Harry Potter

AND THE NOT-SO-SMART PROXY WAR

Jos Wetzels – Midnight Blue

WHOAMI?

JOS WETZELS

@S4MVARTAKA

https://www.midnightbluelabs.com

- Security Research & Consultancy
  - Security Researcher @ Midnight Blue
  - Principal Security Consultant @ Secura
- Focus: Embedded Systems
  - ICS, Automotive, IoT, Comms, …
- Previously
  - Protection of Critical Infrastructure @ University of Twente [NL]

VAULT 7

7 MARCH 2017

- 8761 documents & files
  Belonging to CIA's Center for Cyber Intelligence (CCI)
  Mainly dated 2013-2016
- Exploits, Implants, TTPs
  iOS, Android, OSx, Linux, Windows, Samsung Smart TVs, Routers, …
- Most entries got in-depth coverage
  By press, security researchers, IC enthusiasts, …

WikiLeaks Leaks News

EXCEPT FOR 1 ...

"protego" "vault 7"

Alle Shopping

Ongeveer 1.890 resultaten

"protego" "vault 7"

All Images

2.980 Results

Da

All Releases

Protego - 7 September, 2017

Angelfire - 31 August, 2017

ExpressLane - 24 August, 2017

CouchPotato - 10 August, 2017

Dumbo - 3 August, 2017

Imperial - 27 July, 2017

UCL / Raytheon - 19 July, 2017

PROTEGO

- Wikileaks Claimed Purpose

  “Raytheon-developed guided missile system installed on Pratt & Whitney aircraft”

- 4 secret documents

  And 37 related proprietary hardware/software manuals from Microchip Technology Inc.

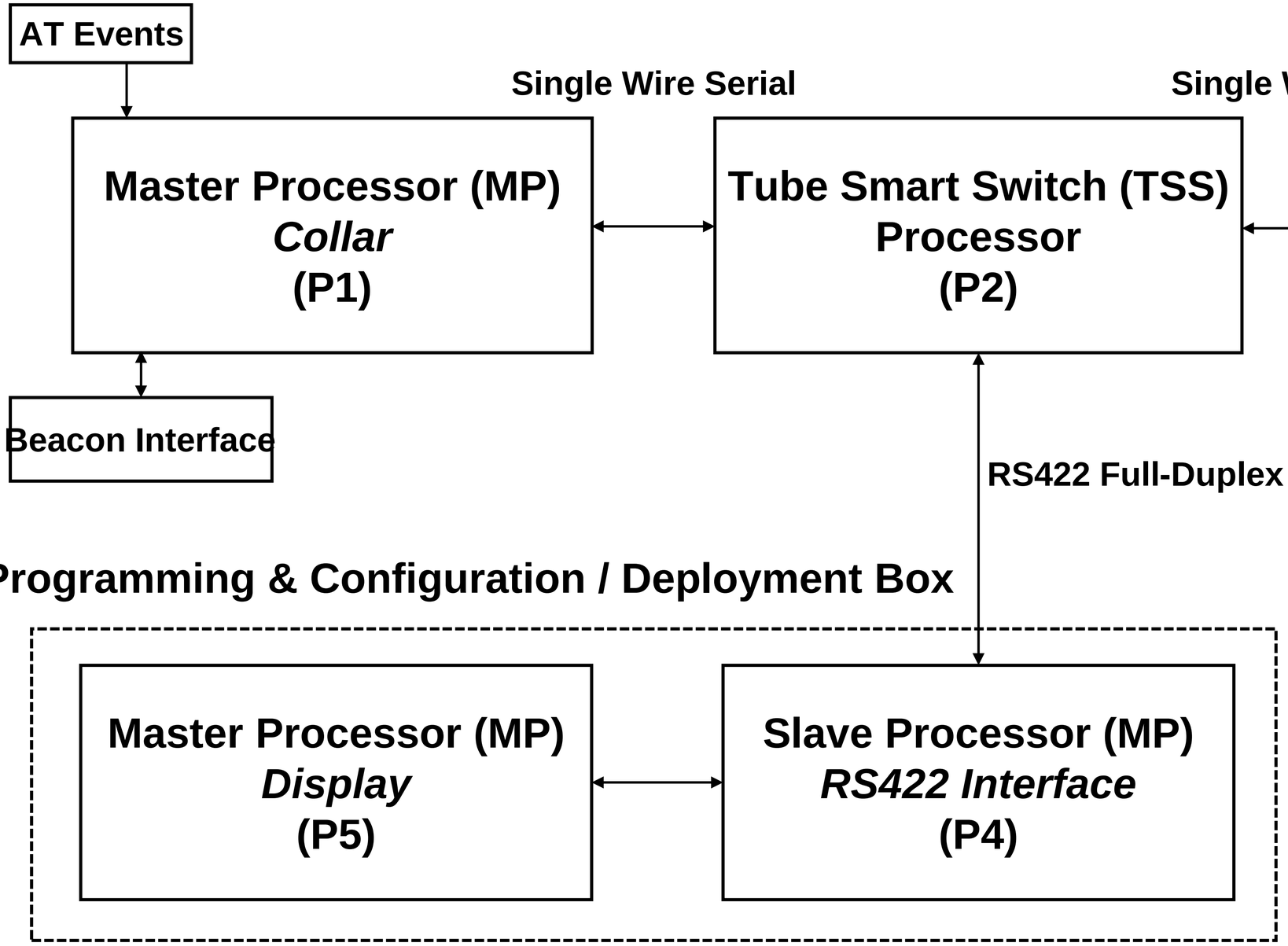
- Maintained between 2014-2015

- Very different from other CCI/Vault 7 projects

  No clear indication why it was in the repos …


SOMETHING’S NOT RIGHT …

PROTEGO ARCHITECTURE (SIMPLIFIED)



- *Protego* subsystem
- Deployment box
- Inter-MCU comms over serial
- Incoming GPS signals

SO FAR, SO GOOD RIGHT?

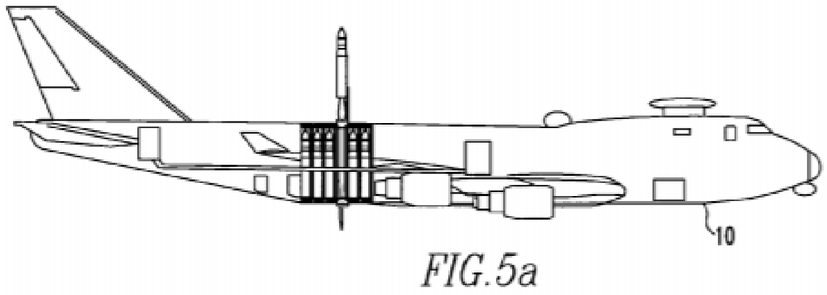


FIG.5a

Missile

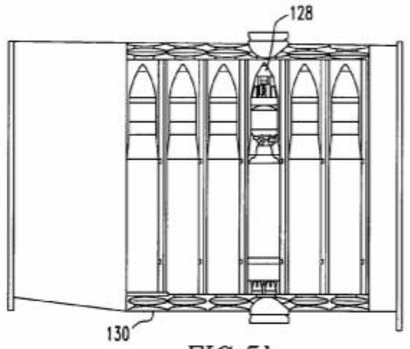
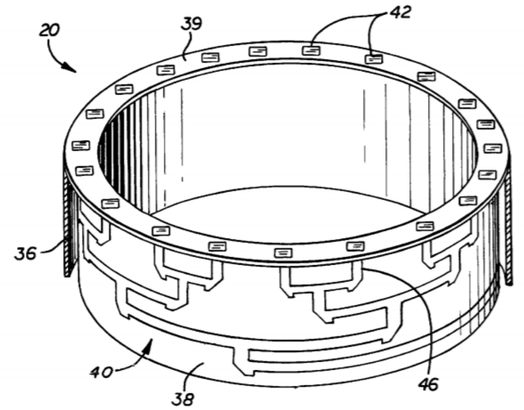


FIG.5b

Tube



Collar

THIS IS ALL CLEARLY MISSILE SYSTEMS TERMINOLOGY

BUT #1: PWA?

documents indicate that the system is installed on-board a Pratt & Whitney aircraft (PWA) equipped with missile launch systems (air-to-air and/or air-to-ground).

