Enabling Smart Home with 5G Network Slicing

Bruno Dzogovic
Oslo Metropolitan University
Norway
bruno.dzogovic@oslomet.no

Bernardo Santos
Oslo Metropolitan University
Norway
bersan@oslomet.no

Josef Noll
University of Oslo/ITS
Kjeller, Norway
josef.noll@its.uio.no

Van Thuan Do
Wolffia AS
Norway
vt.do@wolffia.no

Boning Feng
Oslo Metropolitan
University Norway
boning.feng@oslomet.no

Thanh van Do
Telenor and Oslo Metropolitan
University Norway
thanh-van.do@telenor.com

***Abstract*— In addition to mobile phones 5G mobile networks will have to support billion IoT devices and applications. To achieve this objective 5G relies in the network slicing concept which is not yet fully understood. This paper describes how 5G network slicing can accommodate Smart Home, a popular IoT application. The state of the art of Smart Home is thoroughly studied and the findings summarized. The Smart Home network slicing and its pilot implementation are also described in a concise but comprehensive way.**

Keywords—Smart Hone, Home automation, 5G mobile networks, 5G mobile systems, 5G network slicing, Internet of Things

I. INTRODUCTION

The current wave of mobile communication is between human beings but the next one will be between devices and the next generation mobile system must be designed for that. In fact, the 5th generation mobile system aka 5G is aiming at supporting in addition to data hungry smartphones billion of IoT (Internet of Things) devices ranging from simple low cost low energy ones using massive machine-type communications (mMTC) to advanced ones requiring ultra-reliable and low-latency communications (URLLC). To achieve these rather diversified objectives 5G relies on the network slice concept which makes use of Network Function Virtualization (NFV) and Software Defined Network (SDN). However, this concept is still at earlier stage and it is not yet fully understood. In fact, it is not unclear how 5G can meet the requirements of Smart Home, one of the currently most popular IoT applications. Indeed, Smart Home is very important in an aging Europe because it paves the way for remote healthcare allowing elderly people to stay longer at their own home. This paper presents the work carried out at the Oslo Metropolitan University Secure 5G4IoT Lab[1] within the scope of the H2020 SCOTT project[2], which is aiming at shedding light on how 5G network slicing can efficiently support Smart Home in terms of performance, management, security and cost.

[1] http://5g4iot.vlab.cs.hioa.no/
[2] https://scottproject.eu/

The paper starts with a short but comprehensive introduction of Smart Home. Next, the state of the art of Smart Home implementation is studied thoroughly and the findings are summarized. The 5G network slice concept is then explained. The core of the paper is naturally the presentation of the Smart Home Network Slicing. Last but not least is a concise description of the pilot at the Secure 5G4IoT lab. The paper concludes with a few suggestions of further work.

II. SHORT ABOUT SMART HOME

Smart Home, as known as Connected Home, Home Automation or Domotics has currently a few definitions of Smart Home that provide a common understanding although with some nuances as follows:

Oxford Dictionary:
A home equipped with lighting, heating, and electronic devices that can be controlled remotely by smartphone or computer.
Example to illustrate: *"you can contact your smart home on the Internet to make sure the dinner is cooked, the central heating is on, the curtains are drawn, and a gas fire is roaring in the grate when you get home"* [1].

BT:
The term *'smart home'* is used to describe a house that contains a communication network that connects different appliances and allows them to be remotely controlled, monitored and accessed, according to the Department of Trade and Industry.
Smart devices connect to the internet and many have smartphone apps allowing you to access and control them remotely over Wifi [2].

UK Department of Trade and Industry:
A dwelling incorporating a communications network that connects the key electrical appliances and services, and allows them to be remotely controlled, monitored or accessed [3].

TechTarget:
A smart home is a residence that uses internet-connected devices to enable the remote monitoring and management of appliances and systems, such as lighting and heating [4].
Smart home technology, also often referred to as home automation or domestics (from the Latin "domus" meaning

home), provides home owners security, comfort, convenience and energy efficiency by allowing them to control smart devices, often by a smart home app on their smartphone or other networked device [4].

