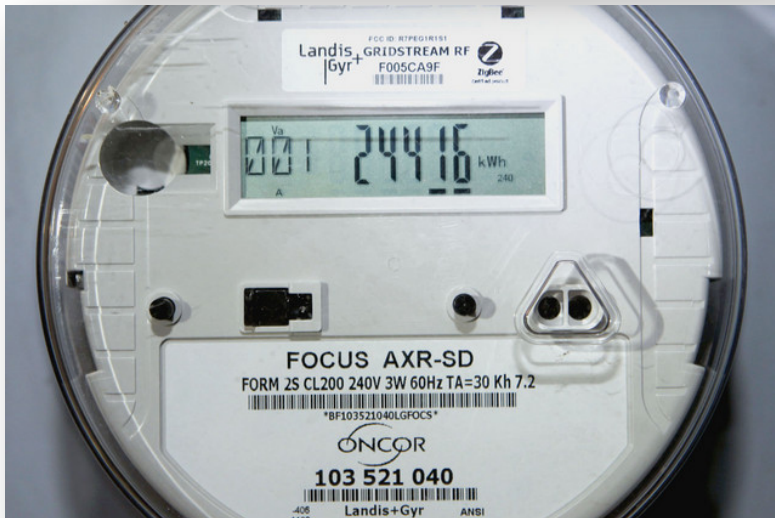
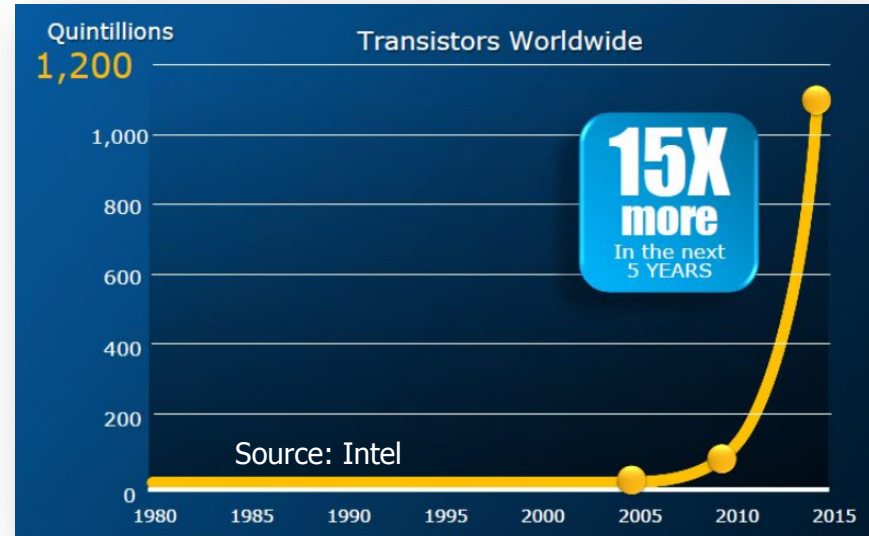