P1 - Master Processor (MP), Master Processor on PWA

P1_S - Master Processor (MP), Slave Processor on PWA

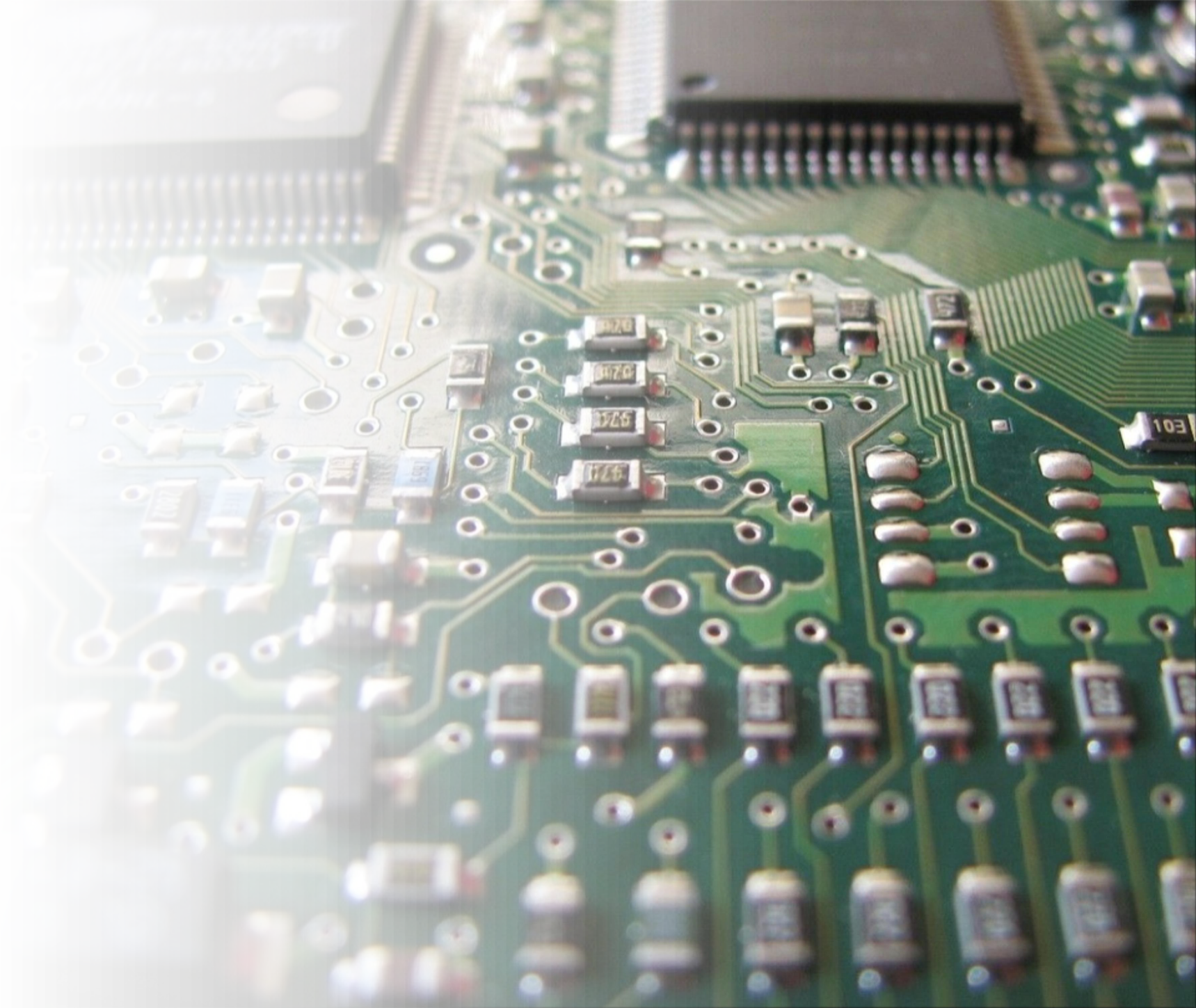
- P&W assertion seems based solely on PWA abbreviation
- P&W manufacture engines, not aircraft
- Doesn't make sense for *Protego*'s MCUs to reside "on" the engine

…

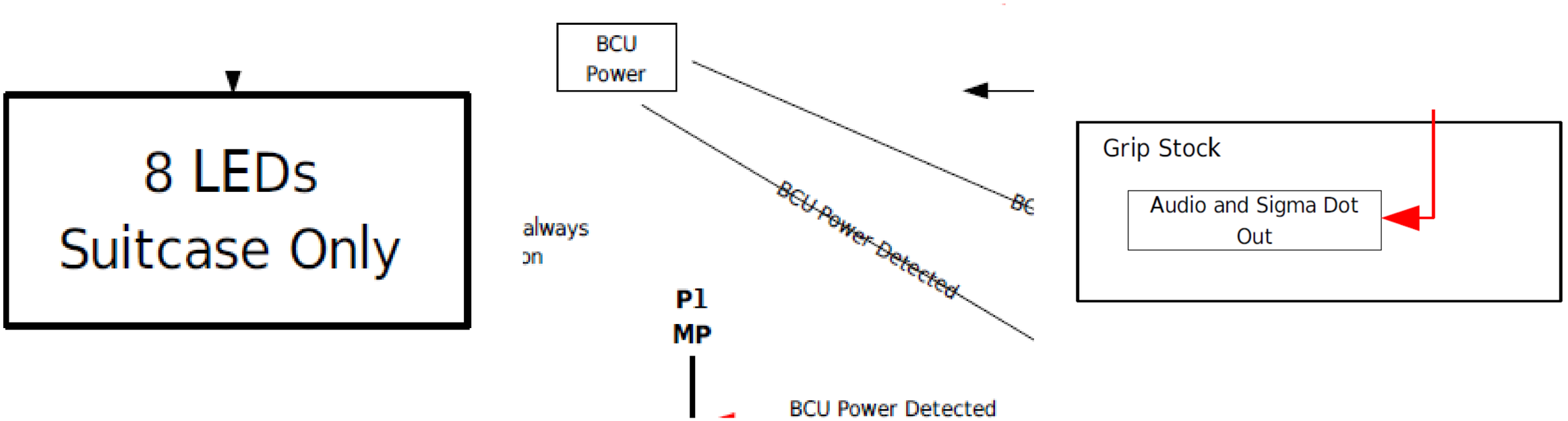
PWA = PRINTED WIRING ASSEMBLY

- PWA is a PCB after all electrical components are attached

- Makes sense that MCUs are referred to as residing “on” PWA



BUT #2: COMPLICATING TERMINOLOGY



NOT TYPICAL AIR-TO-SURFACE (ASM) /
AIR-TO-AIR (AAM) MISSILE TERMINOLOGY ...

ALTERNATIVE HYPOTHESIS

PROTEGO IS A MANPADS ‘SMART’ ARMS CONTROL SOLUTION

Man-portable air-defense systems (MANPADS) are portable surface-to-air missile systems eg. famous FIM-92 Stinger manufactured by Raytheon

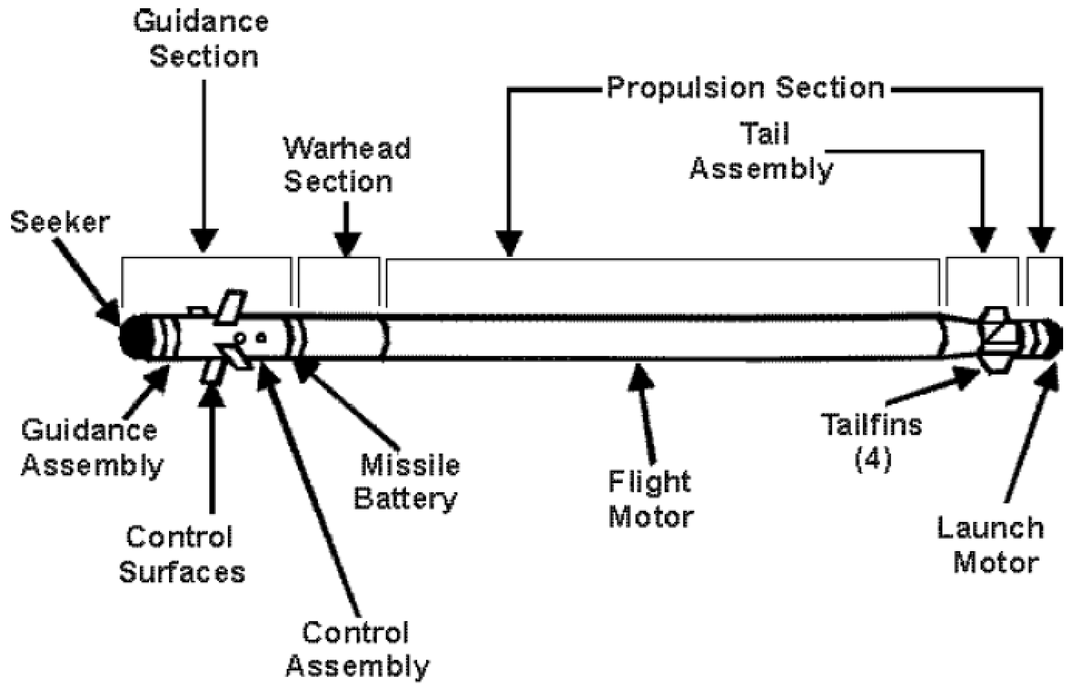
ASSEMBLED, INCLUDING LAUNCH TUBE

MISSILE

LAUNCH TUBE

- Missiles typically delivered in discardable launch tube (includes sight assembly)
- Tubes can be reused but done at depot, not on battlefield
- Transported in dedicated case