Honeywell:

A connected, controllable and intelligent home where all systems, including heating and lighting, communicate with one another and can be controlled from anywhere at any time using a single phone, tablet or computer, with the main goal being energy efficiency [5].

Actually, according to all the mentioned definitions Smart Home does contain the same main attributes, namely *"connected"*, *"controlled"* and *"intelligent"*. However, Smart Homes may differ each other on how well connected, well controlled and intelligent they are. Further, they may have different smart devices and smart applications.

As shown in Figure 1 the most popular Smart Home applications are as follows:

- **Smart locks** and garage-door openers allow the home owner to grant access to friends or visitors
- **Smart TVs** are connected to the Internet and enable access content through applications, such as on-demand video and music.
- **Smart security cameras** enable home members to monitor their homes when they are away or on vacation. Smart motion sensors are also able to identify the difference between residents, visitors, pets and burglars, and can notify authorities if suspicious behavior is detected.
- **Smart blinds** can adjust themselves to maintain the same level of light using sun tracking
- **Smart thermostats** let the users schedule, monitor and remotely control home temperatures. These devices also learn home owners' behaviors and automatically modify settings to provide residents with maximum comfort and efficiency.
- **Smart lighting** adjusts the light intensity, colour according to the lightness of the room, time and human presence.
- **Smart appliances** of all kinds can be programmed to perform their task according to the user's will such as smart coffee makers can brew fresh cups as soon as the kitchen door goes is open.
- **Smart irrigation** is capable of automating the irrigation process by analyzing the moisture of soil and the climate condition.

In order to function properly, these smart devices need to be connected. The first communication protocol for home automation X10 [6] was developed in 1975 by Pico Electronics of Glenrothes, Scotland, with the objective of allowing remote control of home devices and appliances. X10 is a one-way technology and not fully reliable. With the growing popularity of Smart Home several other wireless technologies have emerged.

Today although many smart home systems still use X10 Zigbee [7][8] and Z-Wave [9][9] are two most used home automation communication protocols, which are short range and low power wireless technologies. Lately, both Bluetooth [10] and WiFi [11] have grown in popularity. More details about the usage of these technologies are given in the next section.

Figure 1 Smart Home Application [Courtesy: TechTarget]

III. State of the Art of Smart Home Implementation

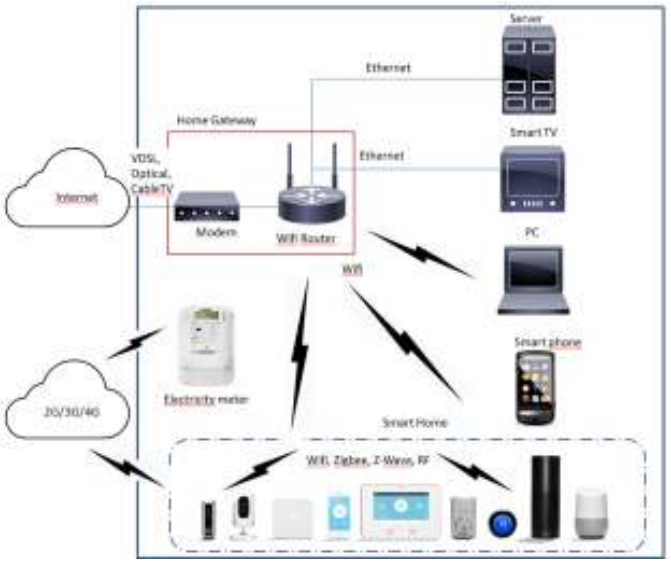

Figure 2 A typical current Smart Home

As depicted in Figure 2 most of European homes are todays connected to the Internet using one of the technologies like ADSL (Asymmetric digital subscriber line) [12], VSDL (Very high speed digital subscriber line) [13][14] optical fibre or CATV (Cable Television) [15] via modem (modulator demodulator). To establish a home network, it is necessary to connect a router to the modem. This router can quite often

provide both Ethernet and Wireless LAN (Wifi) connections to various devices from personal computers, servers, TV, media systems and also home appliances like refrigerators, air conditions, etc. It may act as a DHCP (Dynamic Host Configuration Protocol) [16] server which assigns IP addresses to devices and as DNS server, which translates domain names to the numerical IP addresses needed for locating and identifying computer services and devices.

