HIGH ASSURANCE SECURITY PRODUCTS FOR COMMERCIAL OF-THE SHELF (COTS) PLATFORMS

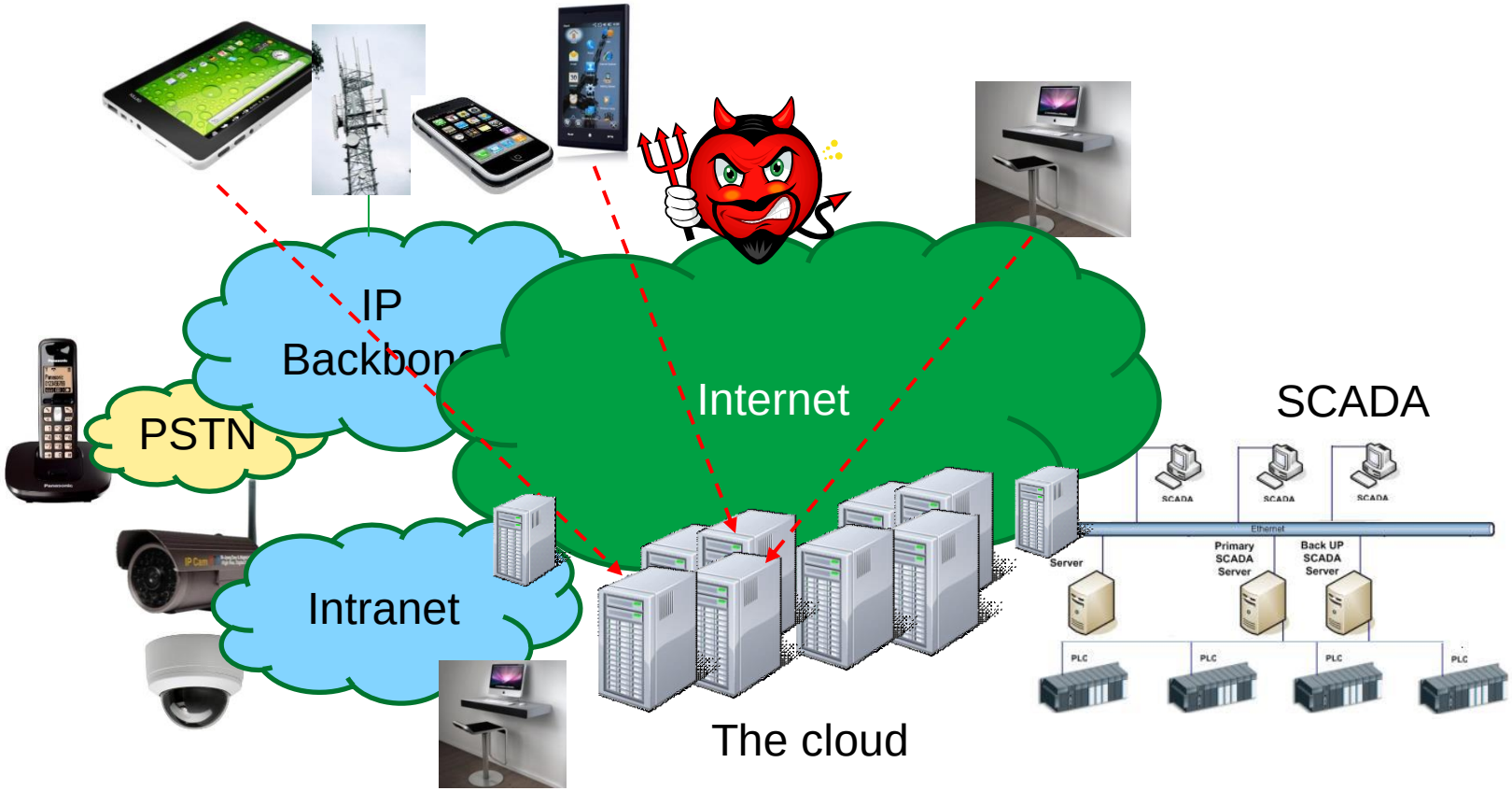
Christian Gehrmann
Lab Manager, Security Lab