** Images: FIM-92 Stinger via Stratfor*

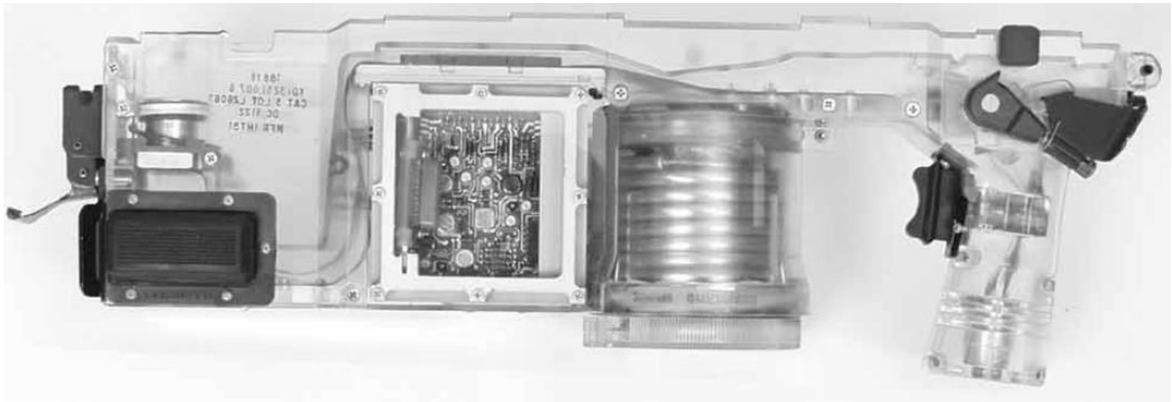


MISSILES

- IR seeker allows for ‘passive homing’ (fire & forget)**
- Guidance & control steer missile during chase
- Warhead goes boom

*** note that there are also active homing ‘command guidance’ MANPADS*

** Images: FIM-92 Stinger via C. Kogler/B.I.C.C. & US Marine Corps Warfighting Publications*



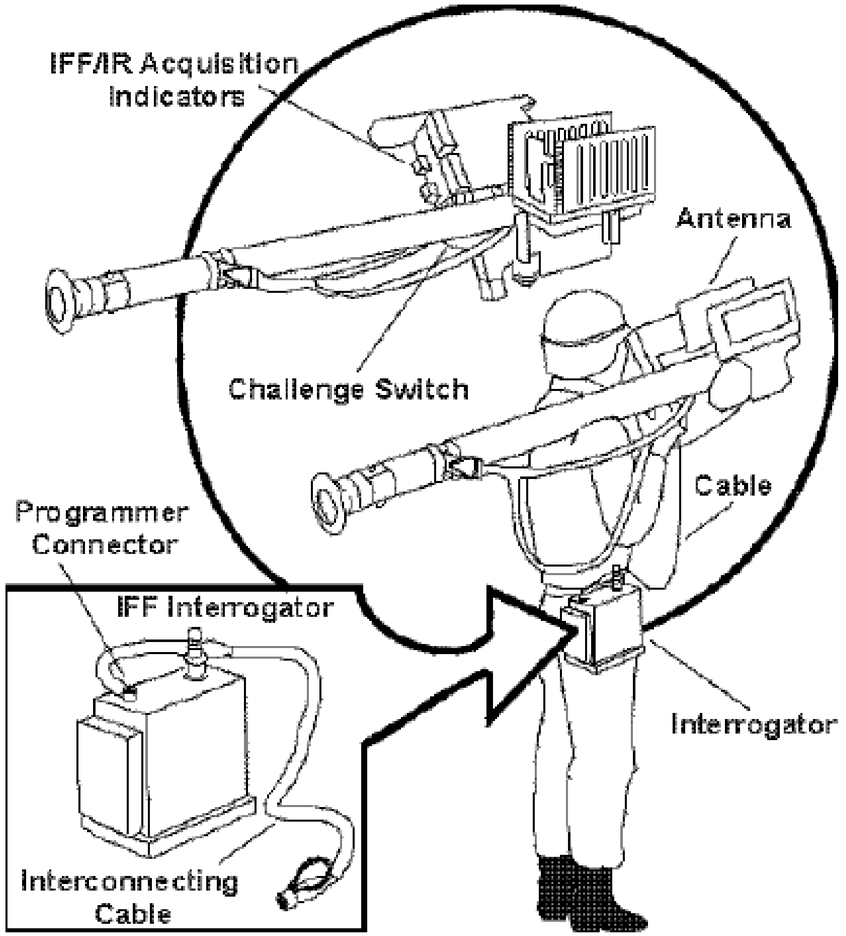
GRIPSTOCK

- Detachable gripstock with trigger & targeting electronics
- Talks to missile to unlock seeker, initiate target lock, trigger launch
- Connection to optional IFF transceiver
- BCU for power & cooling inserted into gripstock