The router may also include a firewall for the protection of the home network and a NAT (Network Address Translation) router which converts a local and internal IP address for an internal host into a global and visible IP address on the Internet.

Although quite efficient and usable the Wireless LAN has a few major limitations as follows:

- **Weak security:** Wireless LAN as such comes without any form of security and packets can be intercepted, read and falsified by external parties. Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). The WPA protocol implements much of the IEEE 802.11i standard. To enable WPA or WPA2 users must define passwords which on one side requires more administration and on the other side is not strong enough if weak passwords or passphrases are used.
- **Challenging configuration:** Devices using wireless LAN cannot function immediately after the first-time power on but need to be configured properly. This configuration although trivial to IT professionals could pose challenges to non-technical users which result to wrong or poor configuration, limited effectiveness and critical security vulnerabilities.
- **Limited coverage and reliability:** The Wireless LAN signal quality in a home depends very much on the walls, ceilings and large objects like fire doors, oven, fireplace, etc. Further, there may be radio frequency interference with devices that emit electromagnetic signals such as AM/FM radios, televisions, microwave ovens, etc. The combination of all these issues may result to poor or unstable connections at some spots.
- **High energy consumption:** While supporting higher data rates Wireless LAN requires on average 30% more energy consumption on data transmission than other wireless technologies like Bluetooth **Error! Reference source not found.Error! Reference source not found.**, Bluetooth Low Energy, Zigbee, Z-wave, etc. Further, devices using Zigbee and Z-wave in sleep mode consume minimal energy and can go on for weeks and months.

Due to the mentioned limitations, there are currently several home devices that do not use Wireless LAN but other wireless technologies such as the electricity meter and the smart home security system.

- **The electricity meter:** A smart meter is an electronic device that records consumption of electric energy and communicates the information to the electricity supplier for monitoring and billing. Smart meters typically record energy hourly or more frequently, and report at least daily. Smart meters enable two-way communication between the meter and the central system. Such an advanced metering infrastructure (AMI) differs from automatic meter reading (AMR) in which it enables two-way communication between the meter and the supplier. Generally, the electricity supplier wants to have an isolated and secure connection between the meter and the central to avoid any tampering of the meter.

  Communications from the meter to the network may be wireless, or via fixed wired connections such as power line carrier (PLC). Wireless communication options in common use include M2M cellular communications, wireless ad hoc networks over Wi-Fi, wireless mesh networks, low power long range wireless (LORA), ZigBee (low power, low data rate wireless), and Wi-SUN (Smart Utility Networks).
- **The smart home security system**: consists usually of a control panel and a series of security devices such as door locks, garage door openers, indoor and outdoor surveillance cameras, lights, sirens, smoke/CO detectors, water sensors, etc. Recent control panels have the ability to connect themselves to the home wireless LAN but in order to ensure 99,99% availability, the communication of the control panel with the security company is usually realised by an M2M cellular subscription with a mobile operator. Home security devices are mostly simple and low energy sensors like smoke/CO detectors, proximity sensors, motion detector, etc. and the usage of wireless LAN will drain all their batteries in a short time. For more optimal energy usage these devices use other wireless protocols which consume at least 30% less energy than wireless LAN such as Zigbee, Z-wave, Bluetooth, Bluetooth Low Energy, or even proprietary mesh protocol.

Findings:

In current European homes there are a variety of devices from very primitive ones with limited energy to very powerful ones having access to continuous power supply, from the open ones to the completely close and high secure ones.

Although wireless LAN is a very efficient and affordable wireless technology and by far the most popular one it fails to give adequate support to the low power devices or the ones with high security requirements.

The demand of a new wireless Home Networking capable of supporting all heterogeneous home devices, especially the simple ones and the secured ones.

IV. 5G Mobile Network Slicing concept

Originally the mobile network is aiming at providing connectivity for mobile phones which are on the move in the outside. With technology advances mobile phones are migrating to 3G and 4G mobile networks and leaving the 2G mobile networks to M2M devices which uses the uplink only at predefined time intervals to transmit a small amount of data to their cloud server.

