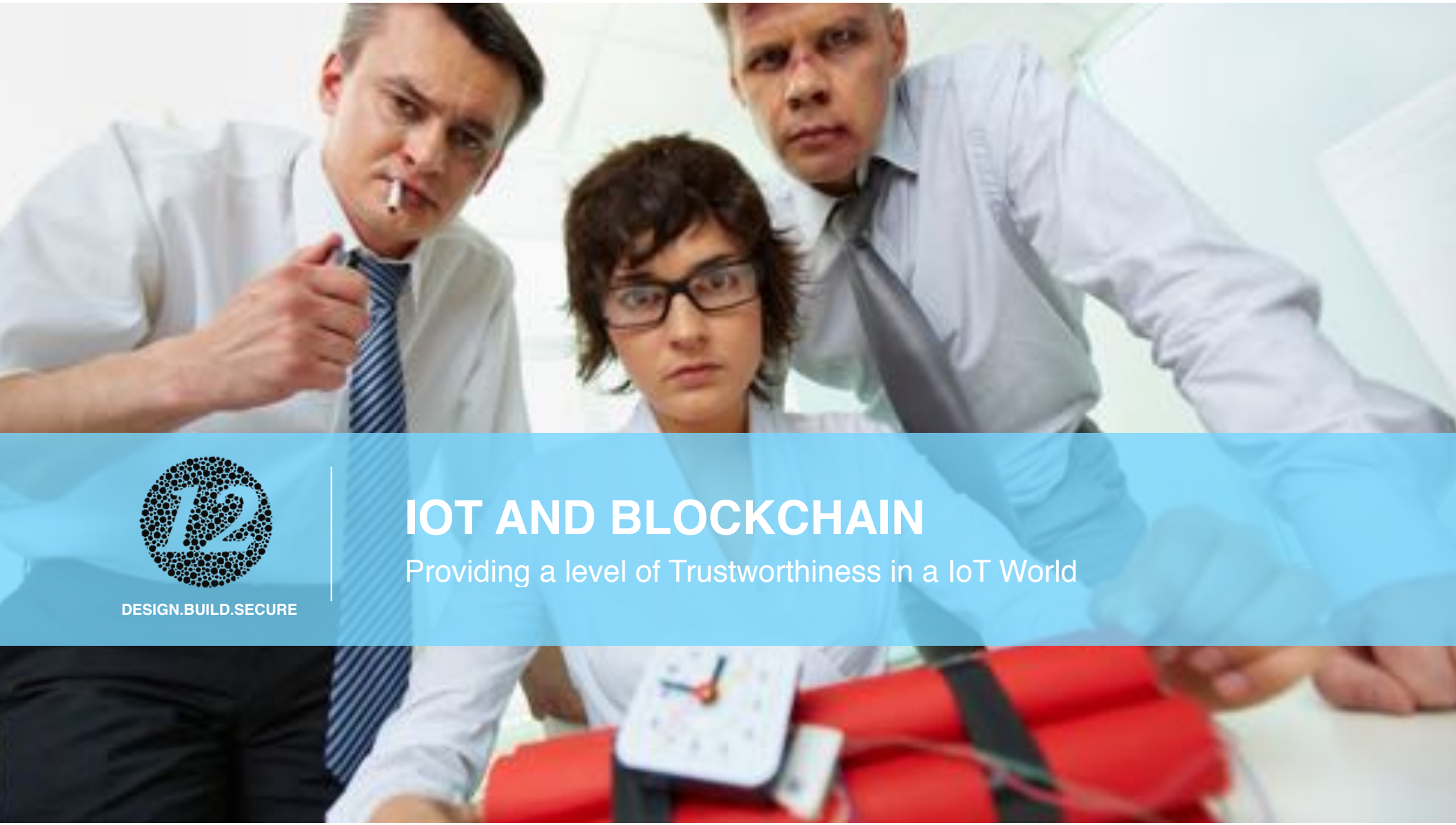


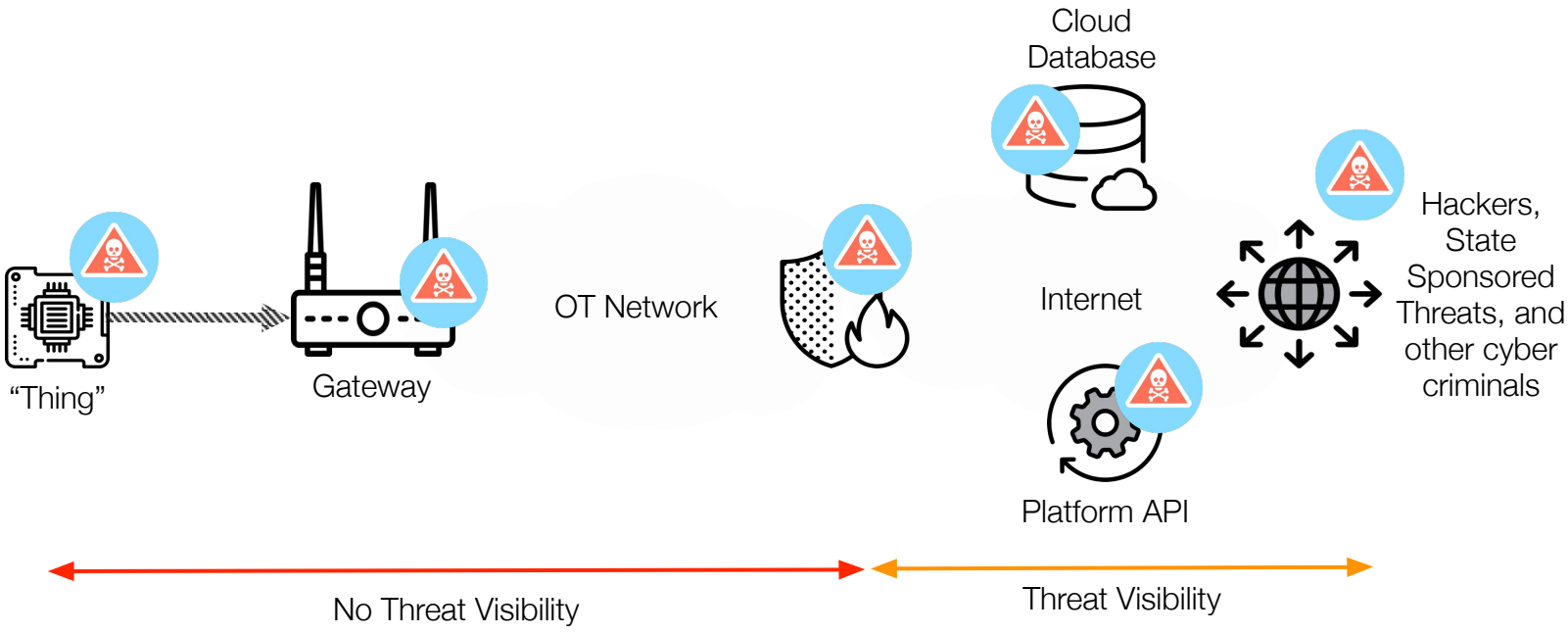
DESIGN.BUILD.SECURE

IOT AND BLOCKCHAIN

Providing a level of Trustworthiness in a IoT World

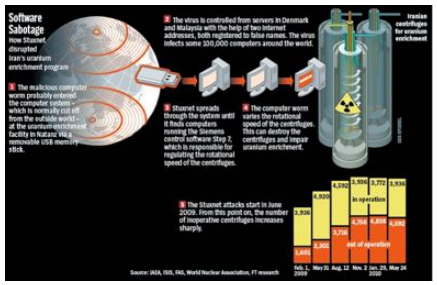

The IoT
Attack Surface

THE ATTACK SURFACE



IOT ATTACK TURNING POINTS

- Stuxnet
- Marai
- Vehicles
- Home Monitoring
- Medical Records



HOW THESE COULD OF BEEN PREVENTED

- Stuxnet - Policy and Threat Modeling
- Mirai - Design, Threat Modeling and Testing
- Automotive - Design, Threat Modeling and Testing
- Consumer Devices - Design, Threat Modeling and Testing
- Medical Records - Policy, Design, Threat Modeling and Testing


