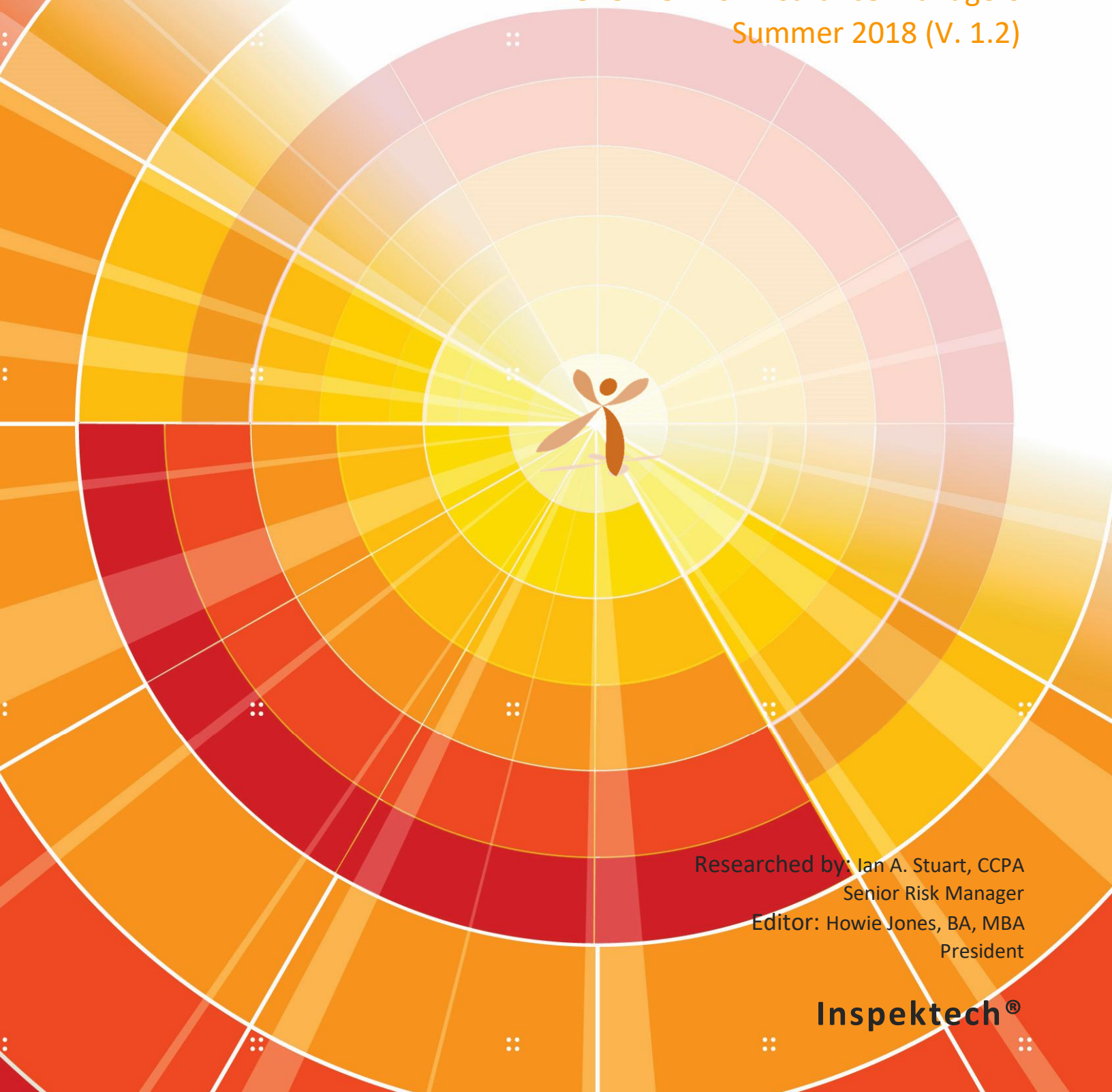
HOME AUTOMATION / SMART WIRED HOMES

InspekTech® White Paper
Overview for Insurance Managers
Summer 2018 (V. 1.2)



Researched by: Ian A. Stuart, CCPA
Senior Risk Manager
Editor: Howie Jones, BA, MBA
President

Inspektech®

The marriage of “electronic reliance” and “on-site risk verification” is both imperative, and the most fundamental combination of mitigating financial and other risk exposures, for the insurance provider ~ and ultimately the insured.