SWEDISH ICT SICS

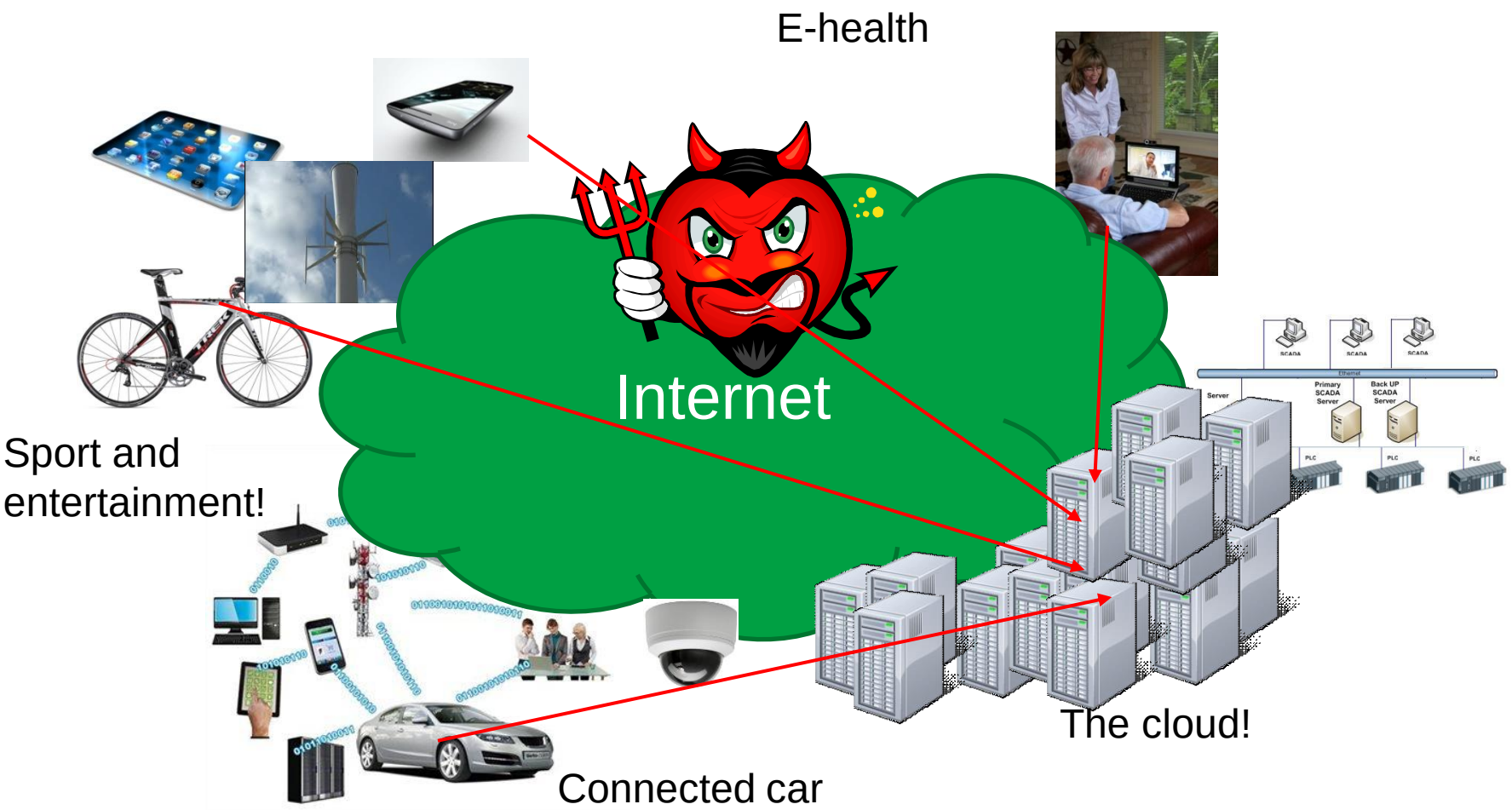
CONTENTS

- A changing security threat landscape
- Why security on COTS?
- The way to high assurance on COTS products
- An IoT scenario example
- The Swedish HASPOC project

HOW THE COMMUNICATION LANDSCAPE USED TO LOOK LIKE



WHERE WE ARE HEADING?

