# IoT Security Concerns and Renesas Synergy™ Solutions

Simon Moore
CTO - Secure Thingz Ltd

Secure. Thingz.
Simplicity through Security™

# Agenda

Introduction to Secure.Thingz.

The Relentless Attack on the Internet of Things

Building protection with Renesas Synergy™

Ensuring Integrity

Enabling Confidentiality

Safeguarding Availability

Summary

Q&A

# Introduction to Secure.Thingz.

## Focus on the specific security issues in rapidly evolving IoT space

Delivering secure platforms in IoT - from mobile to edge nodes

Close partnership with ARM and IMG

## Secure.Thinking. - Consultancy Services

Secure. Thinking.™
Secure. Thingz.
Consultancy Services

Working closely with Renesas on Synergy Platform

**Threat Analysis** – Right-sizing security for *your* application

**System Definition** – From SoC to Solution to deliver holistic approach to security

**Architectural Implementation** – Hardware and software architecture generation and implementation

**Design Audition & Self-Certification Methodologies** – Ensuring compliance and pen testing

## Secure.Deploy. – Manufacturing Secured

Secure.Deploy.™
Secure.Thingz.
Manufacturing Secured

High assurance & secure manufacturing framework

Leveraging high security TPM to deliver key material into contract manufacturers

# What is your strategy for IoT Security?

# Relentless Attacks On The IoT

# “Open season” on the IoT

Billions of devices and trillions of connections provide a huge security surface for attack

Systems are uniquely complex making a “one-size-fits-all” security solution impossible

Cyber attacks are highly profitable for cyber criminals

# Cyber attacks impact real lives

**Capture and Disrupt** attacks on cyber systems can obtain and control critical intelligence, such as propriety information,  without detection

**Manipulation** attacks can take over control of IoT entities that wreck havoc on broad, dynamic system operations

**Privacy / Confidentiality** attacks on users and smart connected objects pose critically high risks to safety, security and privacy

Failure of Industrial Systems

Transportation Gridlock

Personal Identify Theft and Credit Fraud

Life Endangerment

# Cyber warfare is now pervasive

7 JUL 2014 | NEWS

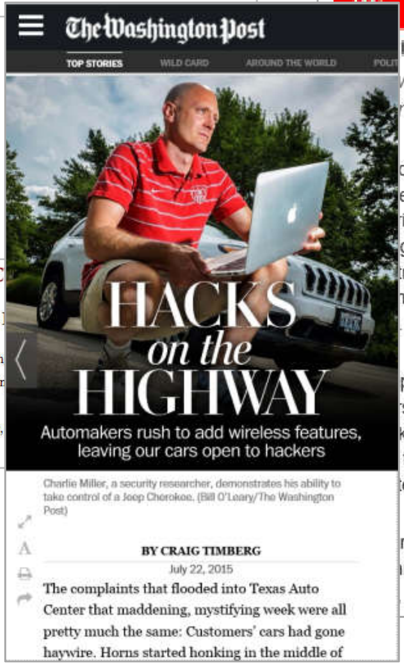
For the Internet of Things, Even a Connected Lightbulb is a Threat

The internet of things (IoT) has been described as creating a coming tsunami of data, as everything from toilets to microwaves get connected. But it's also a security "wave of terror" in some respects as every new connection threatens to be a portal for cybercriminals. For instance, researchers at Context Information Security have been able to expose a security weakness in that most generic of home and enterprise possessions: the lightbulb. Specifically, a Wi-Fi-enabled, energy-efficient LED light bulb that can be controlled from a smartphone.

ENGINEERING.COM ELEC
THE GUTS BEHIND THE GADGETS

Beware of Internet of Things

Recently, HP announced a study concludin
over 70% of devices on the Internet of Thin
have serious vulnerabilities, including
encryption, password, cross-site scripting,
access and permission.



The Washington Post

HACKS on the HIGHWAY

Automakers rush to add wireless features, leaving our cars open to hackers

Charlie Miller, a security researcher, demonstrates his ability to take control of a Jeep Cherokee. (Bill O'Leary/The Washington Post)

BY CRAIG TIMBERG

July 22, 2015

The complaints that flooded into Texas Auto Center that maddening, mystifying week were all pretty much the same: Customers' cars had gone haywire. Horns started honking in the middle of

SC MAGAZINE

IT SECURITY PROFESSIONALS

Stuxnet-style attack on US smart grid could cost government $1 trillion

*y report into the insurance implications of a wide-scale cyber-attack on the US energy r reveals just how costly the breach would be for government and insurers.*

oyds 'Business Blackout' report was co-
ed by the insurer and the University of
ridge Centre for Risk Studies, whilst also
g the advice of the Cabinet Office, the
tment of Homeland Security and security
ncluding IOActive and Context, among many
.

port sets out a scenario where a group of
rs, using the Erebos Trojan, seek to infect
ke offline electricity generation control
to introduce an electricity black-out across
tes including New York and Washington.