Why have a Home Automation/Smart Wired Home system? And what it means for insurance coverages of the future.

Overview

There are 5 main reasons why homeowners include home automation when having a new dwelling built or renovating (i.e. e to often referred to as 'Smart Wired Homes'), as follows:

1. Security and surveillance
2. Energy Savings
3. Cost Savings
4. Comfort and convenience through automation
5. Health monitoring and tracking

The market for home automation is growing very rapidly and hundreds of new products are coming to the market monthly.

The actual usage of these products is growing at a rapid pace as well. In 2014 it was estimated that, globally in 2009, there were 90 million home automation devices in daily use by households. By 2020, it is estimated this will grow to 26 Billion and, by 2030, to 142 Billion (Gartner Inc. a data/analytics research company). This means that "Smart" devices connected to the Internet of Things ("IOFT") will become the norm, not the exception.

What's a 'smart wired home'?

'Smart Wired Homes' is a term used to designate the incorporation of digital control in a home. This can mean control of just about everything – from lights and music to doorbells and the heating system. Even appliances can be a part of a smart home plan. In 2018, homeowners who are interested in smart homes, are typically starting with the basics: entertainment systems, lighting, some basic appliance notifications and then working outward from there.

What's an 'ecosystem'?

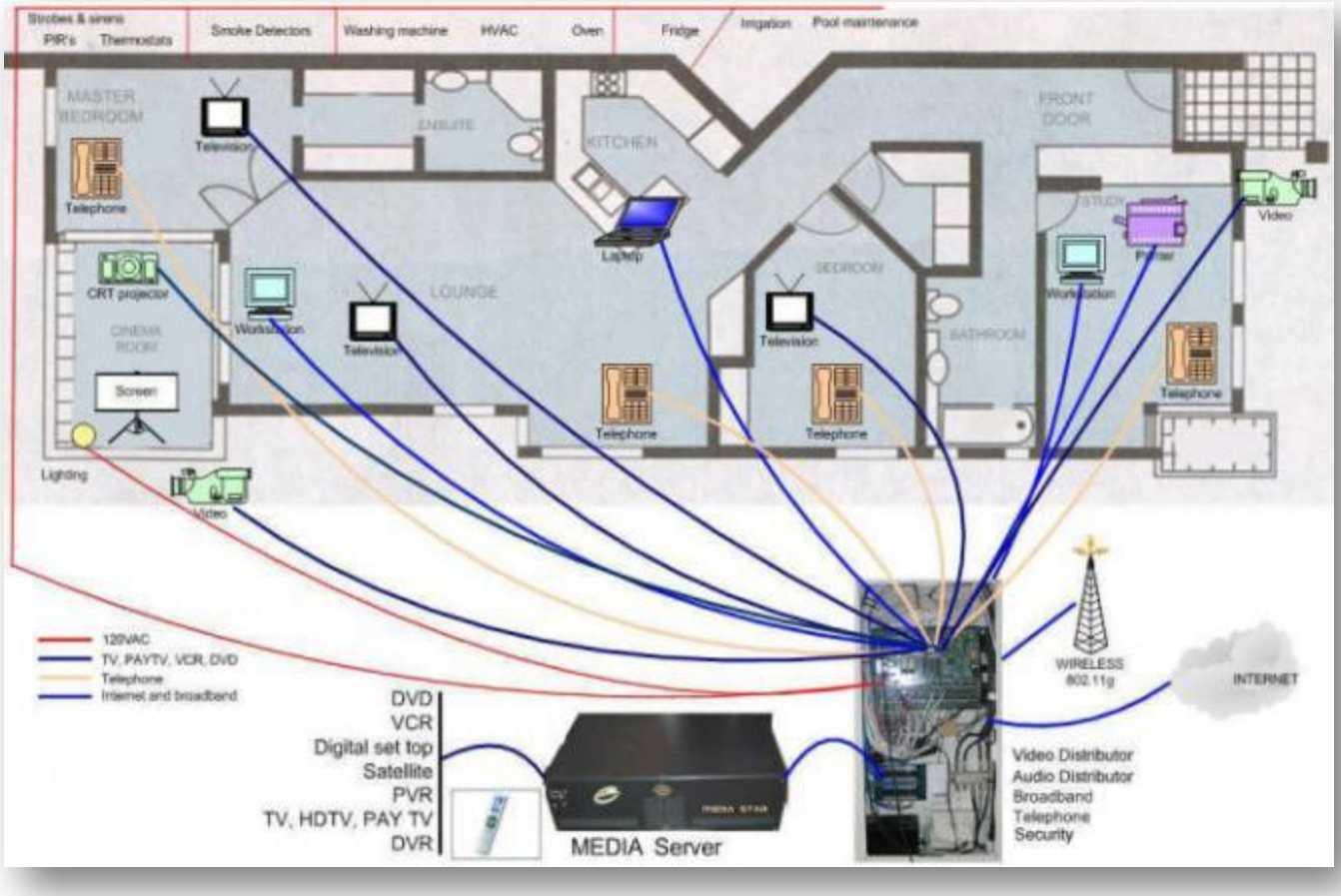
An ecosystem, as it relates to a Smart Home, is an interconnected system where every smart device works together in harmony (or is supposed to!). In a properly functioning ecosystem, devices can be added, or taken away, without a disruption of service.

