs. Klein suffered a heart attack 3 years ago. This is what really motivated them to move into the Park View Homes. They didn't feel safe in their own home and wanted the comfort and security offered by the assisted living environment in Park View Homes, which in many ways resembles the way, every other UK citizen is living.

One of the things they like is the totally non-technical appearance of Park View Homes their apartment and in community buildings. Even though there are – so they are told – all sorts of monitoring and support systems in operation, they really don't notice them. No computer widgets are seen around; no technical gadgets are disturbing their eyes in their neatly furnished apartment. There is nothing to remind them of hospitals and other sad reflections. But when they need assistance, it is always there.

Last week, Mr. Klein woke up in the middle of the night and felt ill. Having eaten a little too much the night before, the diabetes monitoring system told him to increase his evening Metformin dose, but he forgot and now he needs help. The Park View Home has offered all residents a new cognitive alarm system based on semantic speech analysis that automatically interprets dynamic situations, caters for natural and artificial changes in the environment and adapts to different topologies, to different infrastructure and types of sensors. The manufacturer thus claims that the system is able to find and automatically interface to telephones, hearing aids, or any other device containing a microphone within reach of its network and use it to pick-up speech. If the end-user has agreed, the system is able to semantically process the captured sound, detect signs of stress and in some cases extract the specific circumstances of an emergency situation. Necessary information is then fused to appropriate support systems identified and configured on an ad-hoc basis.

Despite all the ubiquitous technology, the Klein's are particularly happy about having a dedicated nurse, Mrs. Rickert, assigned to them even if they are not living in the nursing home section. When Mrs. Rickert is off duty or unavailable, there are three other healthcare workers assigned to Mr. and Mrs. Klein as backup. There is a systemised prioritising scheme in place which automatically calls on the next nurse in line depending on the actual situation and the skills and location of the staff. As soon as a support nurse has been located, the Klein's are automatically informed who will be coming and approximately when. If there are audio channels available (e.g. a radio, a hearing aid, etc.) the message is given in natural language. If visual communication is available, the system formats the message for the appropriate terminal (e.g. a TV, a clock-radio, etc.).

Because of her heart problem, Mrs. Klein carries a wearable heart monitor device with wireless communication from which she can call for assistance 24 hours a day. The device she wears is able to pick up changes and thus send out warnings before anything actually happens. But if she wants to, she can increase the urgency by pressing a simple key pad on the device.

For diabetes patients, control of their blood pressure is extremely important, since high blood pressure can cause kidney failure. The Park View has bought a cognitive monitoring system that automatically detects and connects to available BP monitors on the Park View Homes compound. The system records and monitors the progress of consented patients according to the thresholds and limits set up by the health care professional. When a new device is located, the owner is asked to identify himself. The manufacturer of this system has provided the possibility for different trust models, according to the patient's preferences. If the patient agrees, the data can be stored in the relevant Electronic Patient Record and a healthcare professional can attach an individual monitoring scheme to the person reporting significant deviations from the clinical pathway.

Mr. Klein also uses a mobile device, with which he monitors his blood glucose levels 4 times a day. If his glucose level increases and stays above a trigger point, the wireless device searches the surroundings for communication access points, but means of which it can communicate the stored measurements and detected abnormalities to the relevant health professionals. Wherever he may be, Mr. Klein's device thus automatically identifies and securely sends the request to the Park View Homes diabetes care centre, where Mr. Klein's daily insulin intake is also registered. If the system indicates hyperglycaemia, a message is returned to an available devise in the vicinity of Mr. Klein requesting him to check today's insulin intake and immediately administer the needed dose.

At home, Mr. Klein's keeps his insulin pens either in the fridge in a special box with wireless connectivity. The box records every time the insulin pen is removed. If he does it within 10 minutes of the glucose alarm, no further action is taken. If not, a second alarm is triggered on the wearable device to remind him. The alarm system will now alert the nurse on duty, as well as Mrs. Klein, with information that he has not responded to the hypoglycaemia alarm. The insulin box is powered by a small battery and the manufacturer has had to make very special provisions to overcome the power constrains. The box thus searches for a suitable proxy, which can provide both communication and computing support. At home, Mr. Klein's set top box for his TV is often used for this purpose, but when he is out, the box sometimes finds an un-trusted host, such as a cash register in a restaurant or, if necessary, a mobile phone. The alarm and communication application provided by the manufacturer automatically adjusts itself to the available resources.

4.4 Daredevils

With the increasing number of affordable, networking devices on the market, many end-users can and will set up interoperable applications in e.g. homes, in order to realise the dream of "smart homes". Developers have to provide solutions to end-user issues such as user interaction, configurability, prevention of faulty usage, data protection, privacy and security, and access to devices and applications.