Stuxnet-style attack on US smart grid could cost government $1 trillion

rchers said that the attack, 'improbable' but 'technologically possible', would likely result in huge
ment and insurance pay-o s ports shut
, a disruption to water supp t networks.

InformationWeek DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

How I Hacked My Home, IoT Style

INTERNATIONAL BUSINESS TIMES

FRIDAY, AUGUST 29, 2014 AS OF 6:41 PM EDT

'Internet Of Things' Very Susceptible To Hacking, Study Shows

By Luke Villapaz @lukeydukey l.villapaz@ibtimes.com
on August 04 2014 11:29 AM

VentureBeat

Hackers could use 'The Internet of Things' to turn everyday devices into paths of attack

CNN

Connected TVs, fridge help launch global cyberattack

By Brandon Griggs, CNN
January 17, 2014 -- Updated 2252 GMT (0652 HKT) | Filed under: Gaming and Gadgets

# Enabling IoT Security with Synergy

# Delivering next-generation security capabilities

Integrity framework delivers a strong root of trust

Robust availability enables integrated device lifecycle management

Confidentiality (privacy) of intellectual property and data

Protect Intellectual Property

Protect Data In Flight & At Rest

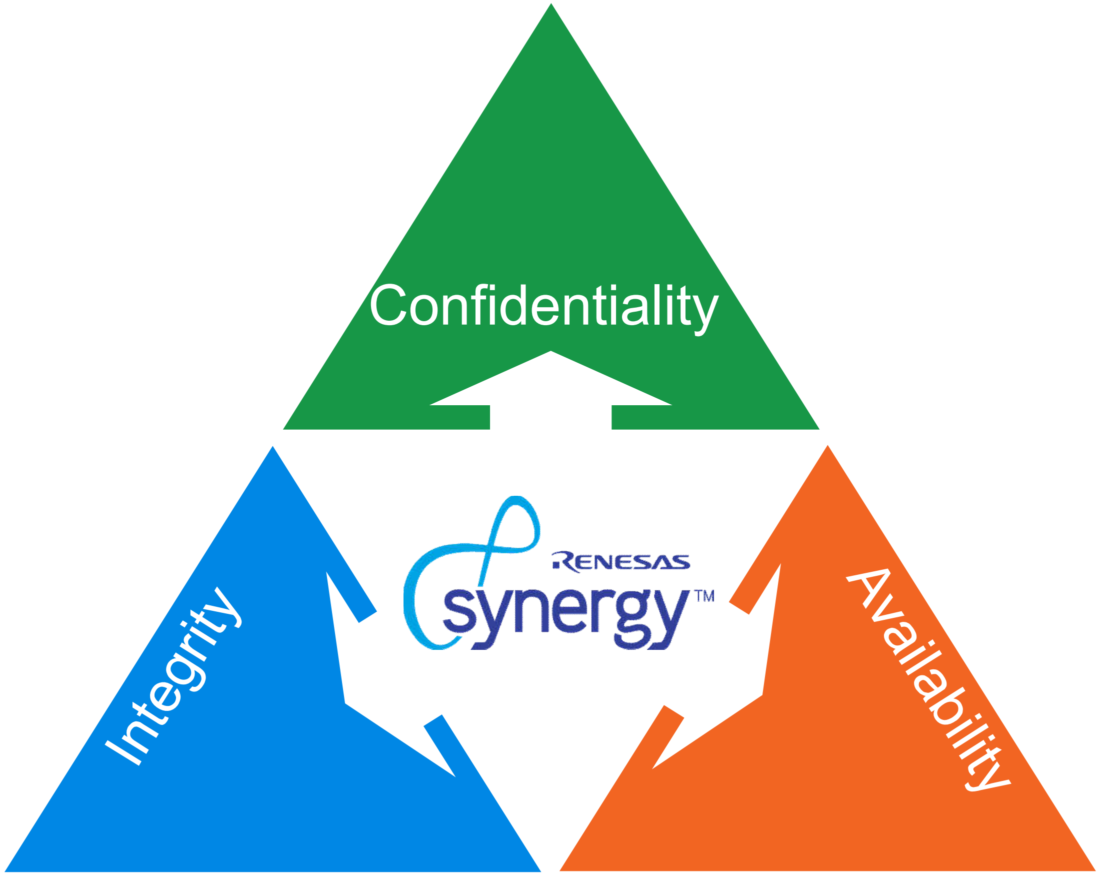
Create Robust Foundations

Separate Critical & Other Functions

Manage Device Lifecycle

**Integrity** | **Availability** | **Confidentiality**

# Critical components of security



# An integrated solution for higher security

## Confidentiality

**Increased protection of data**

- Security across the portfolio
- High performance accelerators including asymmetric crypto
- Smaller code base
- Tightly integrated to protect secrets and prevent leakage

## Integrity

**Delivering a new level of trust**

- Integrated Root of Trust ensures platform protection
- Constrained and measureable boot to inhibit low level attacks
- Isolation of critical code to restrict impact of attacks

## Availability

**Security across the lifecycle**

- Isolation of critical system to promote uptime
- Enables ongoing monitoring and management of functionality before, during and post attack
- Platform for lifecycle management and secure updates