** Images: FIM-92 Stinger via Stratfor, C. Kogler/B.I.C.C.*

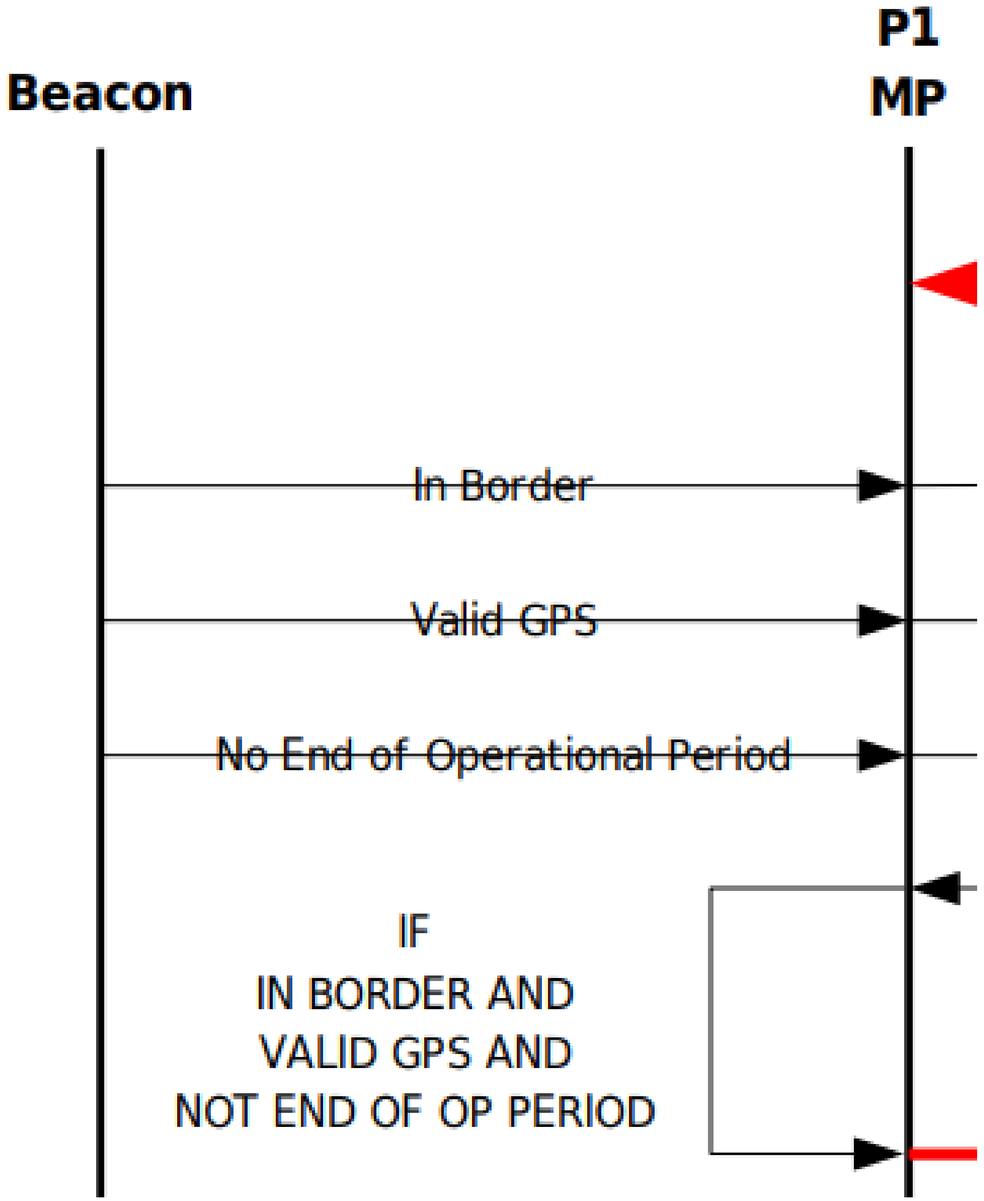
LAUNCH PROCEDURE

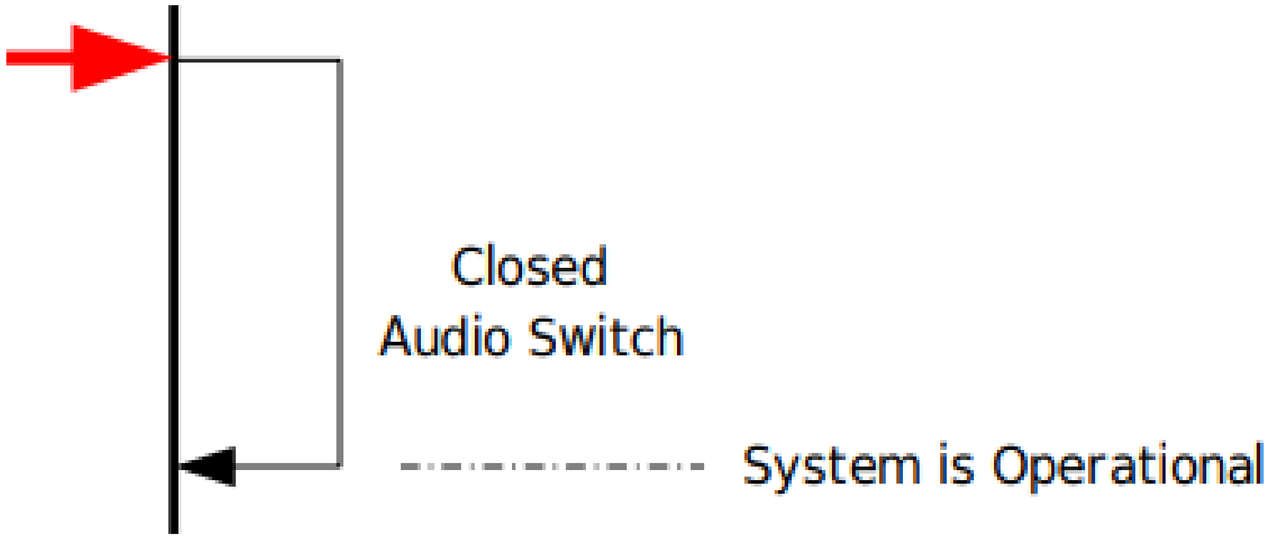
1. Attach gripstock & IFF to launch tube
2. Use sight to track aircraft
3. Get audio feedback from IFF on target status
4. Insert BCU
5. Get audio feedback from gripstock on target lock
6. Pull trigger to fire



** Images: US Marine Corps Warfighting Publications*

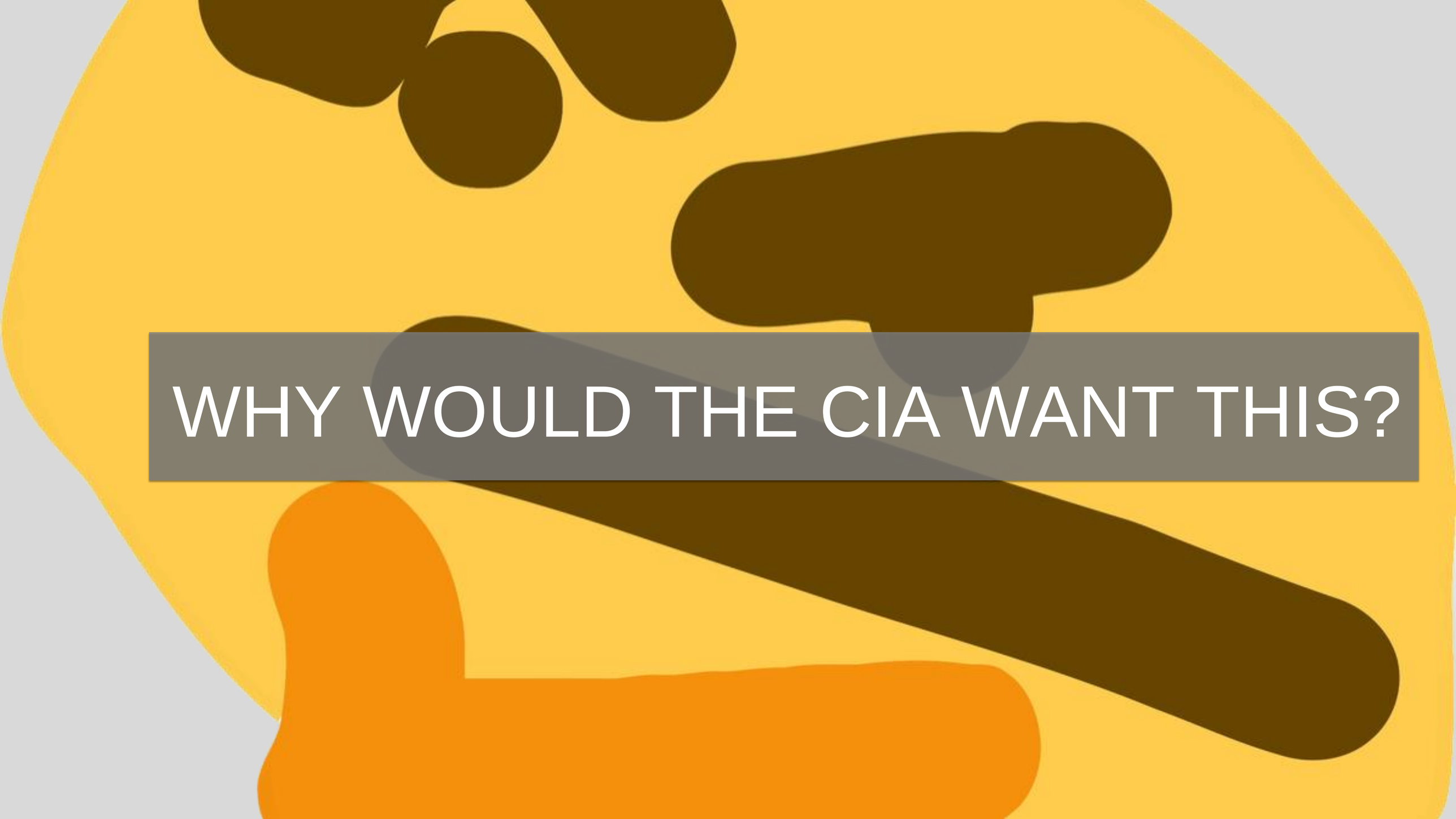
PROTEGO OPERATIONAL CONDITIONS





GEO- & TIME-FENCING

** Image: mobgen.com*


WHY WOULD THE CIA WANT THIS?

CIA ‘Plan B’ for Syria would give rebels MANPADs to 'counter Russia' - report

Russia must find out where Syrian militants got MANPADS that downed Su-25 – MPs

> The pressure on the U.S. and its allies in the region to provide heavier weapons to opposition militias will increase if Russian-backed Syrian forces fully break the ceasefire, which has held in most of Syria for six weeks, the official said. Last month, the Wall Street Journal reported that the CIA is preparing a “Plan B” in case the ceasefire completely crumbles that involves supplying vetted moderate rebel fighters with MANPADS.

** Source: LA Times, RT, WSJ, FP*

Taliban still have Reagan's Stingers

10 / INTERNATIONAL

THE INDEPENDENT

MONDAY 6 DECEMBER 1993

The Saudi businessman who recruited mujahedin now uses them for large-scale building projects in Sudan. **Robert Fisk** met him in Almatig

Anti-Soviet warrior puts his army on the road to peace

OSAMA Bin Laden sat in his gold-fringed robe, guarded by the loyal Arab mujahedin who fought alongside him in Afghanistan. Bearded, taciturn figures — unarmed, but never more than a few yards from the man who recruited them, trained them and then dispatched them to destroy the Soviet army — they watched unsmiling as the Sudanese villagers of Almatig lined up to thank the Saudi businessman who is about to complete the highway linking their homes to Khartoum for the first time in history.