This poses a real challenge for developers, who want to make their products or embedded systems connected and programmable by the user, and still put a reliable and secure product on the market. The manufacturers, who want to satisfy this growing market of do-it-yourself enthusiasts, will need a flexible, fault tolerant and reliable, secure and trustworthy middleware. We call this scenario "Daredevils"

Wolfgang lives with his girlfriend in the outskirts of Hamburg. He is a computer specialist and loves to try out every conceivable new gadget on the market. If it appears in PCWorld, Wolfgang is sure to get it within weeks! His girlfriend Marlene is less enthusiastic due to possible intrusion on their privacy, but she supports Wolfgang, because she sees that some of the things he can do are actually quite sensible. However, Wolfgang has promised her, that she can put full trust in the system and that their privacy is not at risk. No one outside their home can interfere with their private lives. Above all, Marlene accepts it because it seems to please her cat Robinson that Wolfgang has installed an automatic cat feeding device.

When Wolfgang and Marlene return from work, they are looking forward to having a romantic dinner at home, because they both like to cook. Wolfgang opens the compartments of the delivery box. Excellent! The food service has delivered fresh vegetables, chicken and even the Chinese bean paste that Marlene ordered from her cell phone earlier today.

Wolfgang recently bought a new security systems for his home delivery box, which is outside their entrance but accessible from within. The manufacturer provides a full set of biometric security devices for the home delivery box and Wolfgang can select, which types offers the most appropriate level of security. His choice is either to use an ID card or a biometric device. To enhance security, any of these devices must used in combination with his newly acquired voice recognition system.

Using a secure Internet connection, Marlene checked their refrigerator earlier today and discovered that they were running low on several items. Although it does make life easier, Marlene is not too keen on this feature. She fears that someone from the government may sneak around and demand to see what they have in the fridge.

In the back yard, the automatic lawnmower is droning through its last few rounds. The robotic window cleaner has also finished up its chores. The manufacturers of these devices provide their own wireless drivers, but with open interfaces. Wolfgang has programmed his own control platform, using one PDA to control all of the devices. When he looks at the status, he notices that the lawnmower manufacturer has announced a firmware update that cuts the energy consumption by 12%. The upgrade, which costs 18 €, is offered for immediate download. A great offer which Wolfgang gladly accepts since his electricity bill continues to rise with all the new gadgets. Wolfgang has chosen to always trust offers from this manufacturer, because they have good products, excellent support and extended warranty. He uses his national digital signature to sign the purchase.

In the kitchen, Wolfgang again uses voice input to access his electronic cookbook and calls up the Chinese recipe that Marlene says she loves so much. The publisher of the cook book offers a web services with recipes and on-line delivery to appliances that are capable of handling such information. Wolfgang mixes the ingredients, relying on the automatic system in his stove to cook everything, while he heads for the bathroom to freshen up.

Wolfgang is particularly happy about his kitchen. The appliance manufacturer has recently introduced the new range of household goods, all with network access and value-added services.

The different functionalities are fully transparent and Wolfgang is considering having the kitchen system automatically record which ingredients he uses, record the weight on the integrated kitchen scale and learn how he cooks them, so that he gradually could build a knowledge base of personalised cooking habits to augment the online cooking book. Although he gets inspiration from the on-line cooking books, he prefers to be in control of the process when it comes to cooking.

Not so when it comes to security. He is very concerned about Marlene being home alone, which happens quite often, when he goes to the company's headquarters in Munich. Wolfgang has programmed fancy alarms, using the electrical smart home systems and various devices he picked up in the local hardware store. One alarm turns on two lamps upstairs and a CD recorder plays sound bits of a barking dog (Robinson doesn't like this at all), when someone moves around the house after Marlene has gone to bed. Lately, several break-ins in the neighbourhood had worried Marlene slightly, so Wolfgang gave her an outside door camera for birthday. Now the camera takes pictures of everyone ringing on the front door when they are not in. The pictures are stored on the house server and later, they can see everyone, who called at their house. Only one week ago, one of their friends had been burglarised during daytime. The police had told them that had they installed a camera system, they most likely would have apprehended the burglar the same day.

After having started the cooking cycle, Wolfgang heads to the bathroom to refresh. On the way, he tosses his clothes into the washing machine, which determines the ideal cycle from the RFID's in the clothes. In the bathroom, Wolfgang is regularly informed, in natural language via the build-in speaker system, of the cooking progress in the kitchen and what he needs to do next and when, in order to prepare a perfectly timed Chinese meal.