# Ensuring Integrity

# Integrity – the critical foundation to security

Confidentiality is reliant on a high integrity platform because *cryptography is insufficient* on it own

Traditionally embedded systems were “islands” of very narrow levels of connectivity

IoT solutions are naturally widely connected to enable complex system definition

Security requires a high integrity platform

# Verifiable Root of Trust

## Strong Cryptographic Identifiers

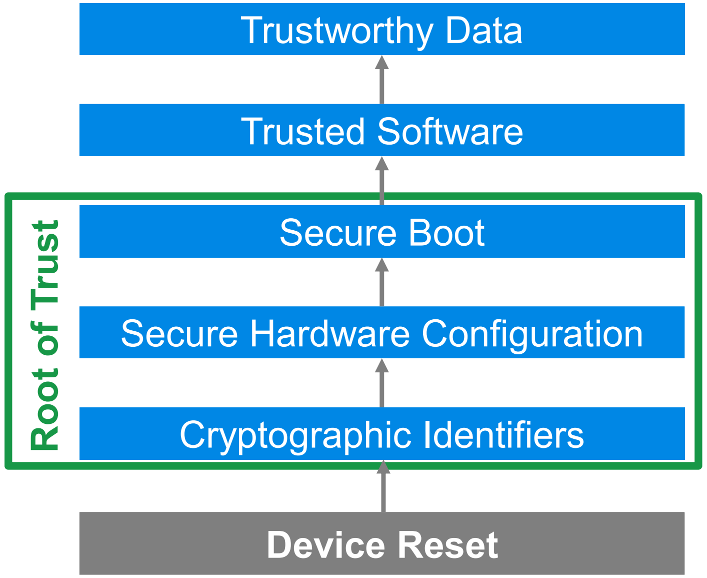
- Synergy Security Engine integrate the True Random Number Generator (TRNG) to create & protect unique identifiers
- Derivation and storage of keys within custom security engine

## Secure Hardware Configuration

- Delivers extensive secure memory partitioning
- Robust defences activated prior to secure boot execution
- Inhibits root-kit attacks

## Secure Boot foundation for trusted software

- Only trusted software installed and executed
- Quick and secure software authentication utilizing Synergy security accelerators