Two Streams of Ecosystem Devices You Need to Know About

Within the ecosystem scope of smart home devices there are 2 main streams, as follows:

1) **Hard-Wired Centralized Hub:** A number of cutting edge tech companies have their own version of smart home implementation by way of providing a central Hub (or 'access point') through which all facets of a home can connect.

In the case of high value home systems, these are now often hard-wired into the home via a centralized Hub. In the Centralized Hub method, all the connected devices report back to the "Hub" and receive instruction from the Hub. If the home is a hard-wired smart home (HWSH), a structured plan is now typically needed to account for the telephone, TV, music, security and data and some HWSH's may take the form of a rack that houses network and cable termination, network modems, switches, routers and audio/video equipment (often located in the electrical room or wiring closet).



2) **Non-Wired De-Centralized IFTTT (If This Then That) via a plugged-in Centralized HUB:** If this header description sounds a little confusing well, you're not alone! But with pause for thought, it's not so difficult to understand at all…

The second and growing category of Smart devices (i.e. in comparison to the hard-wired Centralized Hub method) is referred to as an IFTTT (If This, Than That) which is a **de-centralized method** of bring devices together (debuted in 2010). This is achieved by having all of the devices being able to "talk to one another" using a common language methodology.

IFTTT has pre-made "recipes" that are designed to connect your devices. IFTTT (a free App) regularly releases convenient recipes with popular services for common devices and apps (or, you can customize your own recipes). This means you can program your devices to run routines, react to triggers, or pass commands to other devices in your home (the main advantage being the speed of communications between devices). By way of illustration, imagine a water sensor at the base of a hot water tank becoming wet which then signals (in less than 1 second) directly to powered shut off valves on the tank to close while, simultaneously, sending an alert to the devices chosen by the Insured to receive water escapement alerts – that's IFTTT in action.

Example | De-Centralized IFTTT via a Centralized Hub

There are a lot of smart home brands such as Nest, GE, Philips, Honeywell, etc., but they couldn't always connect, communicate, or work with each other. That's where a de-centralized IFTTT approach using a Centralized Hub (non-hard-wired in this case) such as *Wink* came in and which illustrates our IFTTT point well. Indeed, Wink acts as an IFTTT Hub that brings hundreds of product brands together so such smart systems can connect via a centralized plugged-in system.

By connecting with third-party smart home devices such as thermostats, door locks, ceiling fans, and Wi-Fi-enabled lights, Wink provides a single user interface on a mobile app (or via a wall-mounted screen called Relay). This allows the user to remotely control those devices. The mobile app is free, while consumers pay for a Wink Hub, or Wink Relay, which connects with smart devices in the home.


Home Sitter, Wink turns your lights on and off in a realistic pattern to make it look like you're home when you're away. Or, with Wink Moonlight, the device will sync to your local sunrise and sunset, turning your lights on and off accordingly. Other Wink services give you the power to know how much energy you're using (or, even better, saving).

Wink Lookout sends timely alerts about doors, windows, locks, garage doors, etc. Motion sensors can also be mounted around the dwelling for motion alerts which can in turn be used with the Wink Siren & Chime feature for an added layer of security. The system also allows you to get notified when your kids come home and enter the house, and allows for easy contact for a 'check in', etc.

The **Wink Leak Protection** Kit turns off your water automatically (or receive an alert to turn-off your water main) when appliances malfunction, the toilet leaks or a pump starts to overflow. The Water Main Shut-Off can even automate your water heater. Install it on your existing water main with just a screw driver. No cutting into pipes or calling a plumber.