With his high cheekbones, narrow eyes and long brown robe, Mr Bin Laden looks every inch the mountain warrior of mujahedin legend. Chadored children danced in front of him, preachers acknowledged his wisdom. "We have been waiting for this road through all the revolutions in Sudan," a sheikh said. "We waited until we had given up on everybody — and then Osama Bin Laden came along."

Outside Sudan, Mr Bin Laden is not regarded with quite such high esteem. The Egyptian press claims he brought hundreds of former Arab fighters back to Sudan from Afghanistan, while the Western embassy circuit in Khartoum has suggested that some of the "Afghans" whom this Saudi entrepreneur flew to Sudan are now busy training for further *jihad* wars in Algeria, Tunisia and Egypt. Mr Bin Laden is well aware of this. "The rubbish of the media and the embassies," he calls it. "I am a construction engineer and an agriculturalist. If I had training camps here in Sudan, I couldn't possibly do this job."

And "this job" is certainly an ambitious one: a brand-new highway stretching all the way from Khartoum to Port Sudan, a distance of 1,200km (745 miles) on the old road, now shortened to 800km by the new Bin Laden route that will turn the coastal run from the capital into a mere day's journey. Into a country that is despised by Saudi Arabia for its support of Saddam Hussein in the Gulf war almost as much as it is condemned by the United States, Mr Bin Laden has brought the very construction equipment that he used only five years ago to build the guerrilla trails of Afghanistan.

He is a shy man. Maintaining a home in Khartoum and only a small apartment in his home city of Jeddah, he is married — with four wives — but wary of the press. His interview with the *Independent* was the first he has ever given to a Western journalist, and he initially refused to talk about Afghanistan, sitting silently on a chair at the back of a makeshift tent, brushing his teeth in the Arab fashion with a stick of *miswak* wood. But talk he eventually did about a war which he helped to win for the Afghan mujahedin: "What I lived in two years there, I could not have lived in a hundred years elsewhere," he said.

> 'What I lived in two years in Afghanistan, I could not have lived in a hundred years elsewhere,' said Osama Bin Laden

When the history of the Afghan resistance movement is written, Mr Bin Laden's own contribution to the mujahedin — and the indirect result of his training and assistance — may turn out to be a turning-point in the recent history of militant fundamentalism; even if, today, he tries to minimise his role. "When the invasion of Afghanistan started, I was enraged and went there at once — I arrived within days, before the end of 1979," he said. "Yes, I fought there, but my fellow Muslims did much more than I. Many of them died and I am still alive."

Within months, however, Mr Bin Laden was sending Arab fighters — Egyptians, Algerians, Lebanese, Kuwaitis, Turks and Tunisians — into Afghanistan, "not hundreds but thousands," he said. He supported them with weapons and his own construction equipment. Along with his Iraqi engineer, Mohamed Saad — who is now building the Port Sudan road — Mr Bin Laden blasted massive tunnels into the Zazi mountains of Bakhtiar province for guerrilla hospitals and arms dumps, then cut a mujahedin trail across the country to within 15 miles of Kabul.

"No, I was never afraid of death. As Muslims, we believe that when we die, we go to heaven. Before a battle, God sends us *sagina*, tranquillity.

"Once I was only 30 metres from the Russians and they were trying to capture me. I was under bombardment but I was so peaceful in my heart that I fell asleep. This experience has been written about in our earliest books. I saw a 120mm mortar shell land in front of me, but it did not blow up. Four more bombs were dropped from a Russian plane on our headquarters but they did not explode. We beat the Soviet Union. The Russians fled."

But what of the Arab mujahedin whom he took to Afghanistan — members of a guerrilla army who were also encouraged and armed by the United States — and who were forgotten when that war was over? "Personally neither I nor my brothers saw evidence of American help. When my mujahedin were victorious and the Russians were driven out, differences started [between the guerrilla movements] so I returned to road construction in Taif and Abha. I brought back the tools and roads for the mujahedin in Afghanistan. Yes, I helped some of my comrades to come here to Sudan after the war."

How many? Osama Bin Laden shakes his head. "I don't want to say. But they are here now with me, they are working right here, building this road to Port Sudan." I told him that Bosnian Muslim fighters in the Bosnian town of Travnik had mentioned his name to me. "I feel the same about Bosnia," he said. "But the situation there does not provide the same opportunities as Afghanistan. A small number of mujahedin have gone to fight in Bosnia-Herzegovina but the Croats won't allow the mujahedin in through Croatia as the Pakistanis did with Afghanistan."

Thus did Mr Bin Laden reflect upon *jihad* while his former fellow combatants looked on. Was it not a little bit anti-climactic for them, I asked, to fight the Russians and end up road-building in Sudan? "They like this work and so do I. This is a great plan which we are achieving for the people here, it helps the Muslims and improves their lives."

His Bin Laden company — not to be confused with the larger construction business run by his cousins — is paid in Sudanese currency which is then used to purchase sesame and other products for export; profits are clearly not Mr Bin Laden's top priority.

How did he feel about Algeria, I asked? But a man in a green suit calling himself Mohamed Moussa — he claimed to be Nigerian although he was a Sudanese security officer — tapped me on the arm. "You have asked more than enough questions," he said. At which Mr Bin Laden went off to inspect his new road.

Osama Bin Laden surveys the 800km road he is building in northern Sudan

Photogra

Daily service to the USA

ONLY ON

THE WEEK AHEAD

Gatt set

A lesson i the langu

In recent days, U.S. officials have hinted that they may be willing to provide the weapons — known in military circles as MANPADS, short for "man-portable air defense system" — with one major caveat: They include technical controls that would limit where they can be used to ensure they don't one day fall into terrorist hands.

Using GPS, the missiles could be programmed to lock out users in certain locations, according to the Small Arms Survey report – but

** Source: LA Times, RT, WSJ, FP*

TIMBER SYCAMORE

Operational scope	Weapons sales, training of Syrian rebel forces
Location	Eastern Europe, Jordan, Syria
Planned by	Central Intelligence Agency
Target	Syrian Army
Date	2012 – 2017

- Program supposedly barred MANPADS …
- Other reports claim US-supplied MANPADS did make it into Syria
- Unclear whether PROTEGO was part of this or ever fielded

Charles Lister @Charles_Lister · 5 Apr 2016

Replying to @Charles_Lister

- A small number (+/- 12) of MANPADS were sent into northern #Syria in late-'15 as an immediate reaction to #Russia's intervention in Sept.

10 66 28

Charles Lister @Charles_Lister · 5 Apr 2016

- Those MANPADS were to be used for select political purposes.
- x2 were likely used in March '16 downing.
- Looks likely x1 was used today.