As the successor of 4G, 5G mobile system [17] is well known for its superiority in terms of performance, coverage and quality of service and the promise of enhanced mobile broadband (eMBB) with higher data speed and the support of a wide range of services and application ranging from massive machine-type communications (mMTC) and ultra-reliable and low-latency communications (URLLC). To achieve this challenging objective the concept of network slicing is presented as the ultimate solution which will be clarified in the coming section.

To understand the network slicing concept let us start with a short introduction of the 5G mobile system architecture.

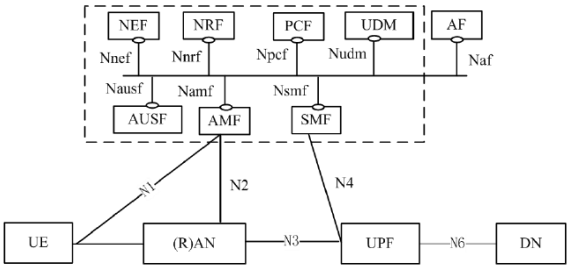

Figure 3 The 5G Reference Architecture (Courtesy of 3GPP)

As shown in Figure 3 the 5G Reference Architecture differs with the 4G architecture not only in their different Network Functions [18] but also in the separation of the User plane and Control plane.

The User plane consists of the following Network Functions:

- **UE** (User Equipment): is the user's mobile phone.
- **(R)AN** (Radio Access Network): is the Access Network Function which provides connectivity to the mobile phone.
- **UPF** (User Plane Function): handles the user plane traffic, e.g., traffic routing & forwarding, traffic inspection and usage reporting. It can be deployed in various configurations and locations depending on the service type.
- **DN** (Data Network): represents operator services, Internet access or 3rd party services.

The User plane consists of the following Network Functions:

- **AMF** (Access and Mobility Management Function): performs access control, mobility control and transparent proxy for routing SM messages.
- **AUSF** (Authentication Server Function): provides authentication functions.
- **UDM** (Unified Data Management): stores subscriber data and profiles. It has an equivalent role as HSS in 4G but will be used for both fixed and mobile access in 5G core.
- **SMF** (Session Management Function): sets up and manages the PDU session according to network policy.
- **NSSF** (Network Slice Selection Function): selects the *Network Slice Instance* (NSI), determines the allowed *network slice selection assistance information* (NSSAI) and AMF set to serve the UE.
- **NEF** (Network Exposure Function): exposes the services and capabilities provided by the 3GPP network functions.
- **NRF** (NF Repository Function): maintains NF profiles and supports service discovery.
- **PCF** (Policy Control function): provides a policy framework incorporating network slicing, roaming and mobility management and has an equivalent role as PCRF in 4G.**AF** (Application Function): interacts with the 3GPP Core Network (CN) to provide services.

Currently, there is no consensus on what a network slice is and how it can be realized. In fact, while the 3rd Generation Partnership Project (3GPP) [19] provides a more network-focused definition stating that "network slices may differ for supported features and network functions optimisations" the 5G Infrastructure Public Private Partnership (5G PPP) adopts a business oriented view mandating that "network slice is a composition of adequately configured network functions, network applications, and the underlying cloud infrastructure (physical, virtual or even emulated resources, RAN resources etc.), that are bundled together to meet the requirements of a specific use case, e.g., bandwidth, latency, processing, and resiliency, coupled with a business purpose" [20].

In this paper we use the 5G PPP's definition that allows the support of a variety of devices. To obtain a wireless Home Networking capable of supporting a broad range of devices the 5G network slicing concept is adopted to establish a Smart Home Network Slice.

V. Smart Home Network Slicing

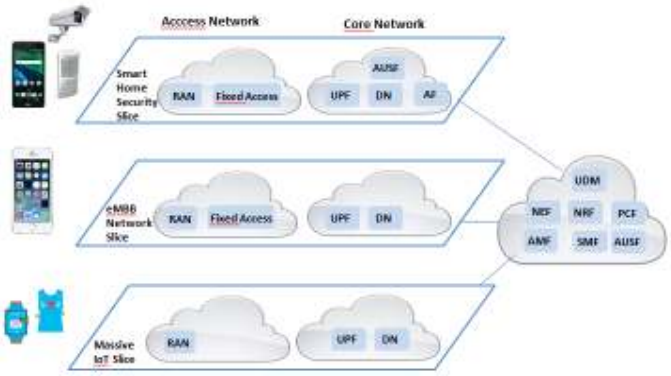

Figure 4 Smart Home Network Slicing

To provide a better home network capable of addressing a variety of devices with different QoS requirements three 5G network slices are proposed as shown in Figure 3