Trustworthy Data

Trusted Software

Root of Trust

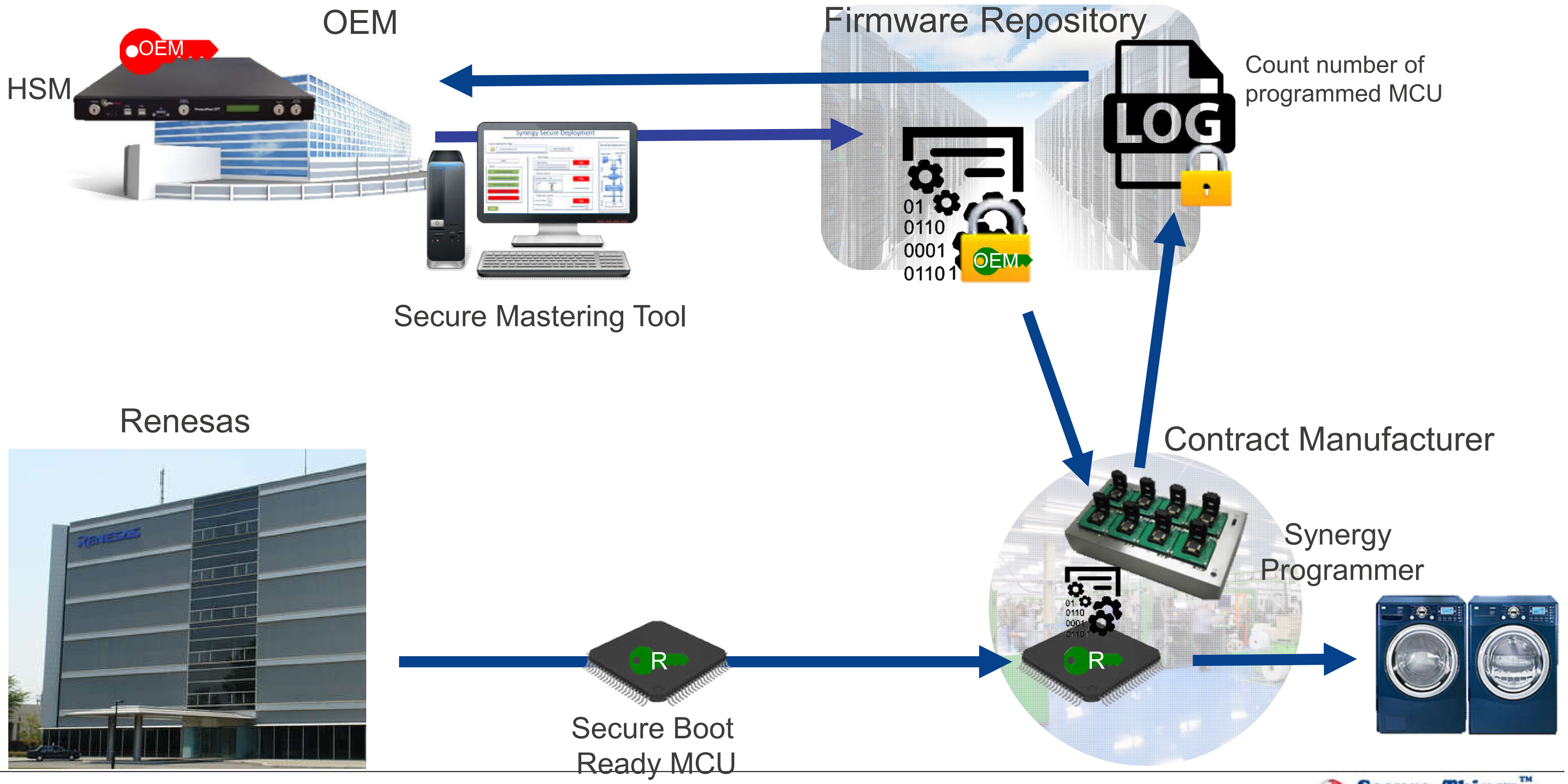
Secure Boot

Secure Hardware Configuration

Cryptographic Identifiers

Device Reset

# Trusted Manufacturing – at Contract Maufacturer



# Secure Mastering Tool

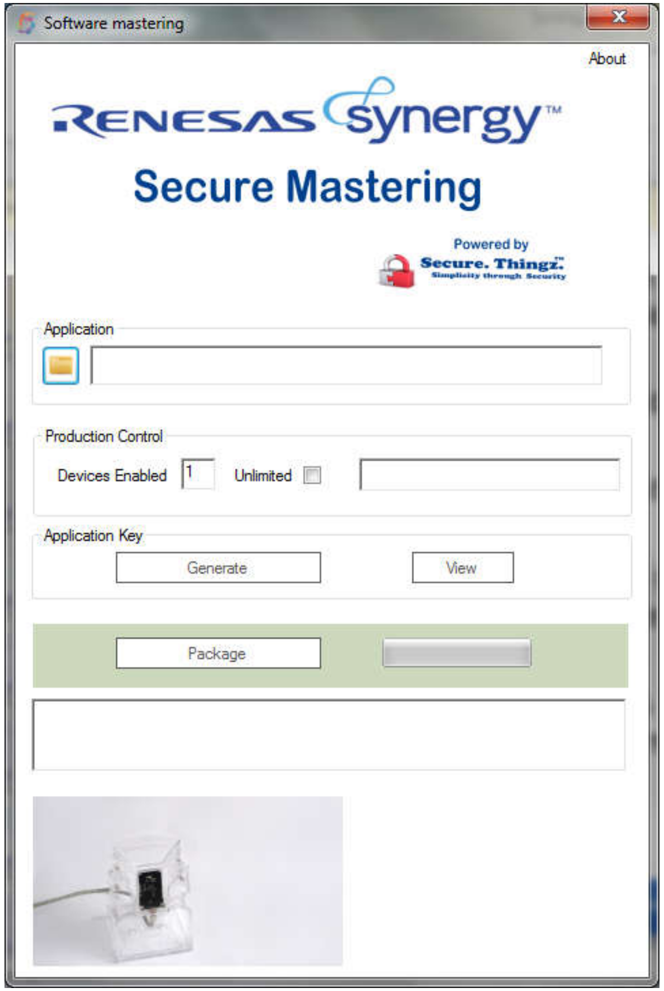
Secure Mastering Tool is a PC tool that responsible for securely packaging Firmware modules

Encrypt Firmware binary and signs with OEM's certificate

Encryption Key managed securely

Capable of controlling the maximum number of devices that the firmware can be programmed