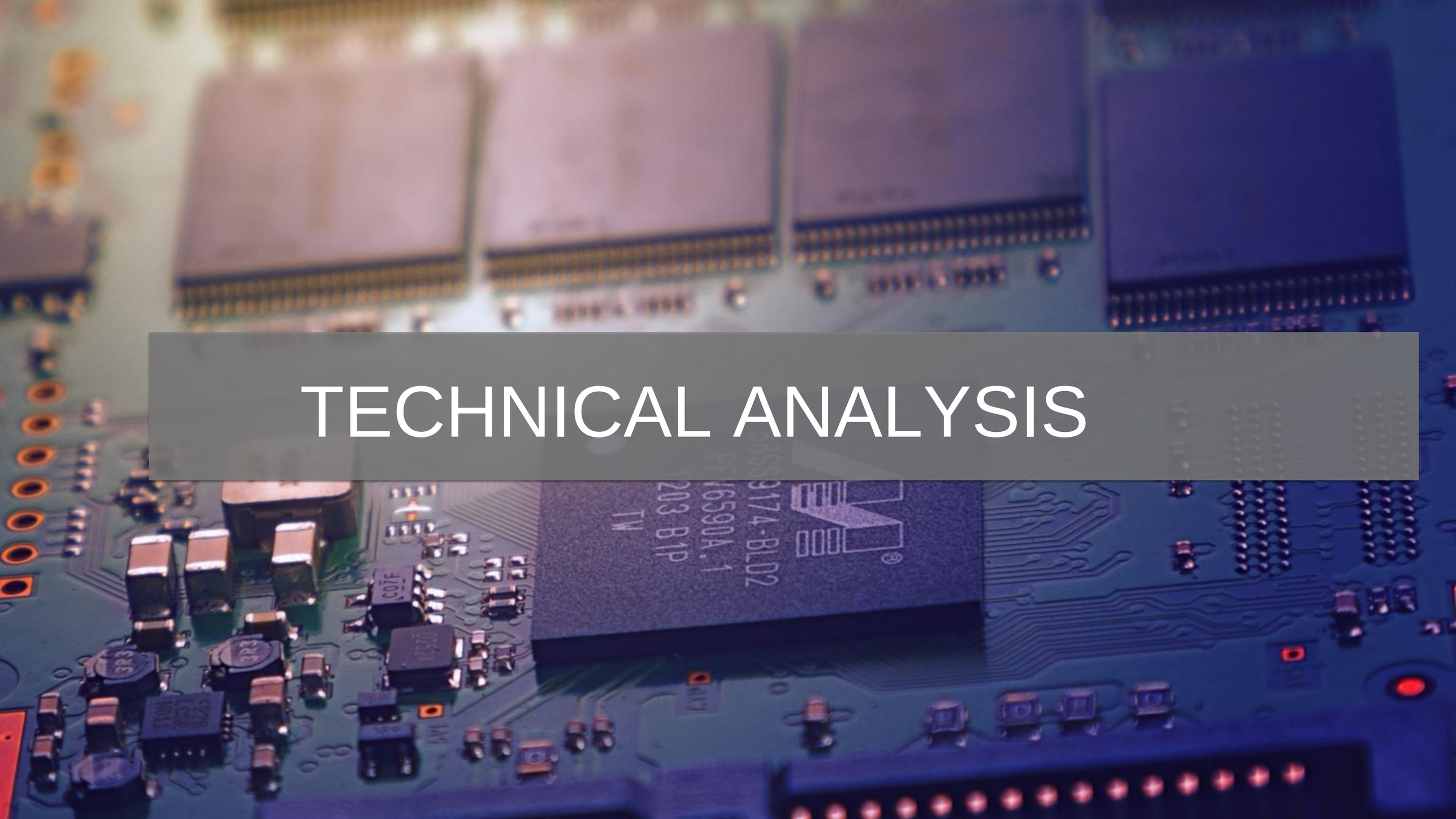
THE HARRY POTTER CONNECTION

To aid in keeping the key numbers grouped, the Devil Snare Keys numbers start at 1000 and Protego Keys numbers start at 2000

Devil's Snare is a magical plant with the ability to constrict or strangle anything in its surrounding environment or something that happens to touch it. Devil's Snare does not seem to be common, but certain Herbologists have access to it.

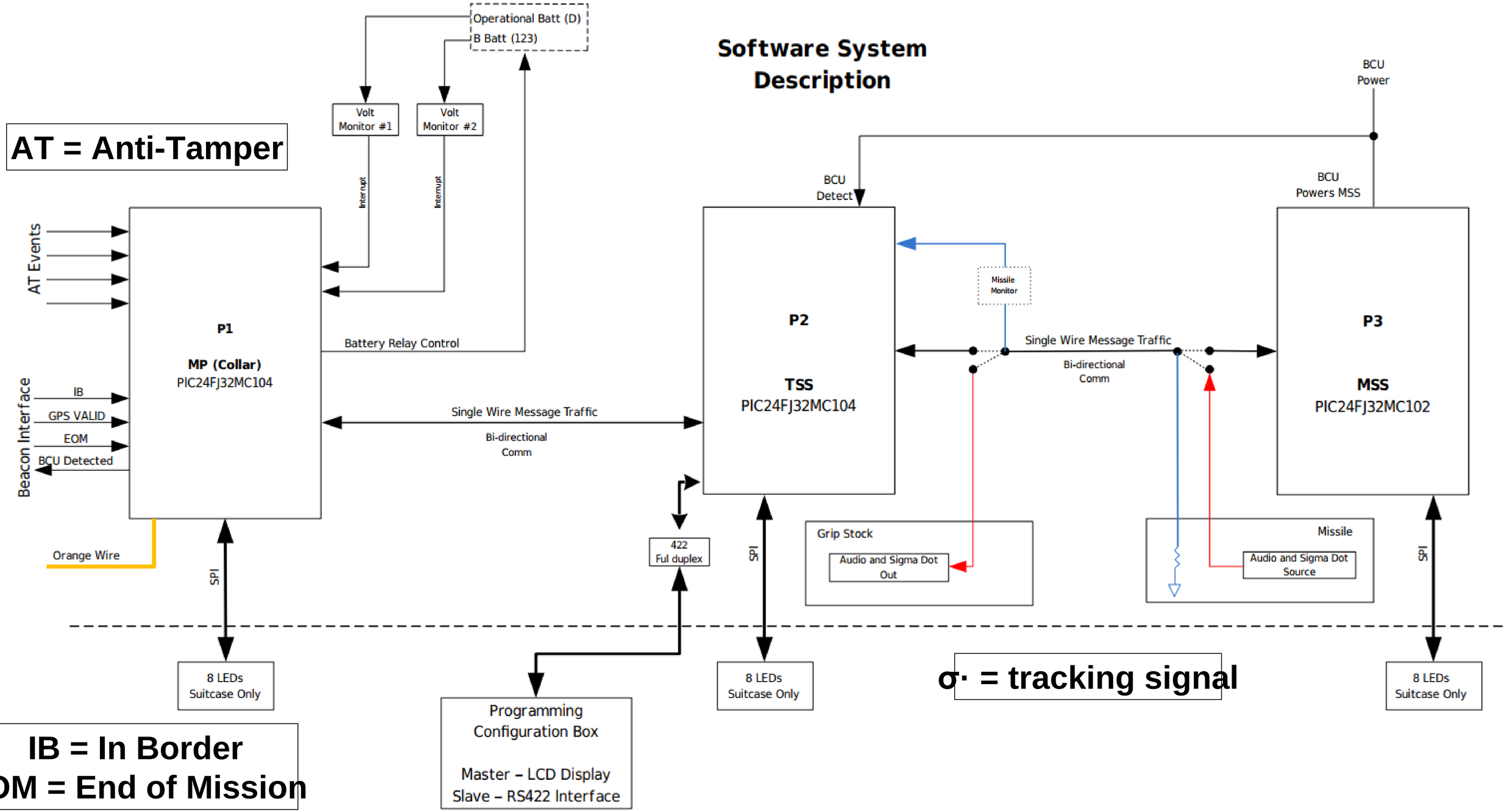
The **Shield Charm** (*Protego*) is a charm that protects the caster with an invisible shield that reflects spells and blocks physical entities.