The Smart Home Security system has higher security requirements than other applications and an isolated dedicated end-to-end network slice will be established for it. To ensure isolation the Smart Home Security system has their own virtual Network Functions both for the access and core network. It has its own instance AUSF (Authentication Server Function) which carries out authentication of devices before granting access to the slice.

The enhanced Mobile Broadband (eMBB) network slice provides connectivity to devices with high data rate demands such as mobile phones, laptops, tablets, cameras, etc. It is worth noting that the access to this network slice can be incorporated to a total subscription for both home and mobile subscription for individual members or the whole household.

The Massive IoT network slice provides low data rate connectivity to low power devices such as diverse sensors e.g. motion sensors, proximity sensors, smoke/gas detectors, etc. or home appliances such as refrigerator, coffee machines, washing machines, etc.

VI. The Smart Home Network Implementation

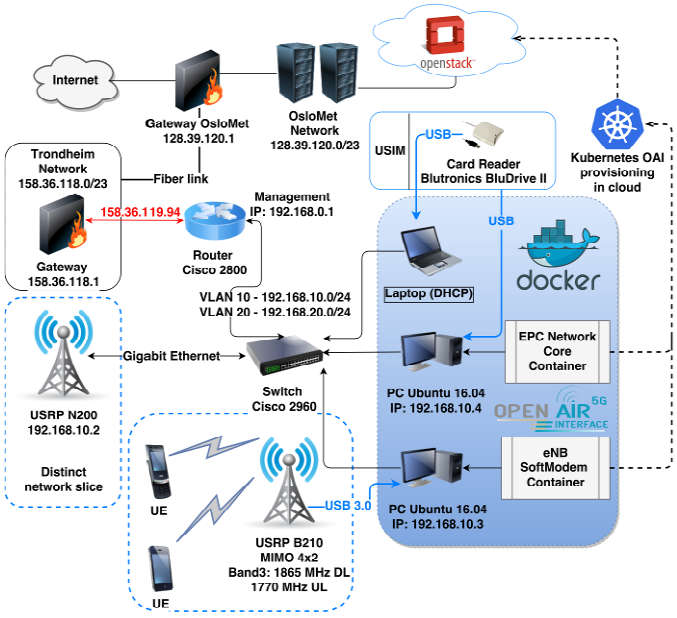

Figure 5 The Internet Light Network Slice Proof-of-Concept

To realise and experiment the Smart Home Network Slicing, it is necessary to establish a 5G network. This can be done by acquiring and using network equipment from Telecom manufacturers like Ericsson, Nokia, Huawei, etc. but within the scope of the H2020 SCOTT project an open source approach using OpenAirInterface (OAI) [21] is adopted. To establish an early 5G network, we carried out the virtualization or more precisely the containerization of the OAI software stack of network functions.

Containerization [22] also called container-based virtualization and application containerization is an operating system level virtualization method for deploying and running distributed applications without launching an entire VM for each application. Multiple isolated systems, called containers, are instead run on a single control host, accessing a single kernel. At the Secure 5G4IoT lab, we adopt a configuration which uses a separate container to deploy the entire EPC, as well as another one for the eNB, as shown in Figure 5. There are few container implementation possibilities, but in our pilot, Docker is used for the containerization of the OpenAirInterface.