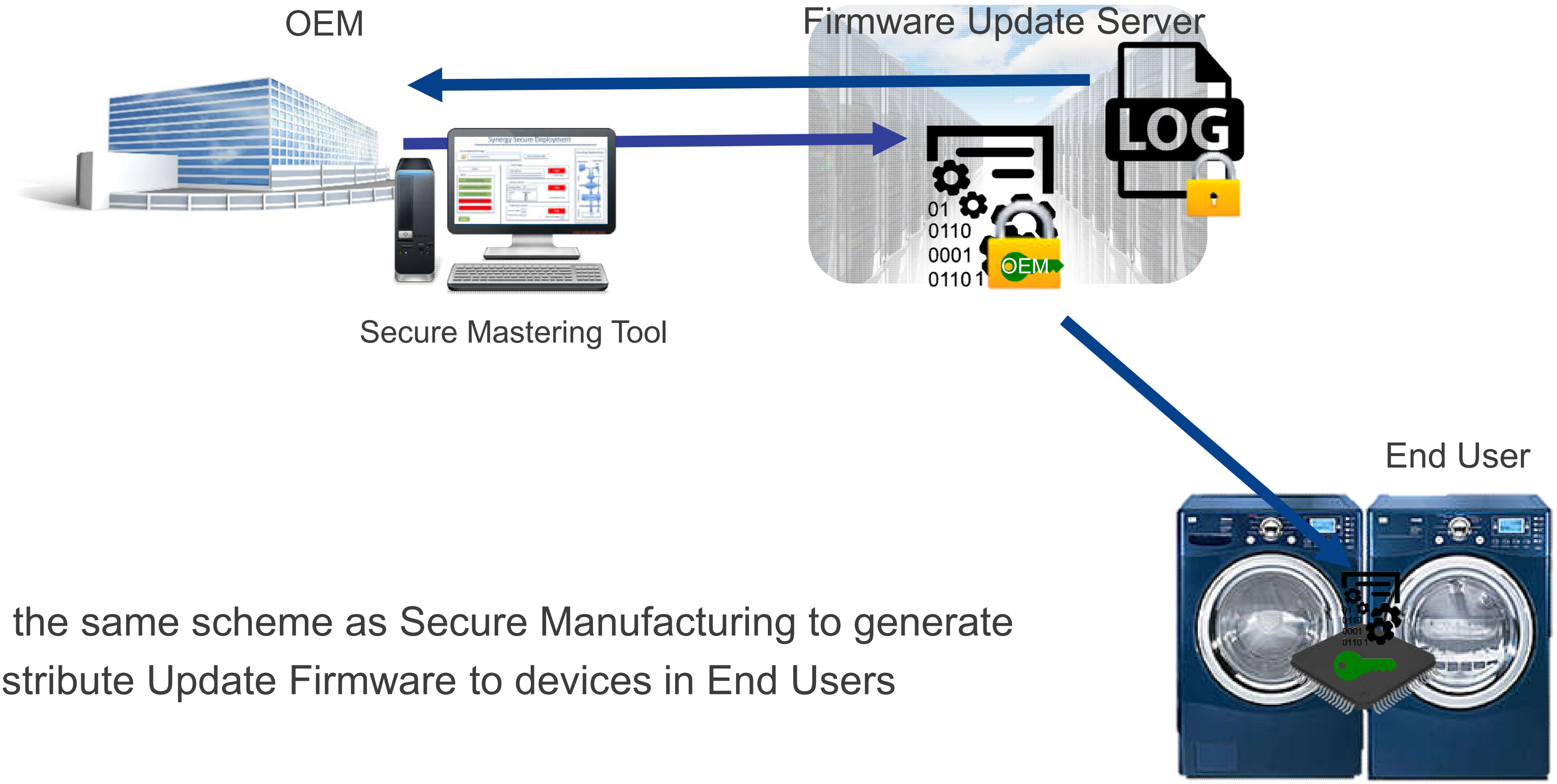
Synergy Programmer limits the programming devices based on this information



Devices Enabled 1

Unlimited □

# Secure Firmware Update



OEM

Firmware Update Server

Secure Mastering Tool

End User

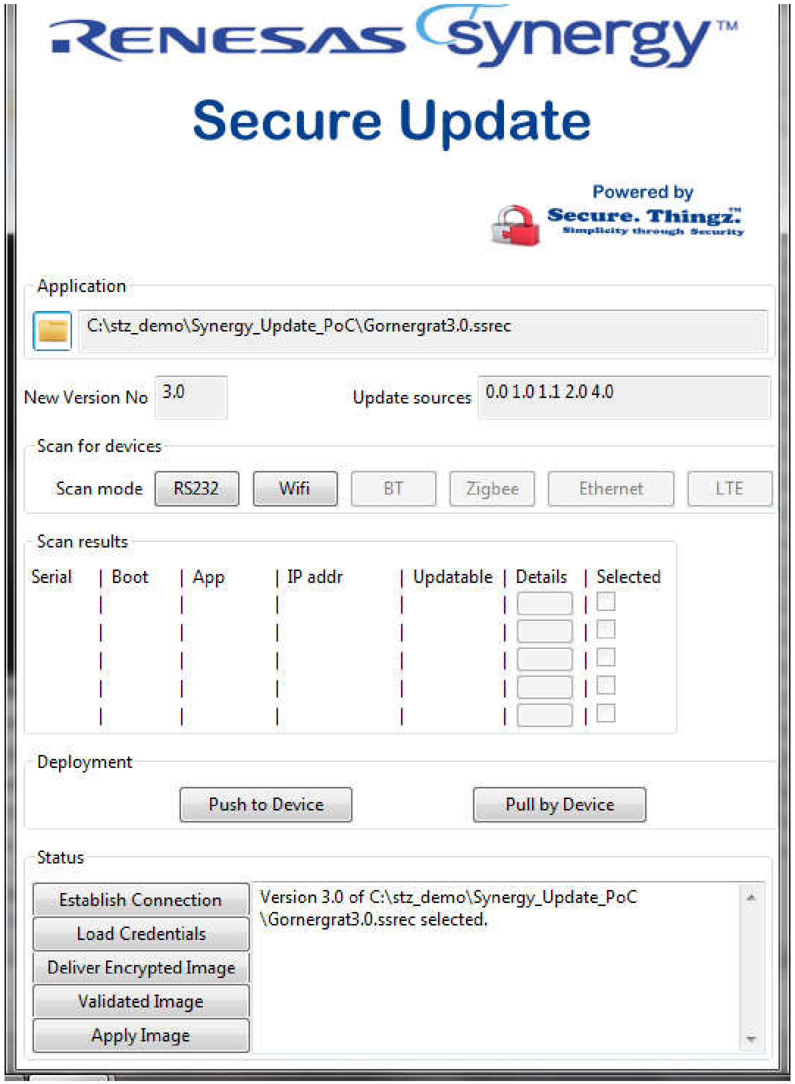
Utilize the same scheme as Secure Manufacturing to generate and distribute Update Firmware to devices in End Users