Additionally, *Amazon's Echo* (called *Alexa*) and *Google's Home* and *Google Home Mini*, fit into this category which are referred to as being a PPi device (Purchase Plug-In). Such PPi devices are often limited in ability which, as can be imagined, are reflected in a lower price point for the consumer. One of main drawbacks to the PPi device type, is data security and hacking vulnerability.

As of 2018, generally during any new build today (and serious renovation) there are going to be some smart elements involved. And this can run the gamut from creating a structure that is super smart, to one that has decentralized recipes (via a centralized plugged in Hub perhaps) that lets you experience a little more convenience.

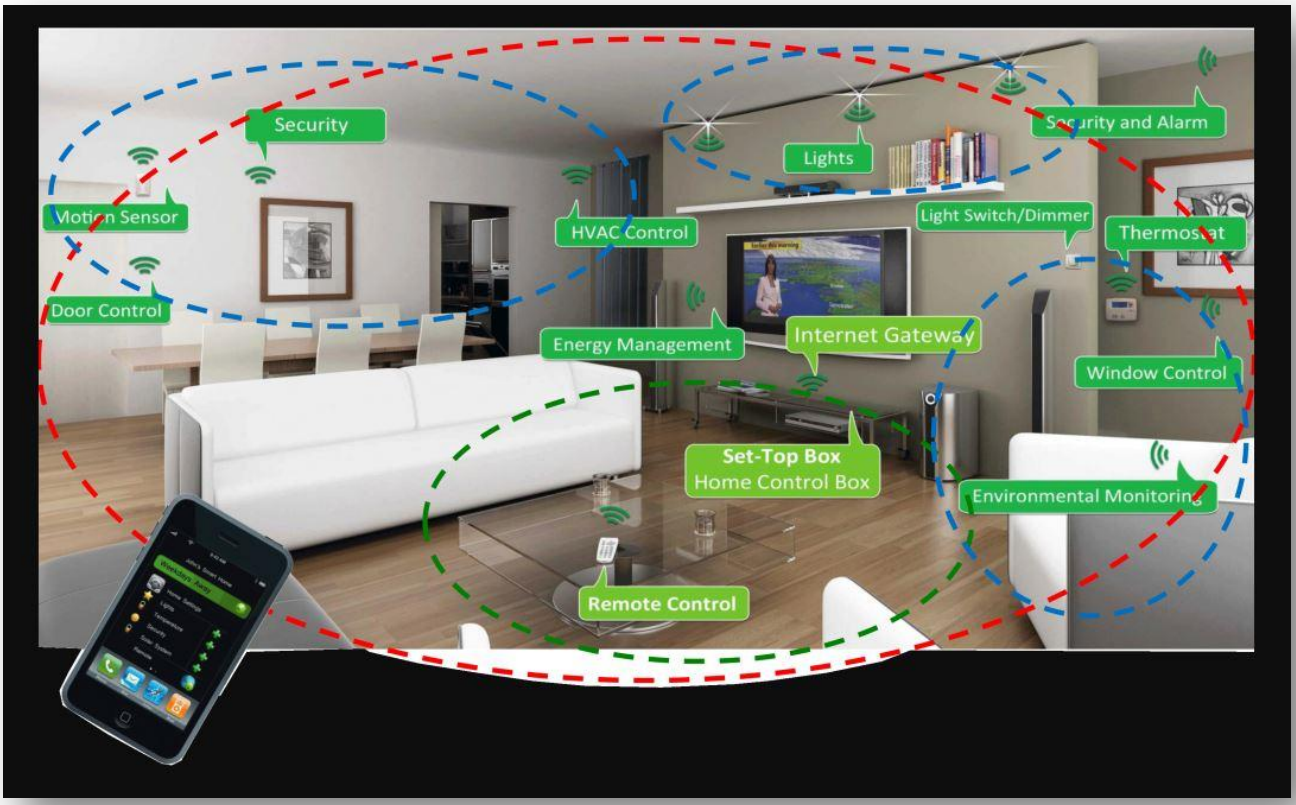
Both technology methods (i.e. Hard-Wired Centralized Hub vs. De-Centralized IFTTT which sometimes uses a centralized plug-in) are going forward rapidly, and it will be interesting to see which one becomes the dominant player!

CORROBORATION OF DATA + ON-SITE VERIFICATION = A WIN

One thing that all devices in a Smart wired home produce is data.

