

IoT Security Assurance Framework

Solving Technical & Commercial Challenges in IoT



RED ALERT LABS
IoT Security

- IoT Device Classes Security Profiles
- System Security Requirements Catalogue
- Process Requirements Catalogue
- Security Assurance Methodology

Our IoT Security Assurance Framework covers the whole IoT solution from Chip to Cloud and could be integrated at any stage or your IoT solution life-cycle.

It consists of a set of strategic and technical guidelines, security profiles, tools, catalogues of security requirements, a risk-based evaluation methodology for each type of IoT devices, based on standards when they exist.

CONSUMER (Electronic connected devices, Smart Home, etc.)

Protection against remote scalable attacks through external interfaces, Data Confidentiality, IP Protection, etc.

ENTERPRISE (Companies, Education, Finance, Retail, etc.)

Secure Firmware updates / Reprogramming and Remote Access Authentication, etc.

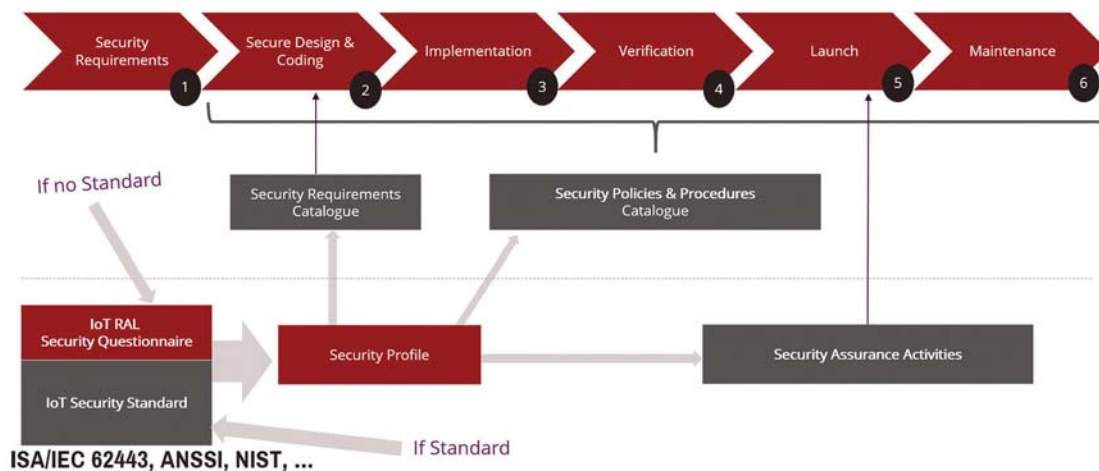
INDUSTRIAL (Manufacturing, Oil & Gas, Predictive Maintenance, etc.)

Local Internal Interface Access Enforced Authentication, Assets Availability, Communication Integrity, etc.

CRITICAL (Healthcare, Transportation, Military, etc.)

Firmware Integrity, Secure Booting and Physical Access Authentication, etc.

IoT Security Assurance Framework //



IoT Security Assurance Framework

Solving Technical & Commercial Challenges in IoT



RED ALERT LABS
IoT Security

What is a security profile and how is it used ? //

It is a dashboard of security requirements relevant to a class of IoT product/solution (e.g. gateway, thermostat, smart camera, RTU, etc.). This approach takes into account the type and sensitivity of the assets, the attacks likelihood and impacts in a specific operational environment (e.g. consumer, enterprise, industrial, critical) and the risk factor.

This is a step forward towards an economical way of dealing with security assessment. It sets up security checks and security policies to be staggered according to the identified risks, i.e. to concentrate efforts where the risks are highest.

Security profiles can be agreed upon and standardized for certain product classes.

Finally, a Security Profile is the result of a detailed risk analysis for each new product instance. It provides a risk-accepted standard security properties for a type of IoT product/solution

Go Back
Scope & Evaluation Identification Questionnaire: Solution Information
Go to Next Step

Others. Please specify:

3. Please rank these impacts by fears. Where 1 is the impact you fear the most and 5 you fear the least. Please select and move numbers in front of the impact text accordingly.

| | | Comments/precision |
|-----------------|---|---|
| Privacy | 5 | Example: disclosure of personal sensitive personal data (GDPR, consumer ID...) |
| Confidentiality | 1 | Example: disclosure of high value information, trade secrets, IP, mission critical data, master-keys, credentials, configuration data, internal data use... |
| Integrity | 3 | Example: changing of the system functioning, alteration of some features ... |

Remote Terminal Unit, (RTU)
Security Profile

| CATEGORY | Remote Terminal Unit (RTU) | DOMAIN | INDUSTRIAL | EDS/APP/PROT | SECURITY FEATURES |
|----------|--|--------|------------|--|---|
| USAGE | <ul style="list-style-type: none"> Collect Measurements from sensors Execute logic & control calculations Modify processes using control commands Communicate with external applications/devices Admin functions to configure RTU functionalities | | | <ul style="list-style-type: none"> No -Secured Physical Location Yes -Data-in-Transit encryption No -Admin Interface authentication No -Credentials & Cryptographic Keys protection No -Secured debug ports | <ul style="list-style-type: none"> Malformed input management Secure authentication on administration interface Access control policy Configuration access control Secure communication Command authorization Secure storage of secrets Secure Update Loss Integrity Secure Boot and Trusted Boot |

| Threat Id | Threat | Asset | Asset Value | Vulnerability | Impact | Likelihood | Total Risk | Security Goals | Security Functional Requirements | Security Assurance Requirements |
|-----------|--|----------------------|------------------------|--|--------|-------------|-------------|---|---|---------------------------------|
| T_FMN_01 | Modifying the configuration of the RTU | Device Configuration | RTU Configuration Data | WEAK AUTHENTICATION IMPROPER ACCESS CONTROL | Severe | Very Likely | SUBSTANTIAL | SECURITY DATA MANAGEMENT, IDENTIFICATION & AUTHENTICATION | EIA_SF_10; EIA_SF_68; EIA_SF_89 | SEE SF_REQUIREMENTS |
| T_FMN_02 | Destroy, Remove or Steal RTU | Physical Device | RTU Hardware | IMPROPER PHYSICAL ACCESS CONTROL | Severe | Likely | SUBSTANTIAL | ACCESS CONTROL | EIA_SF_23; EIA_SF_24; EIA_SF_25; EIA_SF_26; EIA_SF_61 | SEE SF_REQUIREMENTS |