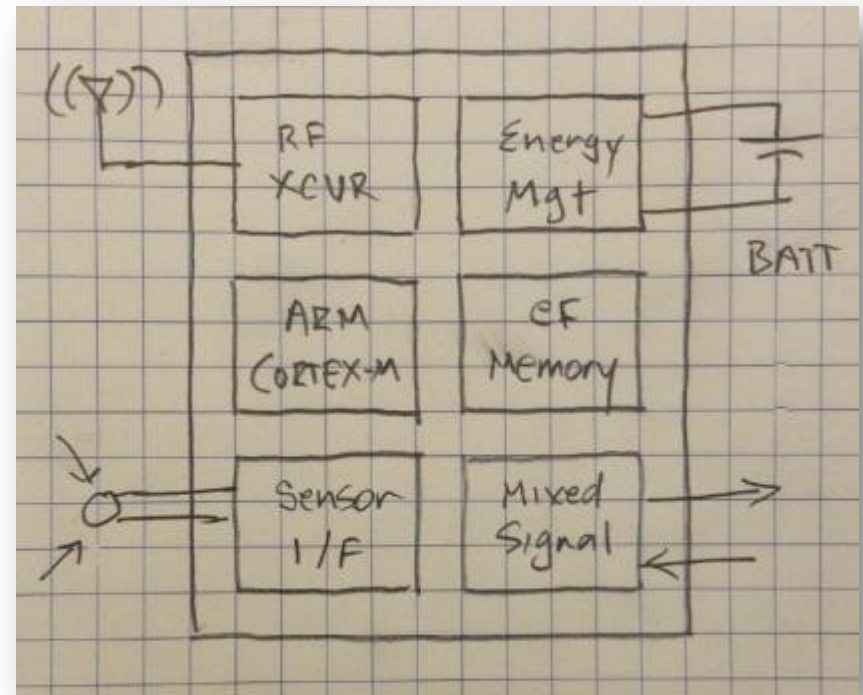
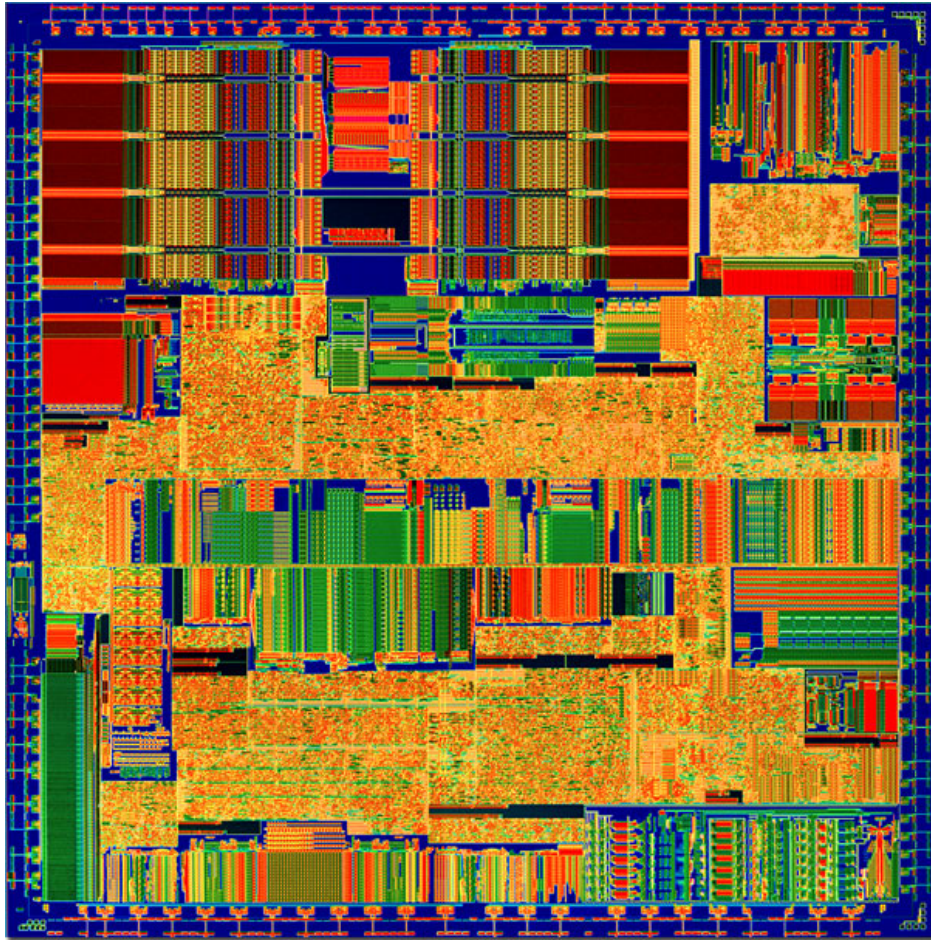


Trends in Hardware — Challenges in Security

Celia Merzbacher, Ph.D.
VP for Innovative Partnerships
Semiconductor Research Corporation
merzbacher@src.org