Wolfgang starts to think of the project he just finished; a green house for Marlene. She loves roses and Wolfgang has built a green house for her in the back yard. He installed a sprinkler system by connecting thin water tubes to all the flowerbeds from three large rainwater reservoirs. Each reservoir is equipped with a controllable pump, so that the water can be turned on and off automatically. One manufacturer has delivered humidity sensors for the flowerbeds, temperature sensors, and a sunlight sensor outside the house. The manufacturer has developed a large program of self-configurable sensors with wireless connection. They are so inexpensive that he just spreads them in the flowerbeds. If one sensor is failing, another will take over. Another manufacturer provides electrical systems for controlling the windows and shades. For optimum operation, the system uses rules based decision support and relies on external sensors for micro-weather monitoring to handle unstructured and conflicting data. For example, the temperature sensors may require outdoor shades to open, but the wind sensors require them to be closed. Marlene's roses can now be kept in optimum conditions.

After bathing and dressing, Wolfgang looks and feels very sharp. He heads over to the living room to set the table. As he sits down to enjoy the music and await Marlene's home coming, he reflects on all the things he has been able to achieve with very little efforts. He is very happy about it and is determined to take the entire system with him if and when they move to a new house.

5. Appendix A: Environmental factors in Building Automation

The following list is provided as a guide to the meaning of the various environmental factors identified and discussed by the expert during the Building Automation workshop.

In the first column is listed the questions being discussed during the workshop and noted by the consortium partners. In the second column is provided a brief explanation of the content of the relevant discussions. In the last column is listed the corresponding short factor description used in the scenario discussion in this document. The identified factors have been listed according to the classification provided by the experts: High uncertainty vs. high certainty and direct impact vs. indirect impact.

Topic, statement or question	Explanation and comments	Environmental factor
High uncertain – indirect impact		
Security responsibility defined and assigned	The responsibility for system security is clearly defined and assigned to specific actors.	Clearly defined security responsibilities
Complexity requires structured access to information	The complexity of networked system requires a logical/structured access to the devices and information sources in the network.	Structured access required
Application programming	Will end-users be required or allowed to perform programming of applications?	End-user programming
Changing in thinking about systems	A systemic approach will prevail for concepts of systems, including logical and ad-hoc connected components.	Systemic concepts
Just one interface	All devices share one common interface.	One common interface
Customers will produce power themselves (solar)	The systems will be extendable with energy producing devices like solar panels.	Energy costs neutrality
Can information overflow be avoided?	Methods exists to avoid information overflow	Information overflow avoided
High uncertain – direct impact – technology push		
Costs of making devices compatible	The additional costs for producers in order to make their devices interoperable are low.	Interoperability costs
Warranty period decrease	The warranty period for products and services will decrease in the future	Warranty period
Warranty issues are purely political	The warranty coverage for interconnected products is a regulatory issue and as such not related to the product or service in question.	Warranty coverage
Human body as connectivity device	New technologies introduced for interconnecting devices	New connectivity methods
PDA's available to most/all	All end-users will have and be able to use PDA's	PDAs available to all
Which standards and programming language	Which standards will be introduced and dominating? Which programming languages will be introduced and dominating?	Technical standards Programming languages
Certification of drivers and applications	Device drivers, interfaces and applications will need a third party certification to be acceptable for interoperable systems.	Certification
Third party authorization	Authorization will be handled by third party authorization bodies	Third party authorization
Proper functioning in operating environment	Systems will function properly in their operating environments	Proper functioning
Customer pays to use devices-does not own it	The manufacturers will introduce new business models	Business models
Security system –centralized or decentralized	The security model generally be centralised across the network.	Centralized security
Will there be a killer application?	The manufacturers will introduce new products and services which have sound value propositions.	Business value creation
End-user accepts responsibility for correct use	There is a common understanding that the end-user is responsible for using the devices/products correctly according the defined guidelines and instructions	End-user acting responsibly
High uncertain – direct impact – market pull		
Can we agree with manufacturers on trust models?	The manufacturers will be able to impose trusts models based on e.g. their reputation and market visibility.	Trust models
More energy is needed to run smart homes	Smart homes will provide more efficient use of energy resources compared to traditional homes.	Energy efficiency
Efforts to save energy are widespread	End-users will focus on systems to save energy	Energy savings

