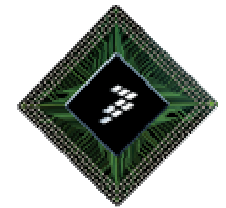




October 2008

Embedded Security - Safety

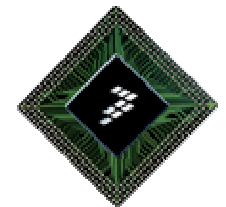


Mats Henriksson
FAE

Freescale™ and the Freescale logo are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners. © Freescale Semiconductor, Inc. 2006.

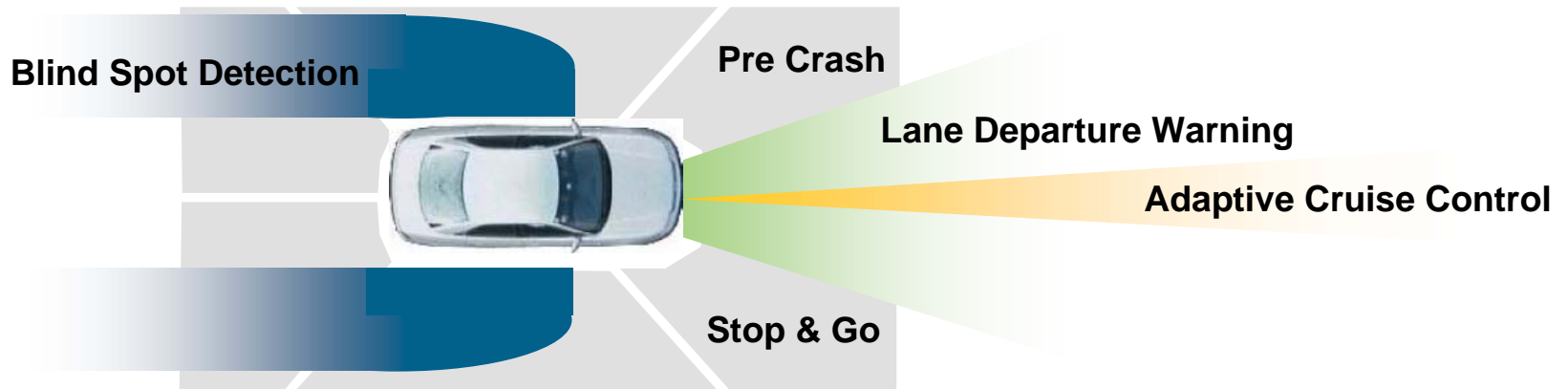


Introduction - Why Security why Safety?



Driving Toward Advanced Driver Assistance

Application	Description	Sensor
Adaptive Cruise Control:	A system to automatically control the speed of an automobile with awareness of other vehicles and obstacles.	Radar Lidar Camera
Pre-Crash	A system to detect an imminent collision and prepare on-board safety systems in advance.	Radar Lidar Camera
Blind Spot Detection	The system that alerts drivers to the presence of vehicles in their blind spot. When the driver is preparing for a lane change or backing up.	Radar Camera
Backup	Warning System is designed to detect the presence of obstructions behind a vehicle and warn the operator.	Radar Camera
Active Front Lighting	A system to increase driver visibility at night by dynamically altering the headlight beam's direction and intensity.	Camera (Low)



Remote Convenience Store Robberies

Thieves Hacking Security Cameras?

Journal written by [Erris \(531066\)](#) and posted by samzenpus on Thu Aug 30, 2007 08:04 AM
from the steel-from-home dept.

The [FBI is investigating fifteen store robberies in eleven states](#), committed via phone and internet. The perpetrators hack the store's security system so they can observe their victims. They then make customers take their clothes off and get the store to wire money. From the article,

"A telephone caller making a bomb threat to a Hutchinson, Kan., grocery store kept more than 100 people hostage, demanding they disrobe and that the store wire money to his bank account. ... officials were investigating whether the caller was out of state and may have hacked into the store's security system. "If they can access the Internet, they can get to anything," Hutchinson Police Chief Dick Heitschmidt said. "Anyone in the whole world could have access, if that's what really happened."