Source: Tyson Tuttle, Silicon Labs

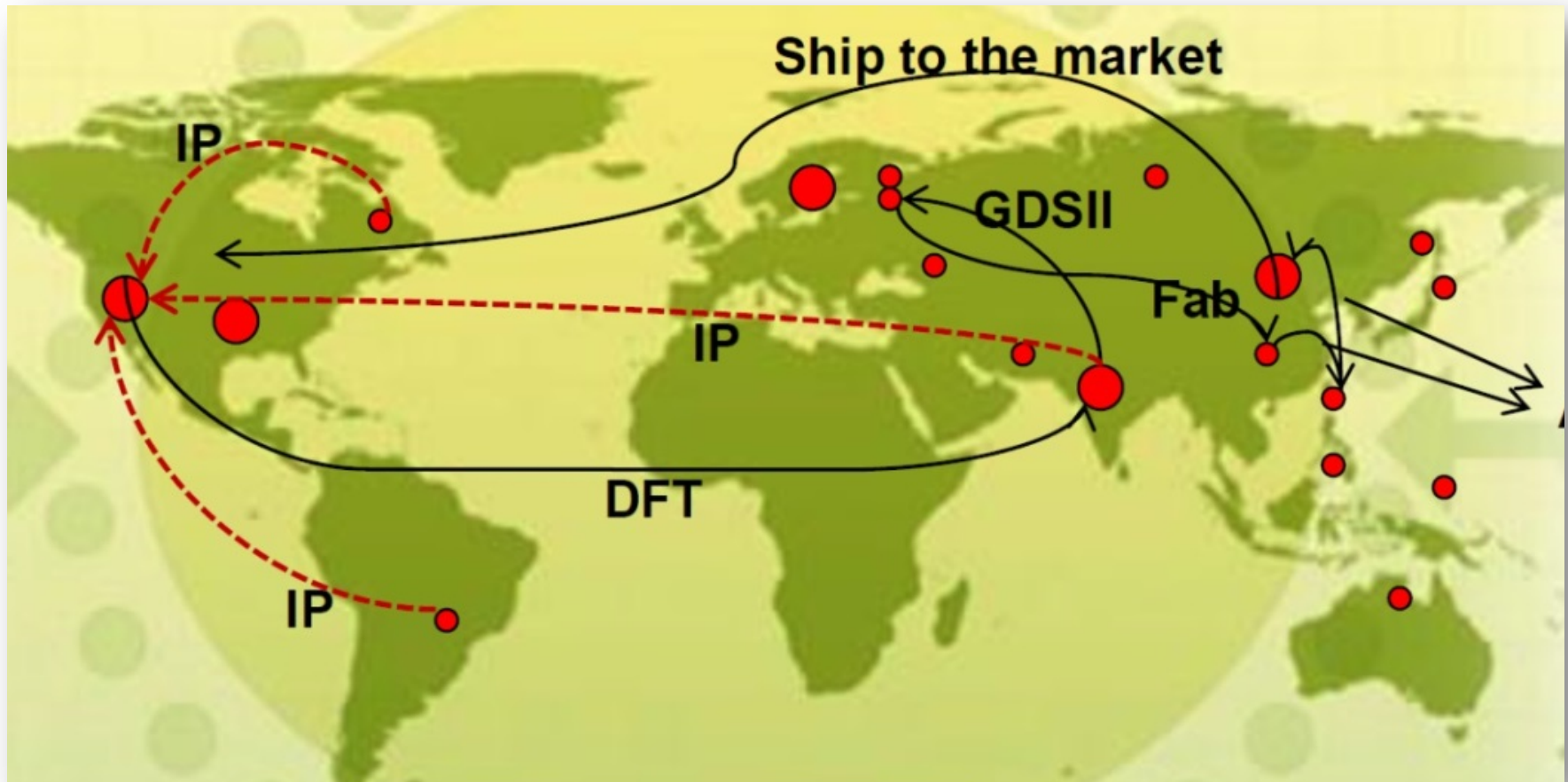
Corollary: Increased use of 3rd Party IP

Trend #3: Things are more Connected



Cisco predicts that 50 billion things will be connected by 2020—an Internet of Everything.