# Secure Update Deploy Tool

Manages the secure update of firmware onto devices

Uploads Signed Firmware modules that are generated by the Mastering Tool

Can specify distribution policy, target device groups that the update binary is distributed to



Application: C:\stz_demo\Synergy_Update_PoC\Gornergrat3.0.ssrec

New Version No: 3.0

Update sources: 0.0 1.0 1.1 2.0 4.0

Scan results

| Serial | Boot | App | IP addr | Updatable | Details | Selected |
|---|---|---|---|---|---|---|
| | | | | | | ☐ |
| | | | | | | ☐ |
| | | | | | | ☐ |
| | | | | | | ☐ |
| | | | | | | ☐ |

Version 3.0 of C:\stz_demo\Synergy_Update_PoC \Gornergrat3.0.ssrec selected.

# Enabling Confidentiality

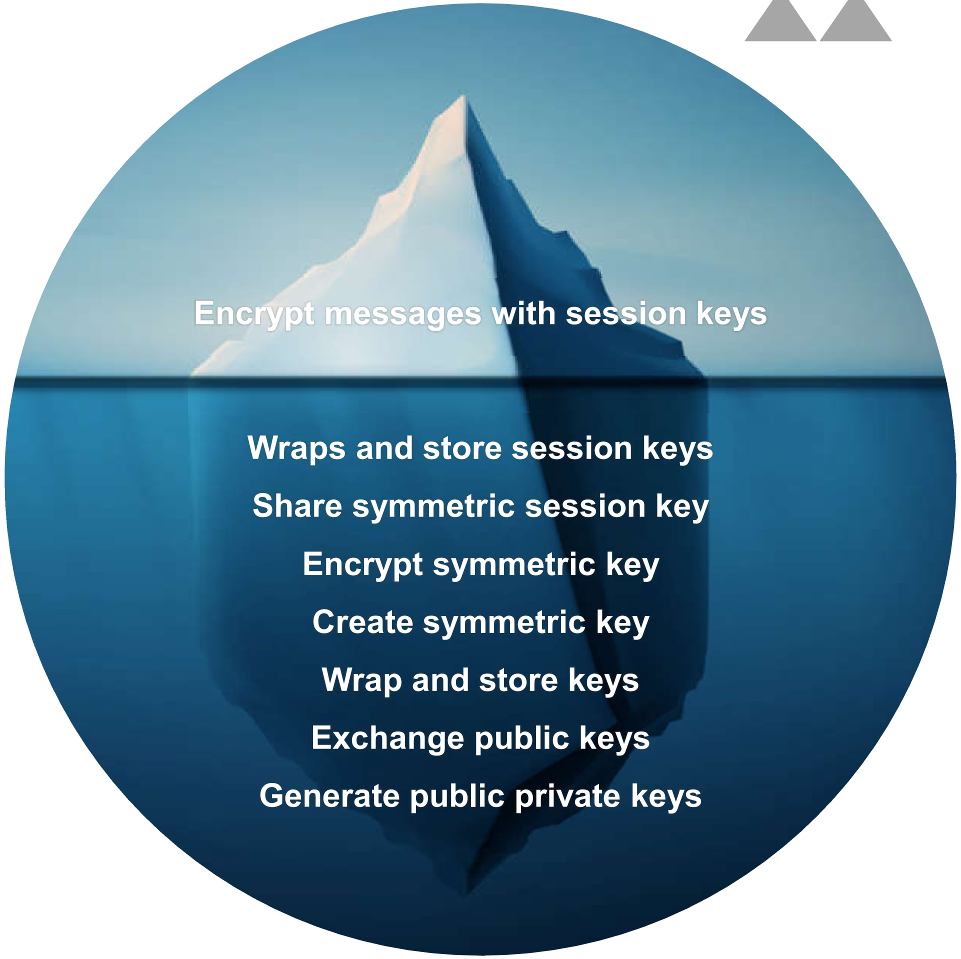
# Confidentiality: Security beyond privacy

## Confidentiality is critical in all IoT systems

- Privacy of data – Inhibit covert monitoring
- Trust of data – Ensuring data is trustworthy is the foundation of Big Data

## Confidentiality is fundamental in conveying data

- Encryption and decryption of messages are the 'tip of the iceberg'


