The challenge to transform secure hardware into secure products

Presented by: Jean-Philippe Fassino
Schneider Electric / Technology / IOT & Digitization
“Rendez-vous de l'IRT Nanoelec” - Jeudi 24 Novembre 2016

Life Is On Schneider Electric

Schneider Electric, le spécialiste mondial de la gestion de l'énergie et des automatismes

Nous concevons, réalisons et mettons en œuvre des solutions innovantes pour une énergie sûre, efficace, fiable et propre.

Nous proposons des services à haute valeur ajoutée pour accompagner nos clients dans leur stratégie de gestion de l'énergie.

Résidentiel
Individuel et collectif

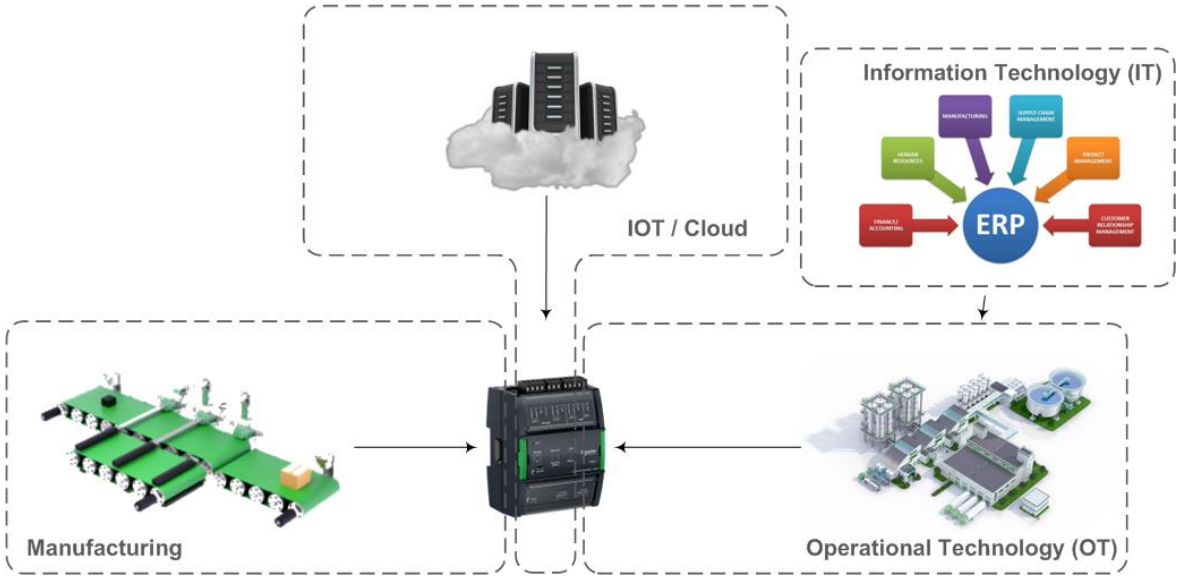
Bâtiments
Bureaux, santé, commerces, hôtels…

Industrie
Agroalimentaire, métaux, eau, machines…

Datacenters, salles serveurs…

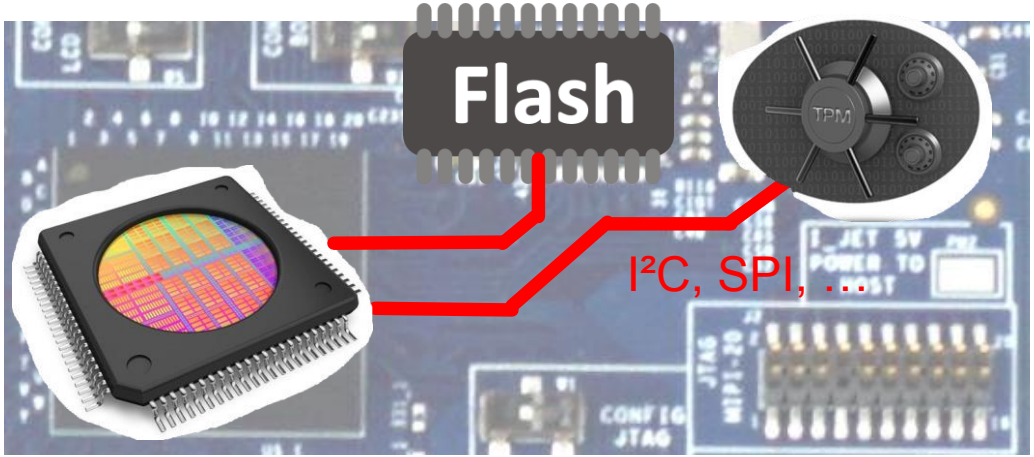
Energie
Production, répartition, distribution
Sécurisation de l'industrie électro-intensive

Cyber-Security challenge in Schneider Electric Eco-System



- Critical Infrastructure
- Connect & unconnected offers
- Several stakeholders in security
- Long product lifetime
- Long history and legacy
- Availability
- Safety
- Counterfeiting

Is the Secure Element sufficient?