Trend #4: Design & Manufacture Involves More People in More Places

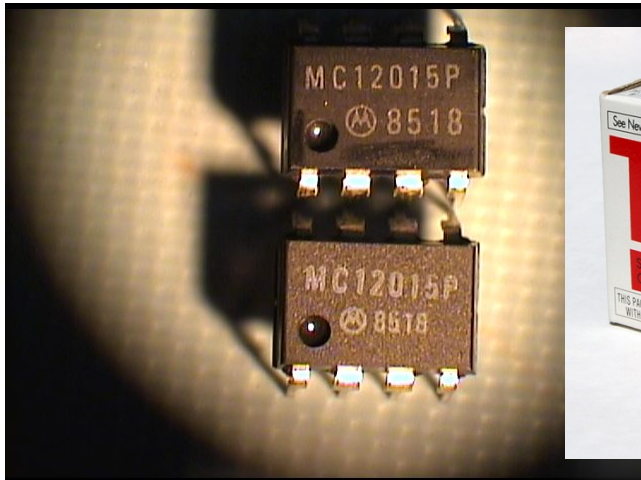


- ★ ***Greater chance of error or attack***
- ★ ***Greater impact if chip fails***
- ★ ***More attractive to various adversaries***

- Economically motivated criminals (counterfeits vs. access to valuable information/IP)
- Individuals with a political or social agenda
- Politically motivated State-supported programs
- Hackers



- Loss of IP/sales (theft or counterfeits)
- Damage to brand
- Risk management
 - Risk = $f(\text{Vulnerability, Impact, Likelihood})$
 - Risk factors are increasing
- Customer demand/requirement

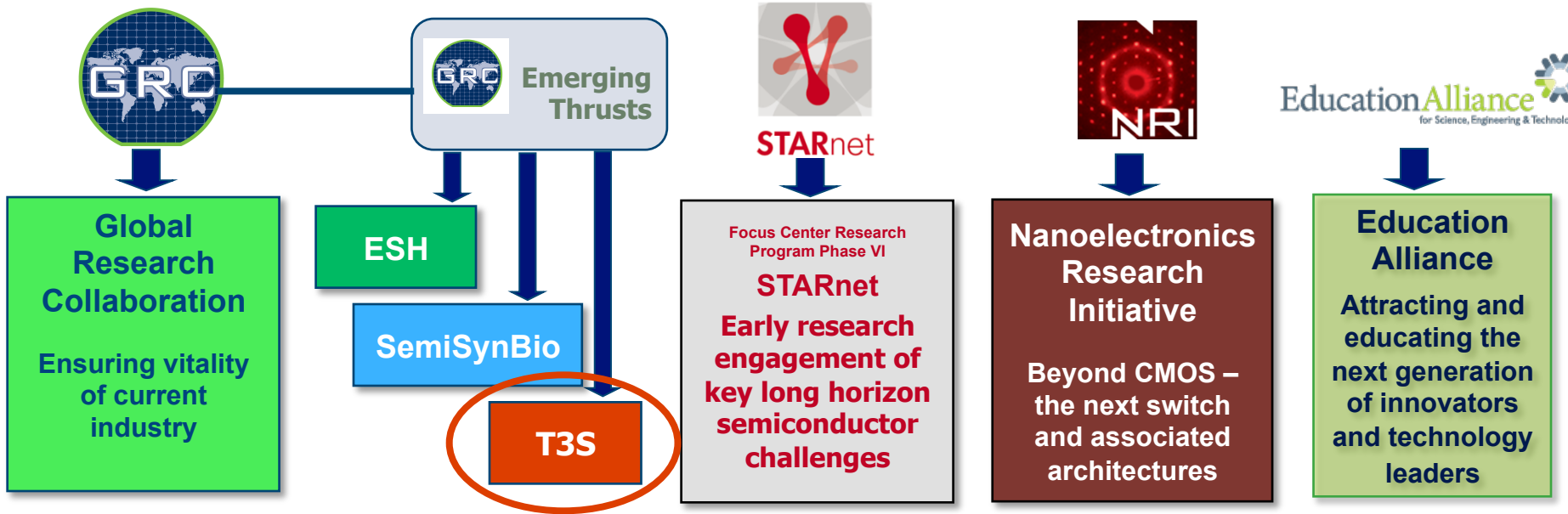


Provide assurance throughout the life cycle
that a product does what it was intended

...and nothing else

***...without unduly impacting
time to market, cost or performance.***

Trustworthy and Secure Semiconductors and Systems (T3S): A New Thrust in the SRC Portfolio



Bringing industry together to identify and support - in collaboration with government - fundamental research for hardware assurance.