* *Source:* https://harrypotter.fandom.com/

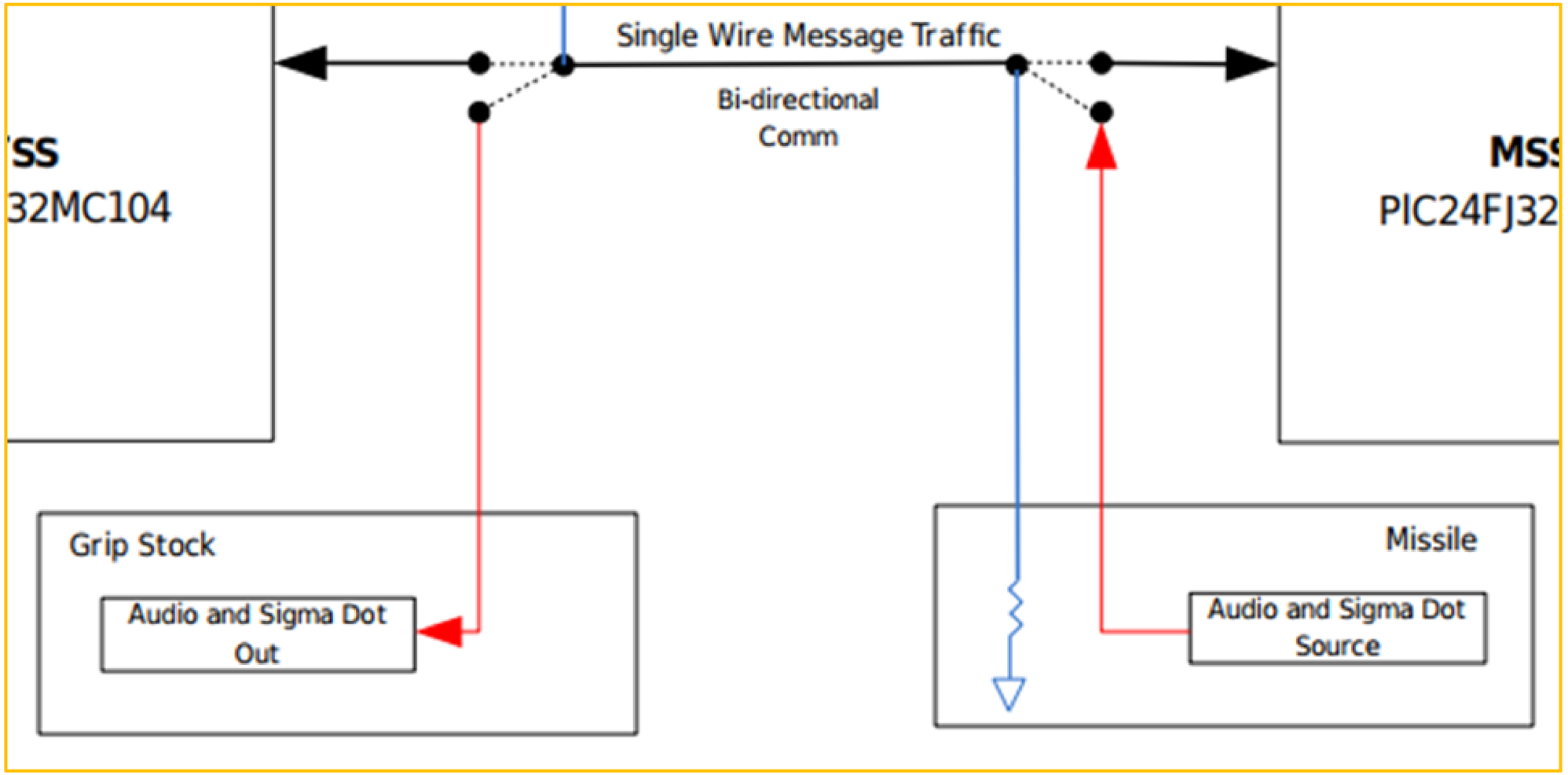


TECHNICAL ANALYSIS

SECRET//NOFORN

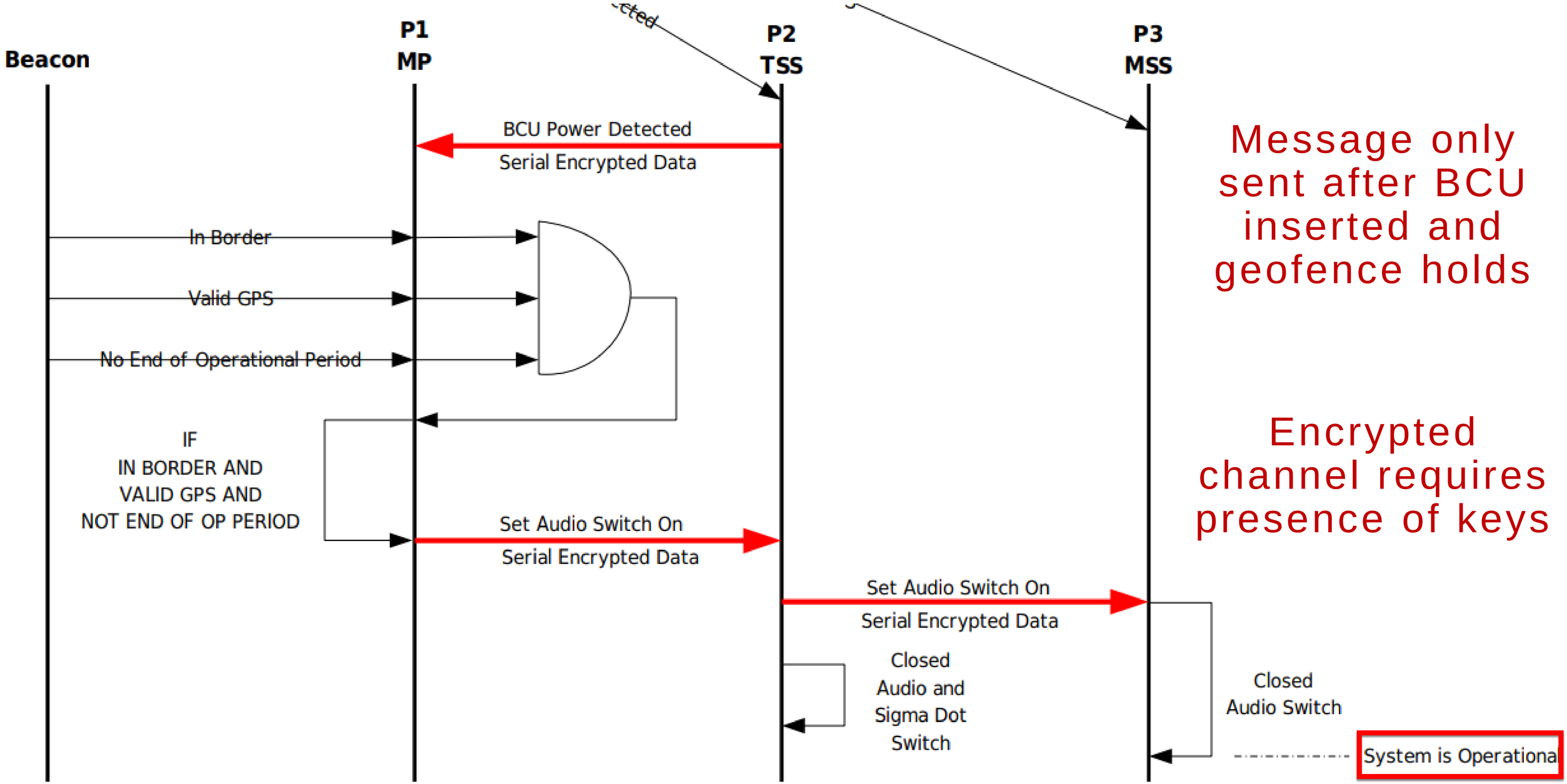


SMART FENCE MECHANISM



Open switch = no signal from missile seeker to gripstock targeting system

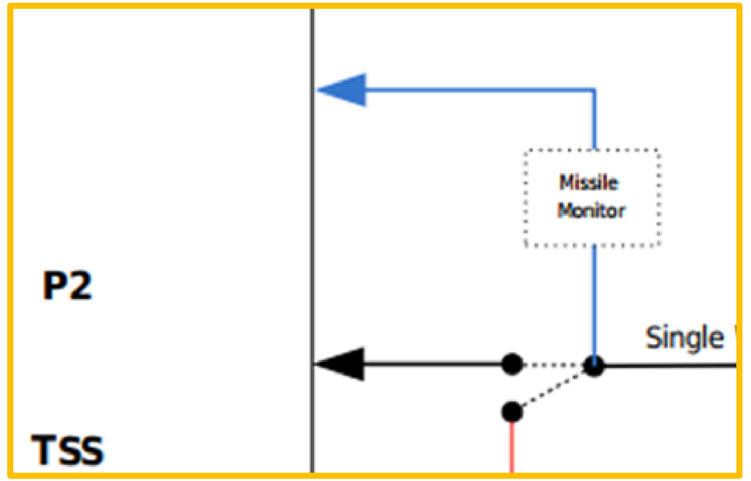
MSS CLOSES SWITCH AFTER MESSAGE FROM MP VIA TSS