Best Buy confirms it sold virus-infected Insignia photo frames, no recall in the works

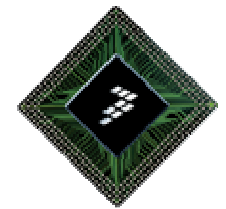
Posted Jan 24th 2008 9:46AM by Paul Miller

Filed under: Household



As we noted a week back, [Best Buy's](#) house-brand [Insignia](#) photo frames are [indeed virus-infected](#), but now it appears Best Buy is doing something about it. Unfortunately, info is still slim at the moment from company lips. Best Buy says it's "connecting with our customers who may have been impacted," and has pulled remaining inventory from the shelves, but there are no plans for a recall of the infected NS-DPF10A, and Best Buy won't specify what specific type of malware we're dealing with. Best Buy seems to think that anti-virus software should have no problem dealing with the old-ish trojan in the frames, and recommends customers plug the frame into a PC and run some current anti-virus software to eradicate the malware. Macs are unaffected, and Apple could be seen on the playground [making smarmy remarks](#) about the incident to anyone who'd listen.

What Requires Protection?



Functional Safety Standards

IEC61508 (Functional safety of electrical/electronic/ programmable electronic safety-related)

- Safety Integrity Levels (SILs)

 - SIL1: Minor injury

 - SIL2: Serious permanent injury to one or more persons; death to one person

 - SIL3: Death to several people

 - SIL4: Very many people killed

IEC26262 - automotive derivative of IEC61508

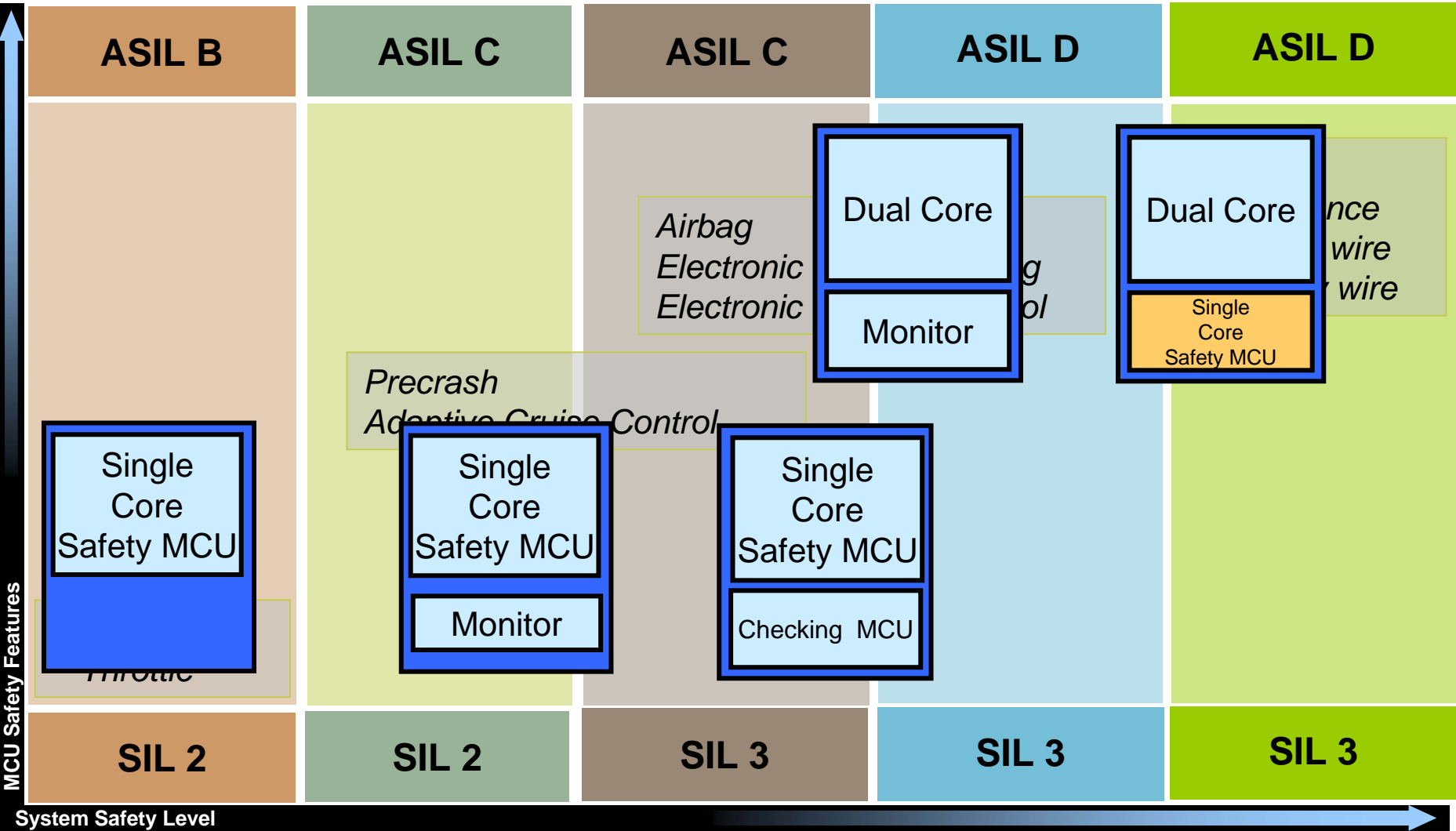
- Published by FAKRA (Normenausschuss Kraftfahrzeuge, part of german VDA)