Aside from understanding the basics of Home Automation and Smart Wiring and their devices, some questions to determine risk in this area will be to determine such factors as: Do doors get locked and how do you know? Can the windows be closed remotely? Heating and Air Conditioning: Is it turned up/down effectively and reliably?

And, of course, one of the biggest challenges to Insurers will be to persuade customers to share data from their devices. When an insured does, this will enable Insurance providers to be in a better position to tailor insurance coverage – and reward insurers for good risk-management. Such an outcome will be a function of real world on-site corroboration of information, that vitally serves to verify conditions and lend support to the interpretation of data.

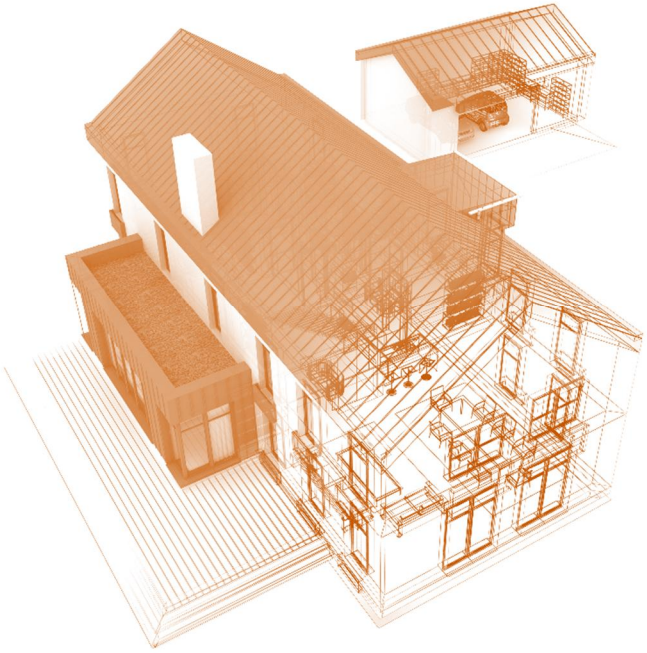


Main Reasons for a Smart Wired Home

1 Security and Surveillance

Security system procedures of various types have been in existence for thousands of years. Whether it was Roman sentries at the gates in the outer walls of city states or our "modern" system of door/window/Passive Infrared Sensor (PIR) connected to horns and lights, humans have sought out peace of mind through security in one form or another for a very long time.

In the "connected" home this ecosystem of security devices has and will continue to develop into a controllable sphere of coverage. Additionally, systems will provide data about their usage (or non-usage) on a continuous basis which, if the insured is willing, will be able to provide valuable information pertaining to the core nature of risk in the dwelling.



Here's what we mean:

- Connected door locks will allow for doors to be locked + unlocked remotely. When combined with occupancy sensors, the security system will now be able to send an alert to Insureds if doors are unlocked and the home not occupied for a given period of time. Not sure if the kids went outside to play? Basic and easily installed surveillance cameras placed around the exterior of the home will be able to pick up activity and facilitate the homeowner knowing if the kids are still in the yard. Already, this trend is well on its way: indeed, as the quality and functionality of cameras has become better, their use is changing from "nice to have" to the very cornerstone of the "connected security system". And there's more. Facial recognition software is now allowing for systems to become even more automatic by unlocking doors for recognized individuals upon arrival at the front door.
- Window sensors ensure that open windows (especially ground floor and basement) are known about and closed before leaving. The future will see windows having built-in motorized opening/closing – both for security and energy management.
- The next level of security are sensors for gas emissions (CO/Radon, etc.) and smoke and water. These "area sensors" are developing and becoming more tightly integrated into the overall security ecosystem. For example, rather than just making a loud noise, these types of sensors now speak and alert users to dangers. Additionally, some systems in high-end home automation can turn on lights at night in an emergency and verbally direct family members to the safest route out of the house while simultaneously calling fire and police services. And - the family's pets haven't been forgotten; they, too are able to be located for removal in emergencies, all functions of a level of security perhaps never dreamed possible.

- The security and surveillance system in some homes now, and many more in the future, provide a large amount of data about their use and the habits of Insureds and their families. For example: Does a family member go jogging routinely at night and leave the garage door open and are house doors unlocked and windows left open? If the data from the door/window sensors and camera is processed correctly, this pattern would be recognized, and suggestions made to correct it.

Ultimately insurance coverage will develop around real-time risk modeling.