Standards Based
Approach

STANDARDS

- Don’t try to boil the ocean
- Why ISO/IEC?
- Determine what you need for your sector
- At a minimum consider:
  - IEC 62443 - for IIoT **
  - IEC 30141 - RA for IoT**
  - ISO/IEC 27000 Series for ISMS
  - ISO/IEC 27034 for Application Security
  - ISO/EIC 29134 for Privacy Impact Assessment

THE GOAL OF SECURITY

- Prove that your organization was not negligent
- Reduce product costs
- Reduce legal fees and possible legal action
- A higher level of assurance for end user
- Create trust between your solution and others in a network
- Competitive advantage

SECURING YOUR IOT SOLUTION

- Implement a Information Security Management System (**ISMS**)
- Create a **SDLC** that implements Secure Coding Methodology
  - Threat Modelling (What is the attack surface?)
  - Secure by Design (Runtime, Updating, Tamper resistance, monitoring, etc)
  - Source Code Evaluation
  - Understand your component supply chain
  - Test (TRA, Pen Test, VA at a minimum) for every major release

SECURING YOUR DATA

- With your ISMS you will know your data at **risk**!
- Ensure your **quality** of data - Integrity
- **Validation** of Data
- Realize that decisions must be **decentralized** vs. **asynchronous**
- You may want to consider a meta data approach

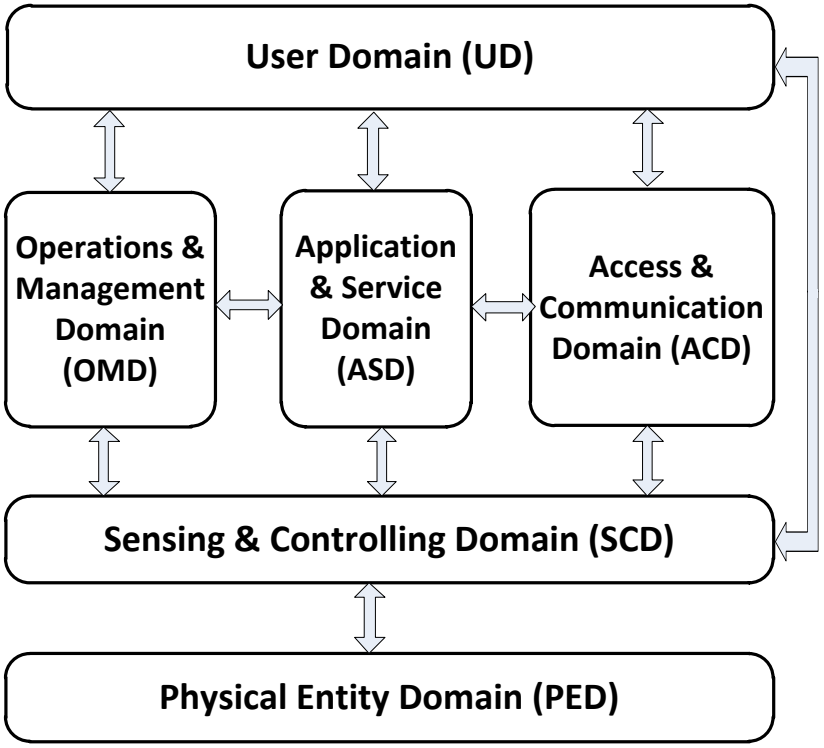
TRUSTWORTHINESS

- Deserving trust within the entire lifecycle of an IoT implementation to ensure **security**, **privacy**, **safety**, **reliability** and **resiliency**.