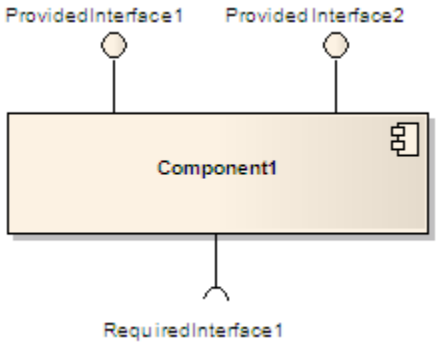


THE BIG CYBER SECURITY CHALLENGES

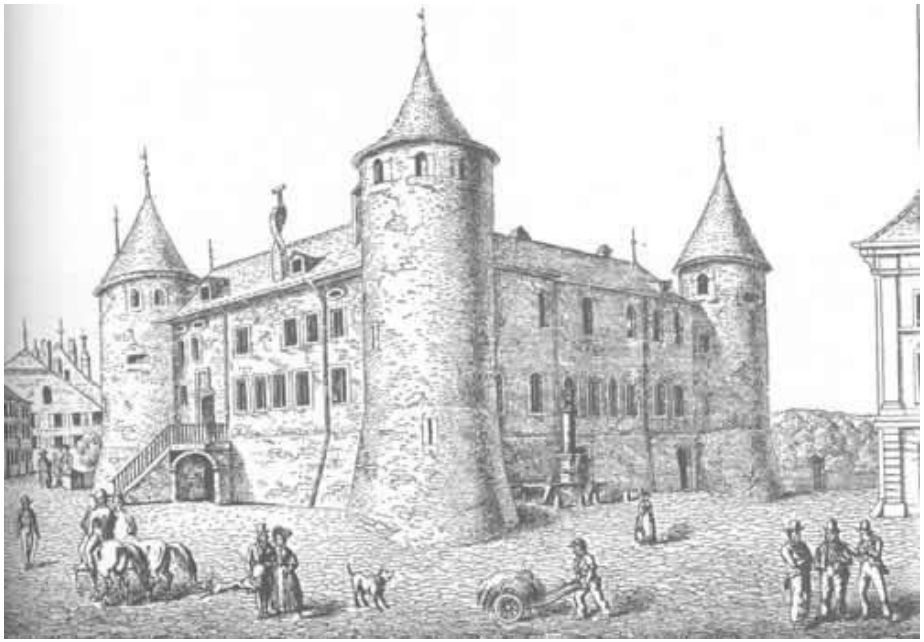
- As more and more systems get general internet connectivity, the different possibilities to disturbing them are growing
- The society is becoming more and more dependent on reliable IT solutions and hence more vulnerable to attacks
- The IT systems are getting more complex => more expensive and harder to make them robust and to protect them
- As many different system are connected and dependent on each other, a single attack on one component or a sub system can ruin the operation of many vital systems

HOW DO WE ACHIEVE HIGH SECURITY!?

- The systems are not more secure than the security of the system components!
  - BUT, the components typically
    - run SW from unknown sources
    - have several non-protected interfaces
    - are wrongly configured etc.