Rewards, backed by supportable risk mitigation at the dwelling that warrant same, will need to be communicated to insureds; that is, what rewards might be provided to Insureds who take corrective action and practice good risk management by use of the available technology? And, at what point in the renewal or overall market message, will such rewards be introduced and emphasized?

Of course, for those messages to be conveyed – whether in formal marketing material or by way of "on the fly" conversations with customers – insurance providers will both need to:

(i) Understand how these systems work at a basic level as well as;
(ii) Be assured they're in place on-site and;
(iii) Are actually functioning as an "extra" level of risk management to the overall envelope of risk at the dwelling which, for that vital component to be realized, **the marriage of "electronic reliance" and "on-site risk verification" is both imperative, and the most fundamental combination of mitigating financial and other risk exposures, for the insurance provider ~ and ultimately the insured**.

2 Energy Savings

As one would imagine, home automation systems wonderfully allow for the efficient control of the interior environment in a dwelling. High value homes now often have their HVAC system designed with this type of automation control in mind. Additionally, renovated homes are also beginning to adopt this approach as well. Energy management is more than just a "connected thermostat" operated by a Smartphone. High end home automation controls include outside air/wind/humidity sensors, as well solar (sun) sensor/interior thermal and humidity sensors (part of good energy management is controlling solar heating with automated shutters/blind/solar films… these types of control devices are often only found in high end home automation systems at present.

Information is collected and utilized to best manage the heating and cooling of the building within the limits set by the home owner. Information collected from these sensor allow high end automation systems to create very complex environment profiles of the interior of houses on a room by room bases.

By obtaining information from motion sensor areas not occupied over a period of time, rooms can be allowed to heat and cool most effectly without compromsing a family members comfort. An example of this would be a basement media room which, during the week is never occupied in the daytime; thus, by widening the control parameters for this room during day and more tightly contolling them for the late afternoon/evening when the room may become occupied, can result in considerable energy savings.

3 Cost Savings

Cost savings through good energy management are achieved over time and, depending on the type of home heating and cooling systems and the form of fuel used, such savings can be considerable.

The next phase of home automation in HVAC control is already under way in Ontario.

Hydro One is outfitting houses with smart meters that tell your home automation system how and when to heat and cool – to save money based on current and immiedate future energy damands. This Smart grid to home energy management connection platform is in its infancy. Interestingly, several large utiltiy companies in the USA are working on developing larger scale models.

Cost savings management also include lighting systems the react to occupant location + use, by turning lights on ahead of usage and off after usage (i.e. based on time of day and other factors).

For example, with only one child at home in his room and his mother in the kitchen getting dinner ready, there's no need for lights to be on in the main hallway or bathroom unitl the motion sensor detects the child leaving his bedroom, heading down the hallway for the bathroom. When the child changes his mind and decides to see what's for dinner, cost management systems determine that lights in the bedroom and bathroom can be turned off and that the hallway lighting need only be on long enough for the child to reach the kitchen. After finding out what's for dinner the child returns to his bedroom, with the system turning on and off as required. This may seem, on first reflection, as a modest cost savings event; however, repeated thousands of times per day, across millions of households, the cost savings could be considerable.

A second example? Let's say the mother decides to start laundry while dinner finsihes cooking. The home automation system detects she has gone into the laundry room and advises her that cost savings in electrical usage will be achieved by simply waiting 30 minutes past peak demand times currently being expereinced in the area.

4 COMFORT AND CONVENIENCE THROUGH AUTOMATION

Often one of the primary reasons to automate a home is simple: comfort and convenience!

By way of illustration, the use of home audio and video systems are becoming very wide spread. To many users, this is the fun part of home automation – whether or not it's telling *Alexa* what song to play next or high end Smart wired home systems allowing a family member to move about the house while still watching the same sporting event on one of several imbedded video screen/audio systems throughout the home.

As a practical spin-out to this "comfort reason" are the media/theater rooms being designed and built with an ever-increasing degree of sophistication. The connected media/ theater room, for example, is fast becoming a standard inclusion in most high value homes. Insurance providers, as a matter of course, should be asking questions about or confirming on-site what type of equipment has been installed (i.e. permanent seating with built in sound and subwoofers, arm chair pocket drink coolers, heat and massage chair features, are all in common usage now and can obviously impact replacement cost). By way of cost implications, projection systems with multiple viewing options can cost between $45,000-$60,000 and, when connected to a high-end speaker system the overall cost of a relatively small media can reach $ 150,000 or more. These are all real costs that need to be accounted and factored when determining replacement cost.