Topic, statement or question	Explanation and comments	Environmental factor
Biometric devices needs freedom of choice	End-users want to have freedom to select the most suited biometric device	Choice of biometrics
Users attitude to configure own system	End-users want to be able to configure their system	End-user configurability
Customer trust in application manufacturer	Manufacturers' reputation will dominate the end-users' trust model.	Reputation of manufacturers
Self learning must be build into system	The systems will have provisions for self-learning	Self-learning capabilities
Houses, hotels used as personalised computer platforms	Houses, hotel rooms etc. are able to adjust to each individual's computing and ambience preferences automatically.	Transferable personalised settings
Consumers wants full transparency	The end-users want to have full insight into the functionality provided by the system	Transparency
Do we need user interfaces?	System intelligence will assume responsibility for large parts of the system's actions.	Intelligence used proactively
Added value must be clear if smart homes is to appeal to customers	The value propositions in smart home systems are generally clear and accepted by the end-user.	Accepted value propositions
Customer confidence	End-users are confident that products work properly	End-user confidence
You can talk to systems	The systems will be based on speech recognition and natural language interfaces	Speech control
Systems can be moved to new home	The system follows the end-user when moving to new premises or homes	Transferability of systems
Laws to protect customers	There are strong laws and regulations to protect consumer interests	Consumer protections
Laws to prevent misuse of data	There are strong laws and regulations to protect private data	Data protection
Procedures for approving updates must be in place	Automatic updating requires approval from end-users and procedures for this are build into the system	Automatic updates
High certainty – direct impact		
Government force public to use ICT	Increasing number of public services will only be available in electronic form	eInclusion
Wearable computers	Wearable computers will be widely available	Wearable computers
Need of flexibility	All systems must be flexible, adaptable, configurable, scalable and modifiable	Flexibility
System reliability	System reliability is crucial	System reliability
Additional functionalities mean additional costs	Additional functionalities in appliances and device will lead to higher cost to purchase and use.	Increased costs for new functions
Trouble-free interaction between many different devices	It will be possible for many different devices to interact and communicate	Device interaction
Need to network (manage) hundreds of devices	The complexity of networks increase rapidly with increasing number of devices.	Network complexity
Need interoperability and standards	Increased demand for networked devices. Increased demand for interoperability standards.	Device networking required Interoperability standards
Simple touch pads	Devices and appliances will be equipped with simple touch pads	Simple touch pads
Easy to use systems	The systems must be easy and simple to use for the end-user	Simplicity
Malfunctions can be predicted	Preventative measures are in place which can predict and thus prevent malfunctions of devices	Predictability
Automatic upgrading	Devices will be upgraded automatically	Automatic upgrades
Manufacturer has remote access to product	Manufacturers will have remote access to any product anywhere, e.g. for maintenance service purposes	Remote access for manufacturers
Multimodal interfaces necessary	User interaction will increasingly take place using multimodal interfaces.	Multimodal interfaces
Devices able to handle abuse	Devices will have preventative measures installed so to prevent misuse by end-user	Prevention of misuse
Customer wants energy-saving products	End-users are demanding products that use less energy	Energy savings
Affordable devices	Devices will be affordable to all	Affordable devices
Graphical displays, especially for older people	Socially and physically disadvantaged end-users will require graphical displays on devices.	Graphical interfaces for the disadvantaged
Interacting systems	Systems will increasingly have capabilities to interact	Interacting systems
Ergonomic	Devices and interfaces must be designed according to ergonomic principles.	Ergonomics
Domestic environment provides a trusted a environment	The domestic environment is trusted and secure for the use of devices and applications.	Trusted domestic environments
Access rules established	Access rules to devices and applications will be commonly understood and accepted among end-users.	Agreed access rules

Topic, statement or question	Explanation and comments	Environmental factor
High certainty – indirect impact		
Access control/ authentication	The manufacturers will be able to impose access control models and authentication schemes on end-users.	Imposed access control
Access control system is open to manufacturers	Manufacturers have open access to their systems on end-users' premises	Open access for manufacturers
Smart home accessible for everyone	Smart home technologies are widespread and affordable to everyone	Smart home affordability
Firewalls in systems	All systems have built-in firewalls	Firewalls
Easy for consumers to configure and manage security	Consumers are able to configure and manage security issues themselves	Security configurability
Devices can live off ambient light in the room	Smart home devices will use new types of renewable energy sources thereby decreasing the need for traditional energy.	Renewable energy sources
High value appliances in homes to attract renters	Smart home appliances have high value propositions and therefore make the homes more attractive to tenants.	Attractiveness of homes
Governments will have a back-door access to data	There will be special legislation to allow the government to access personal data information.	Government access to personal data
Maintenance services contact the customer when needed	Preventative maintenance will be used to increase customer loyalty and create new services.	Preventative maintenance
Mobile phones are available to all	All end-users will have and be able to use mobile phones.	Mobile phones available to all
Using mobile phones and PDAs is not suitable for all of population	The use of mobile phones and PDAs is not suitable for all end-users or all needs.	Suitability of terminals
Constraints in keypads	Traditional user interfaces like keypads are too limited for serious interaction	Interface constraints
Products and services are bundled together	Manufacturers will offer both products and services in bundles	Bundling of services
People live only a short time in each home	People move house frequently	High moving rate