- Planned schedule

 - working document (WD) 2006

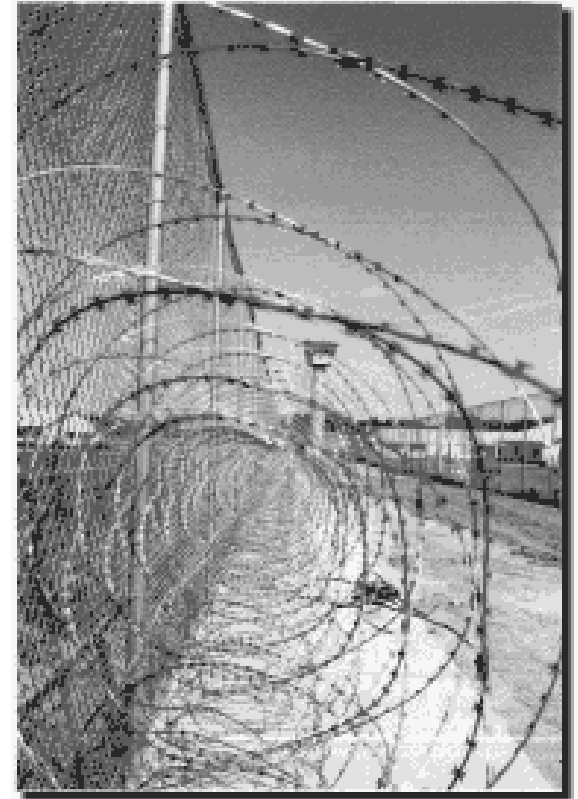
 - draft standard (DS) 2008

16/32-bit Solutions for Chassis/Safety



When protecting a system you must consider:

- What are you trying to protect?
- What types of attack do you need to protect against?
- What are the likely attack points, and methods?
- How much security do you require?
 - How much are you willing to pay?
- How will security impact the underlying system?
- How will you upgrade/maintain the system and security over time?



Electrical

- Over/Under voltage
- Power analysis
- Frequency analysis
- Electrostatic discharge
- Circuit probing

Software

- Spy software insertion
- Flow analysis
- Trojan horse
- Virus

Physical

- Temperature variation (into extremes)
- Temperature analysis
- De-processing
- System theft
- Partial destruction
- Hardware addition/substitution



Classic Security Requirements:

- **Confidentiality** - prevents eavesdropping
- **Authentication** - prevents impersonation
- **Data Integrity** - prevents tampering
- **Non-repudiation** - prevents denial
- **Trusted Processing** - enables trusted platform for authorized access to program and data
- **IP Protection** - prevent software/IP theft



How are Systems Protected Today?

Physical security:

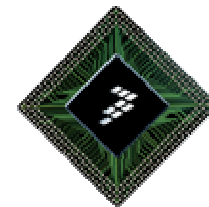
- Secure packaging
- Secure packaging with tamper detect (i.e. pressure monitoring)
- Secure packaging with tamper detect and destruction (i.e. dynamite)
- Obscured part numbers
- Hidden layers
- Protected location

Electronic Security:

- **Security bit, to protect on chip non-volatile memory (e.g. Flash), on MCUs-**
 - Prevent external access to on chip resources:
 - Locks device into Single Chip mode (Disables external parallel bus)
 - Disables Background Debug Mode
 - Disables Test Mode
 - Disables JTAG
 - Disables any (serial) “Bootstrap” functions
 - Memory array bulk erase turns security bit off
- **Secure System (e.g. PISA)**
 - Assurance for stored IP
 - Data stored encrypted in external memory
 - Data decrypted and stored in on-chip private memory at runtime
 - How do you protect software IP?
- **Proprietary (CPU) Design**
- **Silicon obfuscation (e.g. obscuring metal layer)**
- **On-Chip Encryption Acceleration**
 - How do you protect the key?



Cryptography



Symmetric Key Cryptography:

- Same key used to encrypt and decrypt
- Very fast
 - Typically used for bulk of encryption/decryption
- Same key must be at both end points.