Encrypt messages with session keys
Wraps and store session keys
Share symmetric session key
Encrypt symmetric key
Create symmetric key
Wrap and store keys
Exchange public keys
Generate public private keys

# Synergy – Enabling Confidentiality

## True Random Number Generator

- High-entropy TRNG is the cornerstone of all encryption.
- Meets highest NIST 800-90 standard

## HASH Accelerator

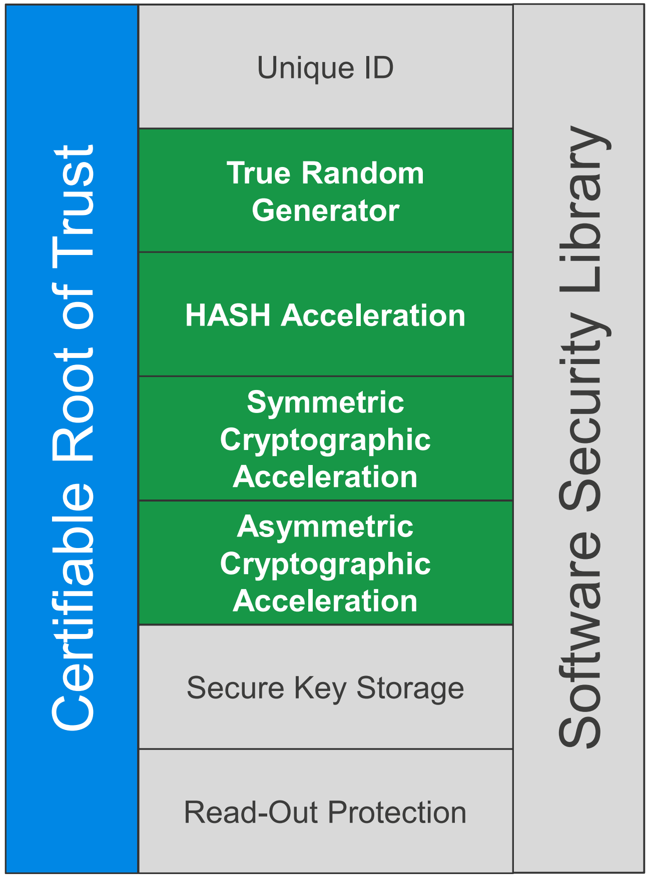
- Critical for authenticating communications and other information

## Symmetric Cryptographic Accelerator

- Industry standard symmetric cyphers accelerated. Includes broadest library of AES modes and 3DES
- Enables rapid encryption and decryption of messages

## Asymmetric Cryptographic Accelerator

- Integrated hardware significantly accelerates asymmetric cyphers. Includes ECC and RSA primitives
- Increased security and minimized computational overhead



Certifiable Root of Trust

Unique ID

True Random Generator

HASH Acceleration

Symmetric Cryptographic Acceleration

Asymmetric Cryptographic Acceleration

Secure Key Storage

Read-Out Protection

Software Security Library

# Safeguarding Availability

# The challenges to maintaining system availability

### A cyber attack is not a “if”, it is a “when”

- Capability of attackers evolving rapidly
- Value of attacks growing
- Number of systems exploding

### Cyber attacks are prolonged and pervasive

- Presume that something in the trusted network is compromised
- Attacks may be silent for months or years
- Blacklisting of known compromises is not sufficient

# What True Availability Requires

### Isolation of system components

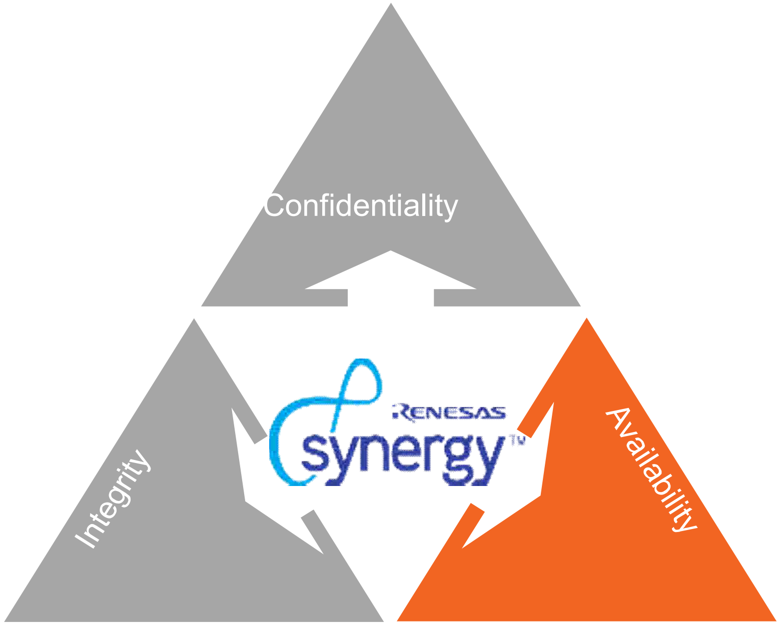
- Isolation of flaws
- Simplify components to enable testing and validation