Threat	Likelihood	Impact
Software vulnerabilities	Remote & reproducible	From low to high
CPU spoofing	Feasible hardware attack	Leakage of data: • Customer data • High value algorithm
Eaves-dropping on the communication link		
Attack on Secure Element	Very complex hardware attack	Compromising of cryptographic keys

Mitigating Secure Element threats

Software vulnerabilities

- Secure Development Lifecycle to improve software quality
- Trusted execution environment to process secure services

CPU spoofing & eaves-dropping

- Secure channel between processor & secure element
  - This lead to obfuscate a secret key in the processor which is not what we want
- Secure Element integrated within System-on-Chip should be a good solution
  - Removing the connection avoid these threats

To guarantee the security of the equipment, the security of the manufacturing line must be addressed

Advanced security features require specific operations during manufacturing

- Key injections for firmware digital signature & confidentiality, secure storage, …
- Certificate Signing Request for device genuineness, asset identity, …
- Locking some keys to avoid depersonalization while allowing late provisioning on customer site (dual security world)

While keeping manufacturing line constraints

- Short production time per product
- No network connection to avoid unplanned stop of the production
- Involvement of many third parties

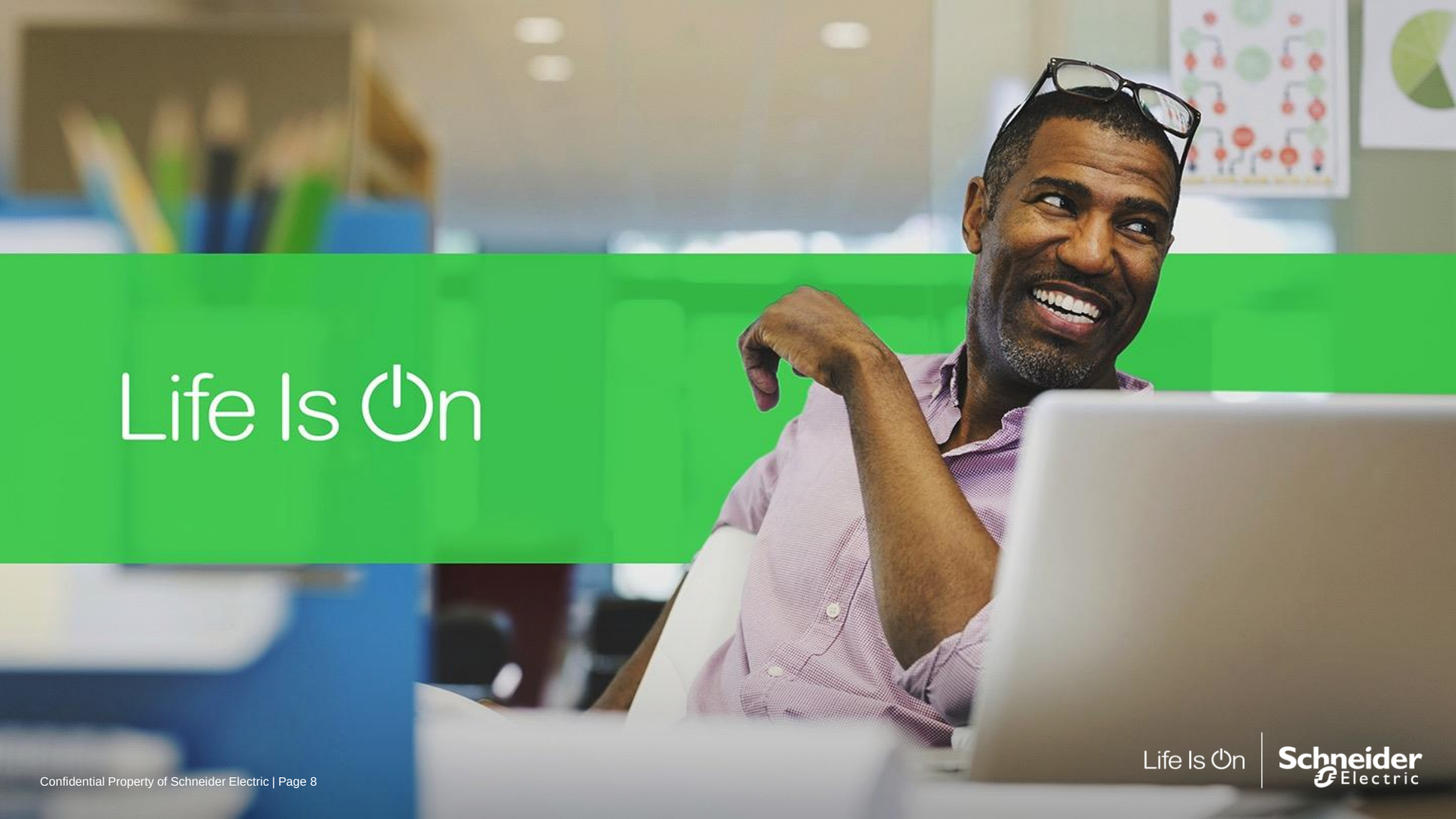
Conclusion

Silicon vendors should **evaluate the cost of attacks** to compromise their Secure Element

- It’s mandatory to choose adequate solution and characterize the resilience of the final product

Secure Element integrated within System-on-Chip should be a good solution

Impact on manufacturing line of adding security features must be correctly anticipated if we want to transform successfully secure hardware into secure products


Life Is On