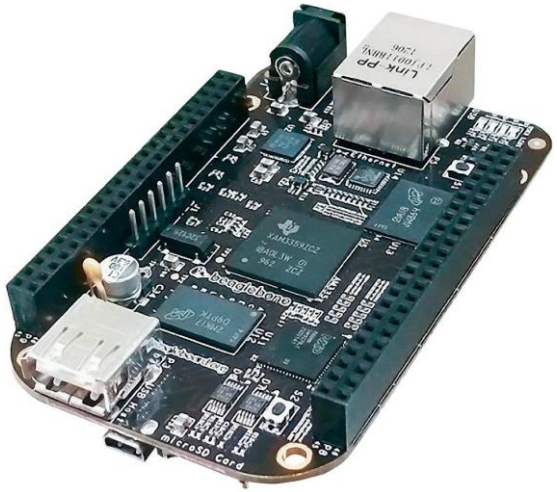
SECURE ISOLATION IS KEY



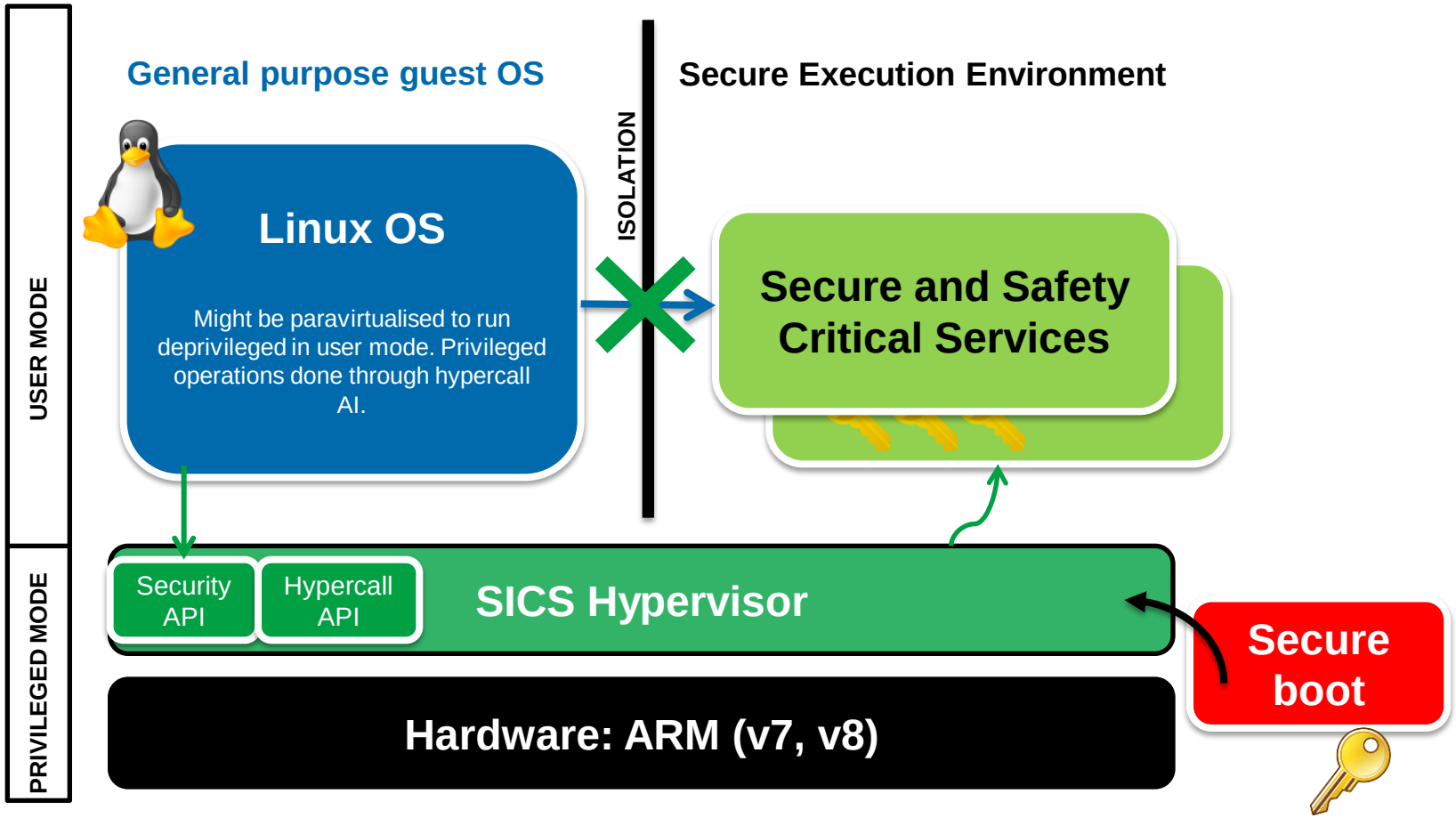
- By isolating the security critical parts of a system from the non-security critical parts a higher assurance level is achieved!

WHY COTS PLATFORMS?

