Below Dr Ploss discusses the need for an overhaul of cyber security policy in Europe and stresses the opportunities that this could bring the European economy.

In the past, we used to see the digital world as one thing and real life as another. Today, both are on the brink of becoming one. The increased connectivity between both spheres creates a new quality of interaction, offering numerous possibilities, yet also presenting many challenges: It urgently raises the need for trusted security solutions for exchanging information. As Europe has all the competencies and tools required for implementation, these solutions could give a push to Europe's economy becoming the world's leading 'security provider' and creating real value for the modern society.

To establish the solutions we could draw on the extensive expertise of Europe's industries in hardware, software, infrastructure, network provision, security systems and integration of systems, and not forgetting industries like automotive and aerospace serving the end markets.

There are plenty of examples of the great need for security solutions in both business and personal life alike. Not least if we strive to turn the visions of tomorrow's connected world into reality, establishing the Internet of Things as a major pillar.

1. The next revolution in industrial production, the so-called 'factory of the future' or 'Industry 4.0', needs the secure exchange of data. Connecting the different players along the value chain is a sensitive matter. The streams of highly valuable data have to be protected against unauthorized use by third parties; facilities connected to the Internet have to be guarded against hackers.

2. A stable and affordable provision of electrical energy is a key factor for industry. Modern electric power generation and distribution with renewable energies as the main source of supply need a reliable and sophisticated grid that can cope with the volatility of demand and supply as well as with the evolving plurality of power suppliers and customers. The active management of the electric power grid will lead to the need and exchange of a vast amount of data, thus raising the need for protection.

3. Managing the public and individual transport infrastructure in modern society will create totally new markets for services – and products. The established taxi services will remember 2014 as the year of a rising competitor they had never thought of before. At the same time, public transport providers have to make their services more attractive for coming generations by, for example, developing new ticketing and pricing solutions. Once again, we see new data streams – and potential threats.

4. Connected Mobility will offer individual mobility in many different ways, like mobility on demand or the further evolution of the car toward assisted and finally autonomous driving. With autonomous individual mobility, time will be given back to the people to be used for a better purpose than paying attention to the traffic, and infrastructure will be used more efficiently, thus avoiding traffic jams and reducing the toll of deaths or injuries by accidents. This scenario can only become reality on one condition: Hackers must have no chance to take over the control of the cars or parts of the vital infrastructure.

5. Healthcare of the future can be much more sophisticated and proactive, but also remain affordable thanks to advanced sensing and telematics systems. Especially in Europe, confronted with demographic change and an aging society, this will substantially add to a better daily life – as long as no unauthorized person or institution can gain access to the sensitive data that has to be available for medical services.

These five examples – many more could of course be listed – represent important market segments of Europe's economy, both business-to-business and business-to-consumer. They offer great real economic and societal value with their products and services. As shown in the brief descriptions though, this value can only be fully exploited if the most important common critical element is provided: security. Or, to be more precise in this context, a secure communication backbone – covering point-to-point and cloud communication – that can resist cyber attacks, provides trustworthy identification of communication partners, be it people or machines, and enables a secure and protected exchange of information between them.

The inestimable value of reliable and trusted communication is obvious and agreed widely among industry and politics. It has also become increasingly common sense in the whole of society. Cyber criminality is a rapidly growing threat and has to be countered fast and effectively.

There is a joint understanding that Europe has to act in order to establish a secure common backbone as the prerequisite for communication that is immune to attacks. Such a backbone is potentially not a differentiating factor by itself, since other economic regions will have their own solutions in place. However, if we do not develop it ourselves, we will make Europe either dependent on others or even frustrate industries into offering respective products and services, and playing a leading role in pushing the Internet of Things. Europe can establish its own secure backbone. To tap the potential and to underpin Europe's relevance, the way is clear: We have to join forces across industries and work closely together with public authorities to establish EU-wide standards and legislation. As mentioned above, we can build on substantial expertise – and strong positions – in the relevant markets like automotive, aerospace and industry equipment.

Despite working on a distinct European answer to security issues, we should always bear in mind: Security in the open world of the Internet requires thinking globally. Thus, Europe has to – and can – act self-confidently as a global player. The time has come for Europe to trigger a joint platform which enables cooperation between the leaders in the industry and, at the same time, also embraces small and medium-sized companies, helping them to contribute and benefit as well. Politics has to play an active and central role in orchestrating this approach due to its competitive nature.

To complement the approach, selective funding programs could be established to foster cross-company cooperation – as valuable support within specific phases as well as for selected topics. For example, purposeful funding could be an incentive for comprehensive concepts for the development and implementation of an overarching system. Programs could also subsequently help to industrialize solutions – establishing "Security made in Europe" as a quality label. And programs should ensure that corporate Europe and political Europe together can act as one key player in the pursuit of joint standards beyond our continent.

Enabling trustworthiness and secure communication in the digital world will serve as a substantial reinvigoration of Europe's economy.

by Dr. Reinhard Ploss, CEO at Infineon Technologies AG