As shown in Figure 5 the PoC consists of the following nodes:

- **EPC:** 192.168.10.3; PC running Ubuntu 16.04
- **eNB:** 192.168.10.4; PC running Kali Linux connected via USB 3.0 interface to a Universal Software Radio Peripheral (USRP) B210 and via Ethernet with a USRP N200 [23].
- Two smartphones Huawei P9 lite, equipped with self-programmed Milenage algorithm SIM cards
- Blutronics BluDrive II SIM card programming device
- Cisco 2800 router and Cisco 2960 switch, separated in two VLANs

VII. Conclusions

This paper focuses on Smart Home, one of the most popular IoT applications which has quite diversified and challenging requirements in terms of performance, security, management and cost. The paper identifies the limitations of the current Smart Home solutions using other wireless technologies and shows how the network slicing concept can address these shortcomings. So far, the implemented pilot is still quite primitive and more elaborated implementation with more home applications and devices should be done as further work. Further, a trial with real users would be quite useful to collect feedbacks that could be used to tune the network slices. Last but not least, activities should be initiated to identify business opportunities and to derive business models for the promotion of 5G Smart Home.

References

[1] Oxford dictionary: https://en.oxforddictionaries.com/definition/smart_home

[2] BT: What is a smart home? How your future family house will look and think - http://home.bt.com/tech-gadgets/internet/connected-home/what-is-a-smart-home-11364214165664

[3] UK Department of Trade and Industry, Project Smart Home. Intertek; https://www.housinglin.org.uk/_assets/Resources/Housing/Housing_advice/Smart_Home_-_A_definition_September_2003.pdf

[4] TechTarget: smart home or building (home automation or domotics) - https://internetofthingsagenda.techtarget.com/definition/smart-home-or-building

[5] Honeywell: Smart homes of the future: An industry view https://heatingcontrols.honeywellhome.com/file_uploads/pdf/116837_Honeywell_Smart_Homes_Final_Int.pdf

[6] Rye, Dave (October 1999). "My Life at X10". AV and Automation Industry eMagazine. AV and Automation Industry eMagazine. Retrieved October 8, 2014 - https://www.hometoys.com/content.php?url=/htinews/oct99/articles/rye/rye.htm

[7] Zigbee Alliance: ZigBee Cluster Library Specification Rev 6 - Draft Version 1.0, Chapter Document: 14-0125, ZigBee Document: 07-5123-06, Jan 2016

[8] Zigbee Alliance: Base Device Behavior Specificatio Ver 1.0 - ZigBee Document 13-0402-13, Feb 2016

[9] https://z-wavealliance.org/about_z-wave_technology/

[10] G. D. Putra, A. R. Pratama, A. Lazovik and M. Aiello, "Comparison of energy consumption in Wi-Fi and bluetooth communication in a Smart Building," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-6. doi: 10.1109/CCWC.2017.7868425

[11] IEEE: IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. (2016 revision). IEEE-SA. 14 December 2016. doi:10.1109/IEEESTD.2016.7786995.

[12] ITU: Recommendation ITU-T G.992.3 - Asymmetric digital subscriber line transceivers 2 (ADSL2) SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS Digital sections and digital line system – Access networks. Telecommunication standardization sector of ITU. April 2009.

[13] ITU: Recommendation ITU-T G.993.1: Very high speed digital subscriber line transceivers (VDSL). July 2016.

[14] ITU: Recommendation ITU-T G.993.2: Very high speed digital subscriber line transceivers 2 (VDSL2)". July 2016.

[15] ITU: DOCSIS 2.0 ITU-T Recommendation J.122

[16] IETF: RFC 2131, Dynamic Host Configuration Protocol

[17] 5G Infrastructure Public Private Partnership (5G PPP): *View on 5G Architecture* (Version 2.0), 5G PPP Architecture Working Group - 2017-07-18

[18] ETSI: GS NFV 002 *Network Functions Virtualization (NFV)*; Architectural Framework, v.1.1.1, 10-2013

[19] 3rd Generation Partnership Project (3GPP): Technical Specification TS 23.501 V1.3.0 (2017-09) Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Stage 2 (Release 15) 09-2017

[20] 5G Infrastructure Public Private Partnership (5G PPP): View on 5G Architecture (Version 2.0), 5G PPP Architecture Working Group - 2017-07-18

[21] http://www.openairinterface.org/

[22] Docker: Docker for the Virtualization Admin, 2016; htttp: www.docker.com

[23] Ettus Research, Inc., USRP N200 (Online] Available at: https://www.ettus.com/product/details/UN200-KIT (Accessed November 2017]

ACKNOWLEDGEMENT

This paper is a result of the SCOTT project (www.scott-project.eu) which has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the EU H2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.