

PROJECT PROFILE

16105

An affordable, open, modular reference-platform to protect critical services on shared networks
[MuSiC]



MuSiC (or Multi-level Security for Critical services) provides scalable and certifiable security to devices within the mid- to high-data-rate, cost-effective range. In particular, this project secures against threats related to applications, operating systems, the web and networks, with the prime purpose of protecting critical services on shared networks.

Cybersecurity Ventures (a cybersecurity researcher) predicts that global annual cybercrime costs will grow from \$3 trillion in 2015 to \$6 trillion annually by 2021. This includes data damage and destruction, lost productivity, embezzlement, fraud, as well as, post-attack disruption to the normal course of business, and theft of intellectual property and personal and financial data. Consequently, integrity and confidentiality of all handled information are becoming increasingly crucial.

The development of internet and mobile communications, and the increasing number and diversity of connected devices, are all making digital services ubiquitous. High-end devices—like smartphones, PCs and tablets in the consumer market—are becoming more secured. However, mid- to high-data-rate, cost-effective devices (such as IP cameras and routers) are still vulnerable due to a lack of certification and off-the-shelf-secured solutions.

Innovative way to secure critical services on shared networks

The goal of MuSiC is to develop an affordable, open, modular reference-platform providing a scalable and certifiable solution for any connected device (including mid- to high-data-rate ones) that secures against any threats related to applications, operating systems, networks and the Web, by protecting critical services on shared networks.

One technological innovation is to develop a novel architecture (both hardware and software), which is optimised for low-power and a cost-efficient IoT (internet of things), as well as, communication devices supporting the security mechanisms existing today on high-end computing and mobile devices. MuSiC plans to target several markets where trusted devices and digital services are required.

The major project outcomes will be:

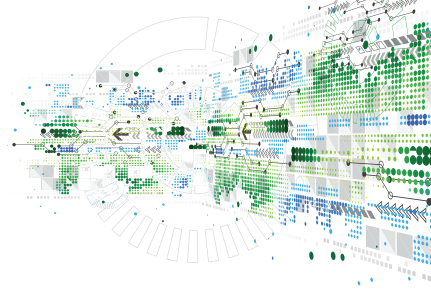
- A scalable secure solution for the development of trusted devices offering adequate processing capabilities to support multimedia services, protecting against various kinds of attack covering secure access and sensitive data protection;

- Cost-effective, common-criteria security-certification paths up to the level required by mission-critical services in order to give users and manufacturers confidence in these trusted devices;
- Demonstrators for representative use-cases within Smart City and public protection and disaster relief applications, integrating these trusted devices and validating their security and performance requirements.

Outputs of the demonstrators using trusted devices will be:

- New services for Smart City applications based on public lighting and traffic monitoring demonstrated in France and/or in the Czech Republic;
- Secure UWB (ultra-wideband), a precise and fast location-detection system which integrates comprehensive security features, including an advanced encryption algorithm for data links;
- High-fidelity simulators to generate the scenarios and test the MuSiC approach;
- Demonstrator to validate optimal network communications during an emergency situation with an unmanned aerial vehicle (UAV);
- Real-time multimedia communication services;
- Built-in adaptive reconfiguration that ensures that the most resource-efficient versions of algorithms are used, based on the context of use;
- Improved IoT platform ready for diverse Smart City scenarios.

The project consortium is a good example of European collaboration. It is composed of 15 partners, with expertise in security and safety, and covering both the project technology and market value-chains. The consortium includes large- and small-enterprises strongly committed to promoting and disseminating industrial standards.



KEY APPLICATION AREAS

-  Transport & Smart Mobility
-  Health & Well-Being
-  Energy
-  Digital Industry
-  Digital Life

ESSENTIAL CAPABILITIES

-  Systems and Components Architecture, Design & Integration
-  Connectivity & Interoperability
-  Safety, Security & Reliability
-  Computing & Storage
-  ECS Process Technology, Equipment, Materials & Manufacturing

PARTNERS

STMicroelectronics / Prove & Run / CEA LIST / CEA LETI / AIRBUS Defense and Space / ADWAVE / FIT of Brno University of Technology / CAMEA / Enigmmedia / HI-Iberia Ingeniería y Proyectos / Quobis Networks SL / Tecnologías Servicios Telemáticos y Sistemas SA

COUNTRIES INVOLVED

-  Czech Republic
-  France
-  Spain

PROJECT LEADER

Marcello Coppola
STMicroelectronics Grenoble2 SA

KEY PROJECT DATES

01 June 2018 to 30 May 2021

Expected market impact

Several key markets, which could be impacted by MuSiC, need attention. The first is the cybersecurity and IoT market one. Here, global spending on cybersecurity products and services for defending against cybercrime is projected to exceed \$1 trillion cumulatively between 2017 and 2021. The global IoT security market was valued at \$4.83 billion in 2015 and will reach \$43.23 billion by 2020, growing at a compound annual growth rate (CAGR) of 55.01%.

Looking at the Smart City market, there are 315m street lights in the world, growing to 359m by 2026. LED (light-emitting diode, a semiconductor light source) and smart street-lighting will cumulatively represent a \$69.5 billion market opportunity over the next decade, as many cities replace their high-pressure sodium street lights with LEDs. And a growing number of cities are also discovering the benefits of incorporating new sensors and networked control into their new lights. Networked street lights provide an ideal platform for a range of innovative Smart City applications. The global homeland security surveillance-camera-market is expected to reach \$6.64 billion by 2021. The increase in traffic surveillance is one of the key factors driving growth in this market. Furthermore, the number of online traffic cameras used to monitor traffic flow on our roads is doubling every two-and-a-half years.

Public safety agencies around the world are echoing demands for the deployment of cost-effective broadband services. The total broadband LTE (long term evolution, a wireless communications standard) public-safety market is expected to grow at a CAGR of 44% over the next six years. Migration toward broadband LTE public-safety brings a new type of competition across the value chain, from content delivery device-providers to infrastructure/service providers. By 2024, there will be over 12m public safety broadband users using LTE-based devices.

Finally, the secure IC (integrated circuit) market will expand from \$1.8 billion units in 2016 to 3.5 billion units in 2021. However, this market will not be driven by a single type of solution. A layered security approach, as proposed by MuSiC, will result in OEMs (original equipment manufacturers) and service providers utilising a combination of hardware- and software-based mechanisms. And as 'things' functions become more standalone, the demand for hardware-based security will increase.

Removing the barriers

Unfortunately, market barriers exist because security has been largely considered a secondary issue. Not all applications require the same levels of security and cost-to-risk analysis. Minor things have low-costs, leading to low-power/memory requirements, thus limiting possible solutions. In addition, new OEMs lack the expertise, manpower or budgets. And fragmentation from an architecture perspective (hardware, software, operating system) is not helping either. Crucially, MuSiC will remove these barriers by offering an affordable open, modular and secure reference-platform.

MuSiC will achieve this by:

- Supporting the competitiveness of major European security-solutions actors;
- Growing the market for trusted devices, thus addressing OEMs and service providers, including emerging IoT suppliers who are often small medium enterprises lacking the required expertise in security;
- Protecting data and privacy of European citizens while reducing cybercrime costs;
- Promoting and extending existing security standards.

Aeneas Office

44 rue Cambronne
F-75015 Paris - France
Tel. +33 1 40 64 45 80
Fax +33 1 40 64 45 89

Email penta@aeneas-office.org
www.penta-eureka.eu

Penta (E! 9911), the EUREKA Cluster for Application and Technology Research in Europe on NanoElectronics, will bring about technological leadership for a competitive European information and communications technology industry.