6 Domains and
Blockchain

6 DOMAIN APPROACH

KEY GOALS:
Communications
& Data
Exchange



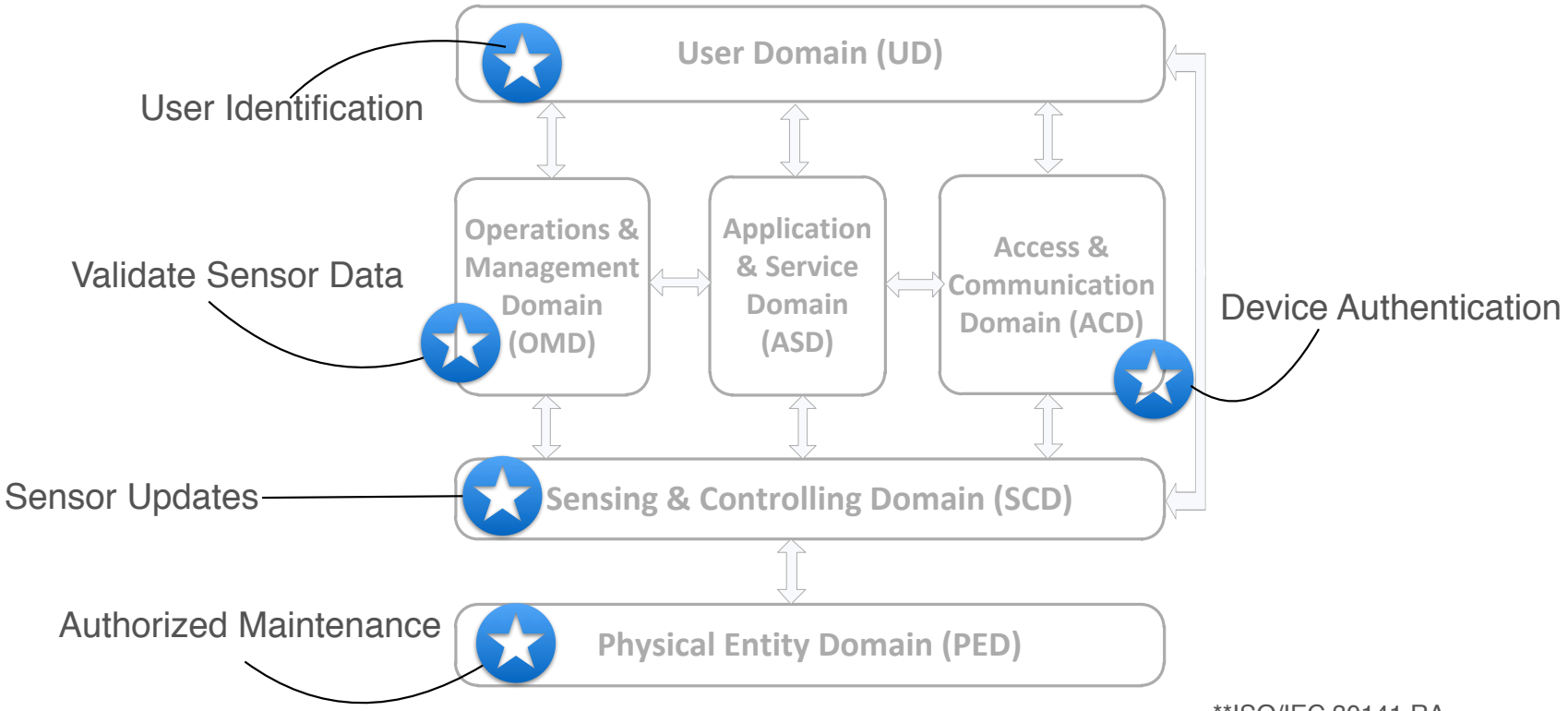
**ISO/IEC 30141 RA

BLOCKCHAIN AND DL

- Goals: Transactional Security and Operational Safety
- **Secure Transactions**
  - Tamper resistance from sensors
  - Secure updates of firmware
  - Authentication of new sensors
  - Communications from sensors to mgmt/ops
  - Communications from mgtm/ops to user
  - Operational trust between components at run time

Trust is a by-product of this process

APPROACH WITH BC AND DL



**ISO/IEC 30141 RA


Conclusions

HOW TO BE SUCCESSFUL AT IOT

- Change your company culture to be secure 1st
- Implement an ISMS
- Implement an SDLC
- Threat Model when designing
- Determine how BC/DL can implement trustworthiness
- Respect PII of your users
- Test, test, and test
- Have a breach plan

YOUR HOMEWORK

- Read:
  - SDChain White Paper
  - IEC White Paper IoT 2020: Smart and secure IoT platform
  - Purchase ISO/IEC 30141
- Get to know your data at risk
- Get to know your risk posture at any given time

THANK-YOU FOR YOUR TIME

faud.khan@twelvedot.com
@encrypto99
+1 613 447 3393

www.twelvedot.com
www.sdchain.io