One of the Hub components of most high-end home automation system is that of a media storage system. In many cases the system includes a secondary computer/server connected to high capacity high speed hard drives, that deliver multiple media streams/channels to locations around the house simultaneously. Insurance policies covering data lost will need to become more developed to that end.

While control of lighting system is often considered an energy management issue, it's also one of comfort. LED lighting will continue to advance and, for other than very specialized needs, the only type of lighting found in most homes by 2030. Being able to control the light in a room to set a "scene" is one the hallmarks of high-end smart wired homes (in soon to be forgotten days, this was achieved is early systems using pre-set programing, directed to a wall mounted controller switch. Now, it's typically activated by voice command or Smartphone app).

Additional "comforts" include Smart appliances and in the Smart wired home, such comforts will be treated as part of the structure; subsequently, insurance policies may need to be adapted to cover such structural variances.

5 HEALTH MONITORING AND TRACKING

The aging population demographic in North America, along with a continual desire to maintain and improve health outcomes, is driving a growing segment of the home automation marketplace, particularly in the "home wellness monitoring and tracking" segments of this niche.

Many people with aging parents or relatives are aware of the personal bracelet or pendent alert devices that allow a person to press a button and summon help if needed. The next generation is being automated and improved upon whereby home automation systems can monitor the breathing and position of a person wearing a device while predict if the user needs help of any kind or is likely to fall or induce some other risk upon themselves. In co-operation with various health care providers, systems are being developed that track personal wellness on a daily basis while providing auto-electronic suggestions to improve and correct "circumstances".

In the future insurance coverage is likely to move towards taking greater account of the daily risks being taken inside the home and by the insured, as being one of the many determining factors in pricing models. The extent of that "daily risk" movement seems at present to be a long way off in terms of wide spread acceptance and use (i.e. with privacy issues and other social factors yet to have even been debated let alone accepted). However, the point is this: the technology is there for the most part for a wider use net of health monitoring possibilities – how that will be used and the extent thereof is something insurance providers will be watching.

Summary

If a fire breaks out in a home today while no one is home, the best-case scenarios involves a lot of improbable things: (i) neighbours watching the house for signs of smoke or flame; (ii) the house having fire sprinklers and smoke and/or heat detectors in the right place to detect and extinguish the fire with minimal damage, etc. Without these conditions, in most cases, presuming the security alarm system has a smoke detector, an alert to a monitoring station and the fire department will result – hopefully in time to save some of the house and reduce Insurance exposure.

In all cases, such fires will cause damage and claim coverage will be involved. But this all potentially changes with the Smart wired home.

In the next generation of Smart wired homes, the use of interconnected sensors and devices will know you are not home, be able to identify the origin of the fire while still in its infancy, direct the fire sprinklers to activate in just that area for maximum effect, and alert the home owner and others immediately of the problem – all in the blink of eye.

Will there be damage? Yes. Will it be minimized to a degree not possible today? Absolutely, yes.

The use of home automation will continue to grow at a rapid pace with many of innovations being developed as the software controls mature and hardware sensor devices become more advanced and tailored to particular areas of need. With the increase use of home automation will be the collection of data that is very particular to the automated household and the Insured.

If managed properly and supported by corroborating on-site verifications of other risk and cost factors, smart related data will facilitate a move toward more refined policy management systems; that is, of rewarding good risks and aiding in the correction of bad risk behaviors.

Misc. Notes

- *High end automation systems by brand name in common usage today: Control4, Crestron, Elan, QSC systems, RTI, URControls, Savant.*
- *A word about hardware and connection methods. High end security systems are mostly wired as this method is most secure for critical sensors and allows them to be powered continuously. Where necessary, wireless devices use high-level security methods; however, this added level of interaction can at times effect their timing performance.*
- *Wireless devices and system (most common in "Do It Yourself"/DIY and low to mid quality systems), while very easy to setup, have poor security; indeed, almost every manufacturer of cameras and door locks report hacking of their devices. Additionally, such DIY type systems need to have batteries changed periodically. These issues represent perhaps the biggest hurdle to wide spread adoption; that is, gaining consumer trust and confidence is using the devices in their home.*
- *Solar power generation, on a small scale, is being worked on with home automation systems and are considered as being in the forefront of the control of such systems.*