### Awareness and communication

- Monitoring and analysis of the system
- Cryptographic measurements of status

### Recovery and remediation

- Isolate and replace compromised components
- Update and manage the system over the full life cycle



# Enabling Reliable System Availability

## Synergy supports multiple Memory Protection Units (MPU)

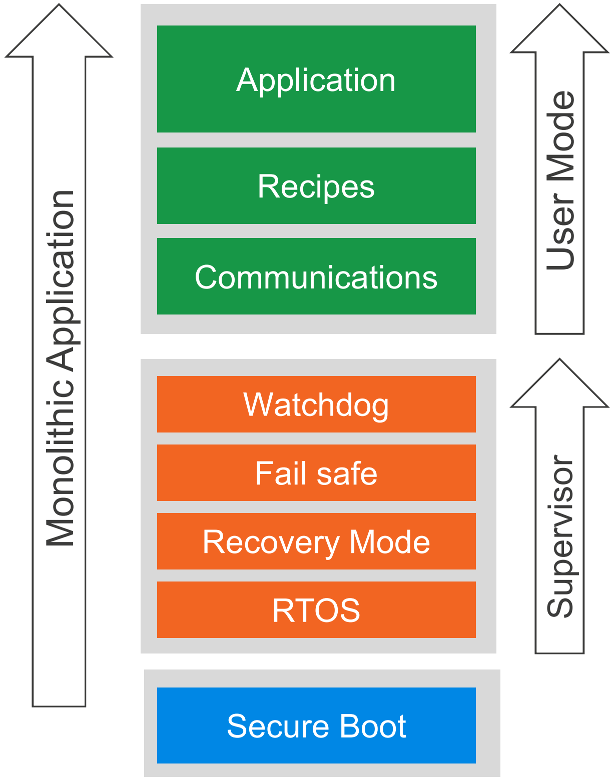
- Extends traditional ARM MPU model
- Enables separation of application and critical functions
- Ensure watchdogs can monitor system resources

## Secure Boot validates application software

- Ensures correct code installation and execution
- Protect against injection attacks using cryptographic HASH

## Structured recovery capabilities after successful attacks

- Reset of device
- Verify device status
- Managed encrypted code download
- Re-flash of device to remove infected components



# Building More Secure Systems

- **Security cannot be an afterthought**
  - What do you need to protect
  - What is the impact – catastrophic failure, data leak, brand damage
- **Cryptography is not sufficient on its own**
  - Requirement to secure the device
  - Understand how you recover the device
- **Leverage the right tools and industry best practice**
  - Synergy has security in its DNA – Confidentiality, Integrity & Availability
  - Synergy Booth – Implementation of Secure Boot & Deployment
  - Leverage emerging standards groups – IoTSecurityFoundation.org

# Summary

# Synergy – Enabling next-generation security

## Real defense capability against cyber threats

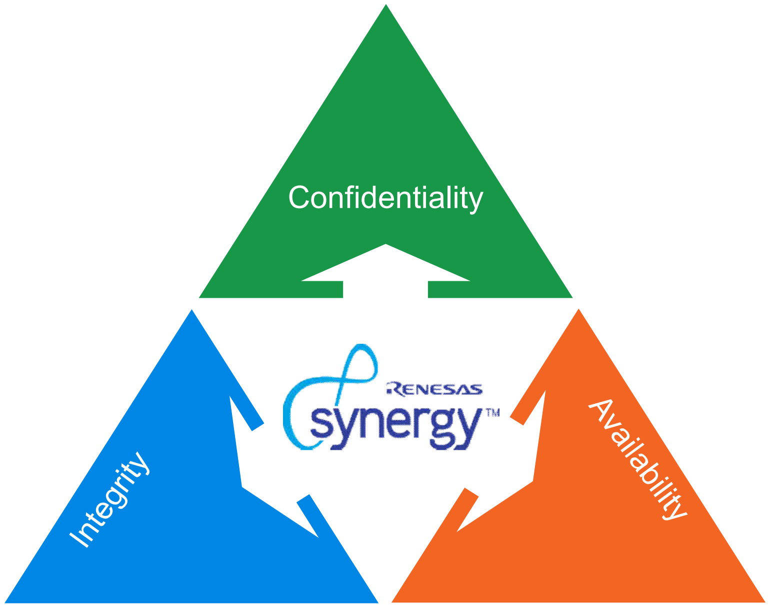
- Asymmetric and Symmetric Cryptography Accelerators
- True Random Number Generator
- HASH Accelerators
- Secure Storage

## Security that meets every challenge

- Integrity – Security of the device from Reset
- Confidentiality – Authentication of multiple devices and users
- Availability – Poised for system compromise and ready for remediation

## Don’t let attackers win

- Could your organization recover from a successful attack?
- Is your system secure against the next-generation of cyber attacks?
- Could you design a successful attack of your own system?
- What is your information worth?



# QUESTIONS

Secure. Thingz.
Simplicity through Security™