Asymmetric (Public) Key Cryptography:

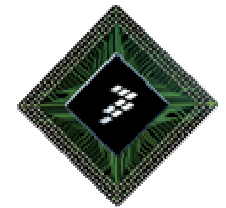
- 2 related keys are required (known as a public and a private key)
- 1000 times slower than symmetric key
- Typically used for exchange of symmetric keys
- and, sender authentication
- End points need have had no prior contact

Authentication:

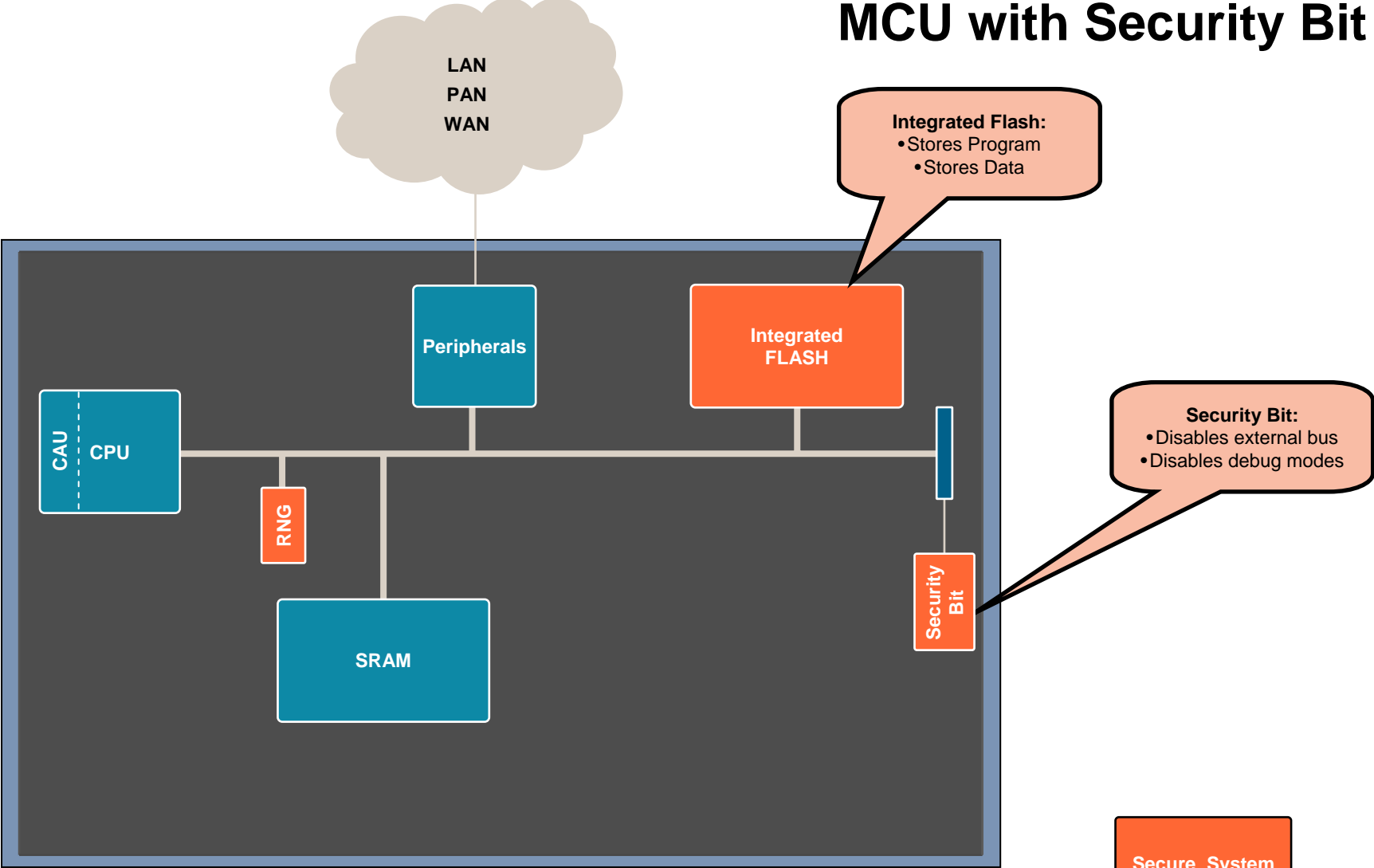
- Necessary to know who you're speaking to
- Certificates used to verify identity



Secure Systems: Platform Independent Security Architecture (PISA)



MCU with Security Bit



Available today on most MCU products

Protecting a Program in External Memory (3)