Acknowledged Sources of Reference

1. AXA.com, *The Home (Insurance) of the Future*.
2. Swiss RE Institute, James Stansberry, *Latest Technology and Product offerings in Smart Homes.*
3. Control4 website and press releases.
4. Audio and Video Invasion website.
5. *Chowmain Software* and *Apps 9developers of Software* for home automation system.
6. Engeris Home Management website.
7. National Research Council Canada, *NRC capabilities in Smart infrastructure and Cities of the Future*.
8. IRMI - *Addressing Liability Risks for Data Loss from an Insurance and Contractual Risk Transfer Perspective*
9. LMK Homes: Creating a Smart Home
10. Wink Labs Inc. website
11. The IT Guys, *Smart Wiring*
12. Aartech Canada Inc. *Wiring Guide for the Smart Home*.
13. PC Magazine: *How to Control Your Smart Home with IFTTT* (May 21, 2018).

Appendix (next page)

APPENDIX

TED 2018: The smart home that spied on its owner

By Jane Wakefield, Technology reporter, 14 April 2018

Image copyright GIZMODO

For two months in early 2018, technology journalist Kashmir Hill let innocent household items spy on her.

She had turned her one-bedroom apartment into a "smart home" and was measuring how much data was being collected by the firms that made the devices.

Her smart toothbrush betrayed when she had not brushed her teeth, her television revealed when she had spent the day bingeing on programmes, and her smart speaker spoke to the world's largest online retailer every day.

It was like living in a "commercial, surveillance state" with "not a single hour of digital silence", she said.

Kashmir filled her home with smart gadgets. Ms Hill, who reports for the technology news website Gizmodo, gave a TED talk describing her experience.

Her colleague Surya Mattu had built a special wi-fi router to monitor the devices listening to her life. They found that she was giving away a lot of information.

"The Amazon Echo [a smart speaker] talked to Amazon servers every three minutes and the TV was sending information about every show we watched on Hulu, which was in turn shared with data brokers."

But perhaps more worrying than the data she could track, was the vast amount that she could not.

Image copyright GIZMODO

Kashmir's television viewing habits were tracked. "With the other data I don't know ultimately where it was shared," she said. The lack of transparency about what happens to the huge amount of consumer data that is sucked out of smart devices and social networks every day has been in sharp focus in the last few weeks.

Facebook remains under intense scrutiny after it was revealed that up to 87 million Facebook users may have had their profile information accessed by marketing firm Cambridge Analytica without their knowledge.

Even Kashmir's toothbrush was internet-connected.

But while some consumers are prepared to part with their data for the convenience of access to free services such as Facebook and Google, Ms Hill did not feel this was true of her smart experiment.

"My smart home was not convenient. Things didn't work, the smart coffee was horrible, Alexa didn't understand us and my take-away was that the privacy trade-off was not worth it."

Facebook may currently be in the spotlight, but it is by no means the first to be caught out over the mishandling of user data.

In 2017, smart TV manufacturer Vizio agreed to pay $2.2m to settle a lawsuit brought by the US Federal Trade Commission over charges that the company installed software on 11 million of its smart TVs to collect viewing data, without informing customers or seeking their consent.

In addition, it also gathered each household's IP address, nearby wi-fi access points and postcode, and shared that information with other companies to target advertisements at Vizio TV owners.

And in August 2016, in a particularly intimate example of data misuse, hackers at the Def Con security conference revealed that Standard Innovation's We-Vibe smart vibrators transmitted user data - including heat level and vibration intensity - to the company in real time.

"It is interesting that the issue has coalesced around Facebook but it is a much wider issue," said Ms Hill.

"We use platforms on our smartphones and social networks that introduce us to third-party apps and we haven't yet come to terms with what this means, and how much responsibility the companies have to vet these apps and keep us and our data safe."

That is all about to change in Europe with the introduction of the General Data Protection Regulation (GDPR), which promises consumers far greater control over their data.

Currently the situation in the US is very different. Citizens do not have the right to access the information that companies have stored on them.

However, California, which is home to most of the biggest tech giants, is currently considering a law that would give users access to their data and let them ask firms not to sell it.

For Ms Hill, the changes in Europe cannot come soon enough.

"I absolutely hope that GDPR has a trickle-down effect on the US," she said.

Meanwhile, she is not willing to totally abandon her smart home experiment.

"We will keep the Echo and the smart TV. I don't love all this stuff, but it is going to stay in our home.

"What I hope is that we can make better products in future - devices with privacy protections built-in."

Source: https://www.bbc.com/news/technology-43747421