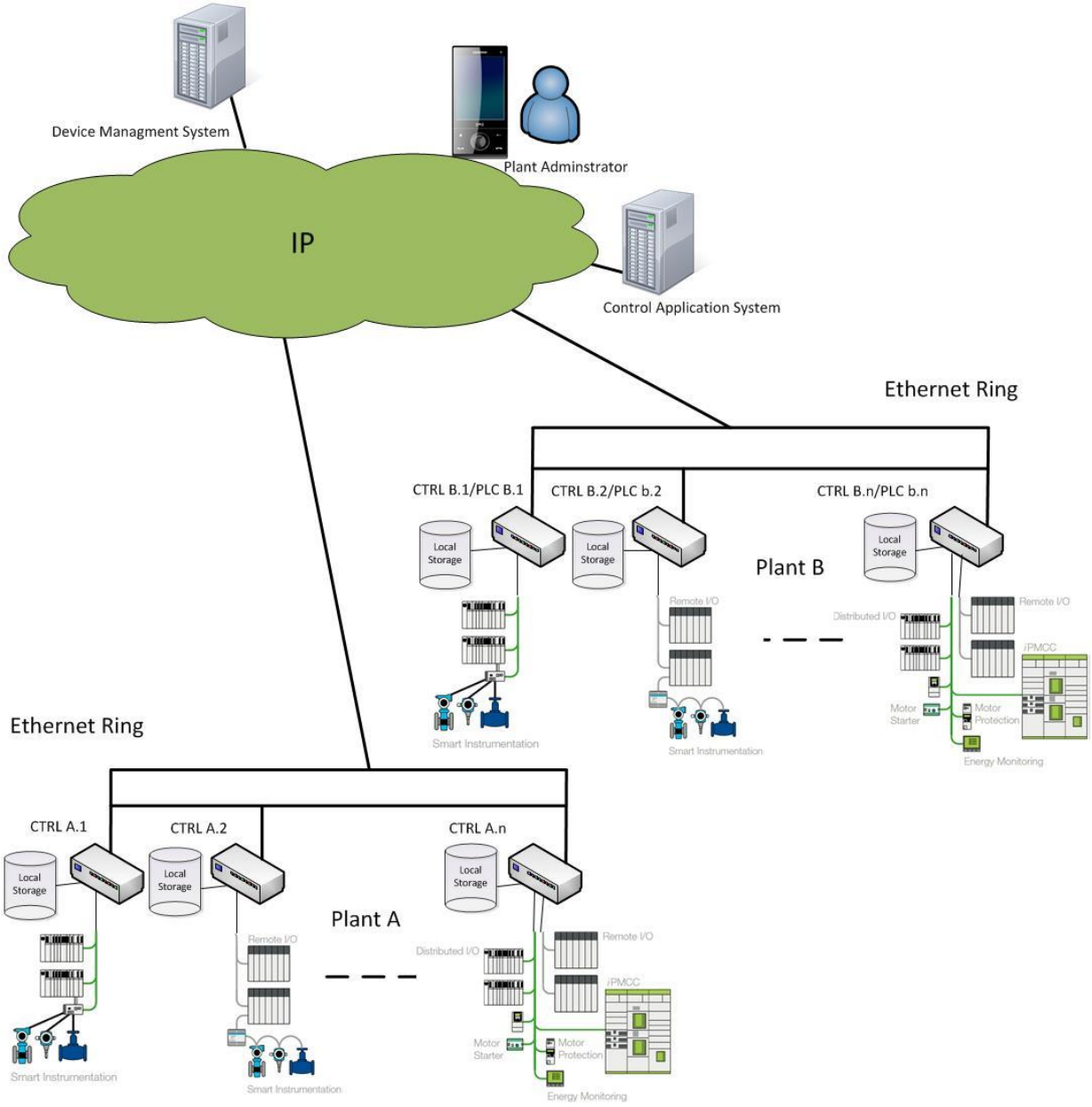
- The highest security is given by usage of special purpose hardware modules performing security critical tasks
- But, special hardware security modules are making the systems more expensive and requires substantial integration efforts
- Secure isolation on COTS have lots of cost benefits as long as we really are able to achieve *high security guarantees*



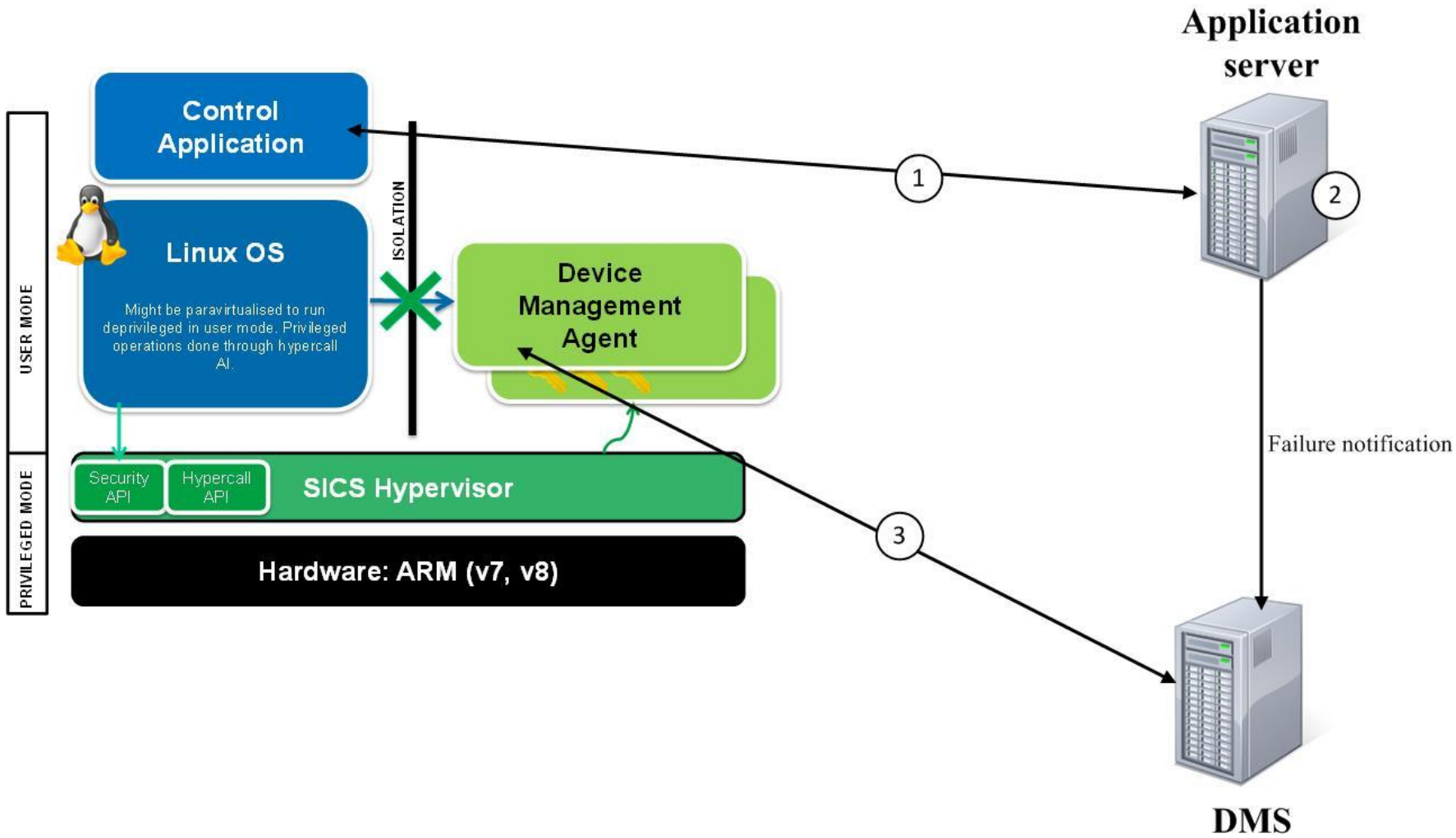
SECURE ISOLATION ON COTS PLATFORMS



AN IOT SCENARIO

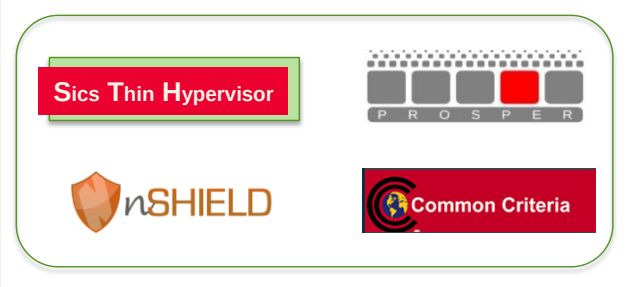


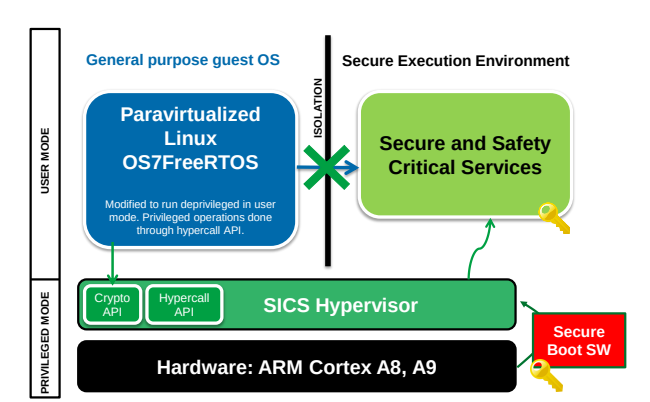
SECURE RECOVERY



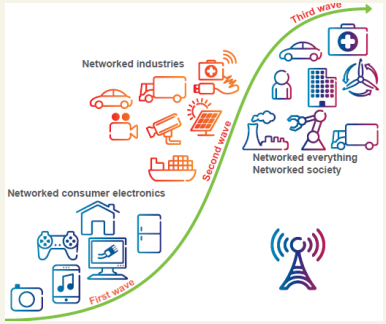
THE HASPOC PROJECT

High assurance security products on COTS platforms





Security for critical digital services and infrastructures



VINNOVA

SWEDISH ICT SICS

HASPOC PARTICIPANTS

Partners

Reference Group
Requirements Owners

Sponsored by