Message only sent after BCU inserted and geofence holds

Encrypted channel requires presence of keys

KEY ERASURE



Beacon

After entering in border once

MP

TSS

AT or low battery event

Out of border or End of Mission

Missing missile detected

Erase MP key

Erase pulse

Erase MP key

Erase pulse

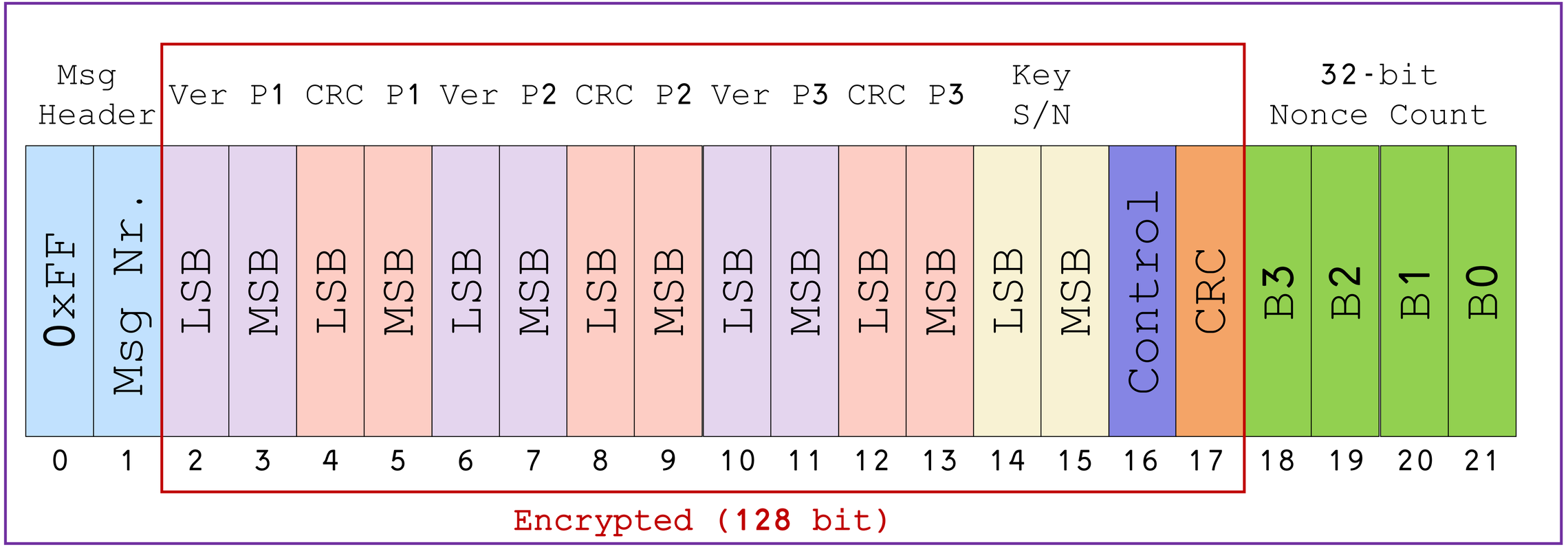
Erase TSS key

STATUS INDICATION LEDS

		LEDs on Suite Case							
	LED	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
MP	**Green**	Tactical	Batteries On	Batt Ok	No AT Event	In Fence	GPS Validity Good	Mission Time Good	Operational
	Off	Storage					Unknown		Sleep
	Red	Factory	Batteries Off	Batt Low	At Event	Out of Fence	GPS Validity Bad	EOM	Erased*
						These three LEDs reflect what the MP is seeing at it's inputs			
TSS	**Green**	Tactical	BCU Detected		Missile Present		Prog MP	Prog Box Connected	Operational
	Off	Storage	No BCU	Audio Relay Off	No M Check				Sleep
	Red	Factory		Audio Relay On	Missile Missing		Prog Beacon		Erased*
MSS	**Green**	Powered On							Erased*
	Off	Powered Off	Audio Relay Off						
	Red		Audio Relay On						

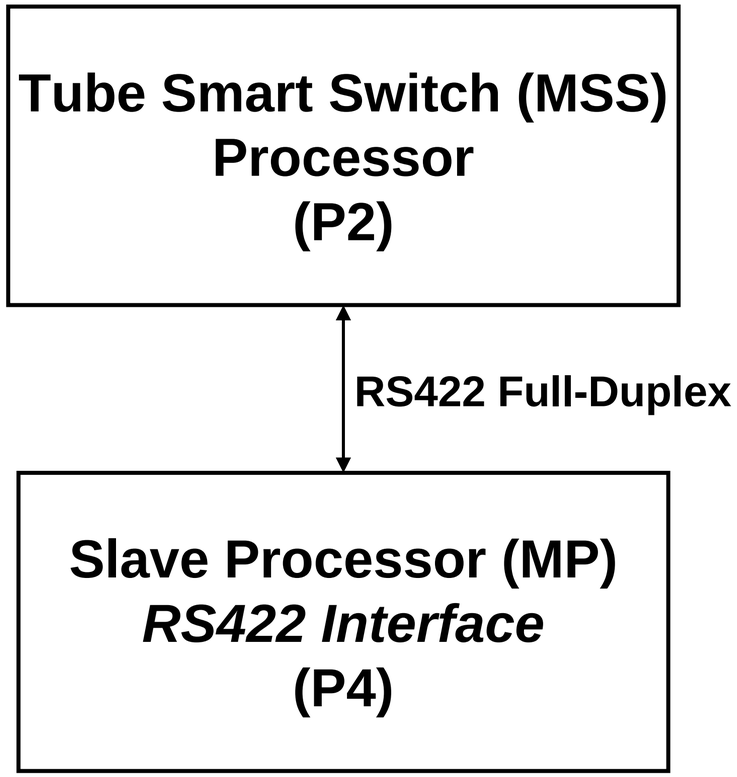
Operators need to know system is ‘good-to-go’ before running up to aircraft …

P MESSAGE FORMAT



- Sent over RS422 and internal serial bus between different MCUs
- For unencrypted messages, only Key S/N and control/CRC bytes are set

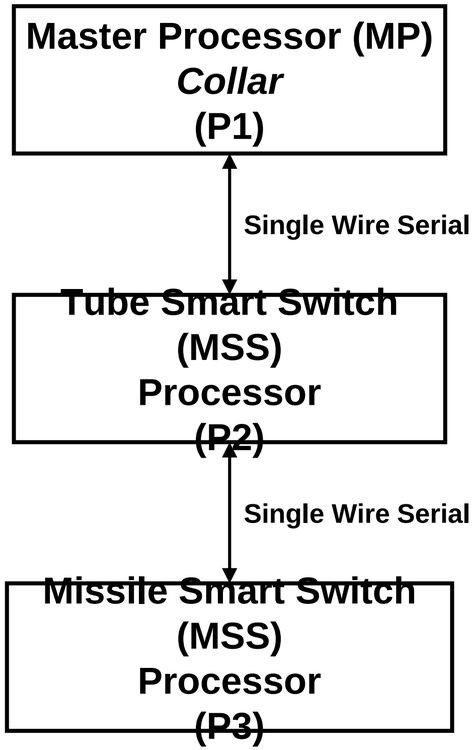
PROGRAMMING BOX <-> PROTEGO



Messages of Interest

RS422 Messages		Msg Tx By		Msg Rx By	
Ctrl	Command	P4	TSS	P4	TSS
0x00	Do nothing (ret Ver+CRC)	X	X	X	X
0x01	Request MSS Ver	X			X
0x02	Request MP Ver	X			X
0x03	Request TSS Ver	X			X
0x04	Set MP to Prog Mode	X			X
0x05	Set MP to Prog State	X			X
0x06	Set Beacon to Prog State	X			X
0x07	Stop Prog States (MP+Beacon)	X			X
0x08	Set to Factory Test Mode	X			X
0x09	Set to Storage Mode	X			X
0x0A	Set to Tactical Mode	X			X
0x0B	Turn Batteries On	X			X
0x0C	Turn Batteries Off	X			X

PROTEGO INTERNAL



Operational Messages

Serial Messages		Msg Tx By			Msg Rx By		
Ctrl	Command	MP	TSS	MSS	MP	TSS	MSS
0x00	Do nothing (ret Ver+CRC)	X	X	X	X	X	X
0x01	Set Audio Relay	X				X	
0x02	AT or low battery detect	X				X	
0x03	BCU inserted		X		X		
0x04	BCU removed		X		X		
0x05	Missile Missing		X		X		
0x06	Set MP to Prog Mode		X		X		
0x07	Set MP to Prog State		X		X		
0x08	Set Beacon to Prog State		X		X		
0x09	Stop Prog States (MP+Beacon)		X		X		
0x0A	Set to Factory Test Mode		X		X		
0x0B	Set to Storage Mode		X		X		
0x0C	Set to Tactical Mode		X		X		
0x0D	Turn Batteries On		X		X		
0x0E	Turn Batteries Off		X		X		
0x0F	Missile Detected		X		X		

SECURITY ANALYSIS

HYPOTHETICAL PROTEGO LIFECYCLE

1. Programmed with key material, switched to storage mode

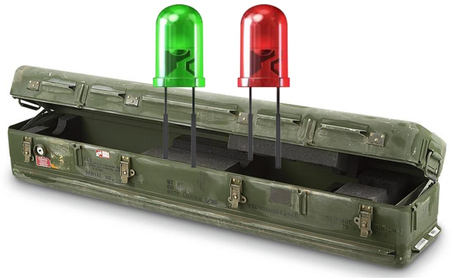
2. Shipped to (covert?) facility in/near theater

3. Programming box configures geo- & time fence, enables tactical mode

4. Handover to *"less-than-trusted"* 3rd party

5. If stolen, rendered inoperable outside fence

6. If mission period expires without use, returned to facility



7. Status check (LEDs), either put in storage mode or reconfigure

8. If AT event detected, raise alert

http://www.smallarmssurvey.org/fileadmin/docs/G-Issue-briefs/SAS-IB11-MANPADS-use-control.pdf

CRYPTOGRAPHIC ARCHITECTURE

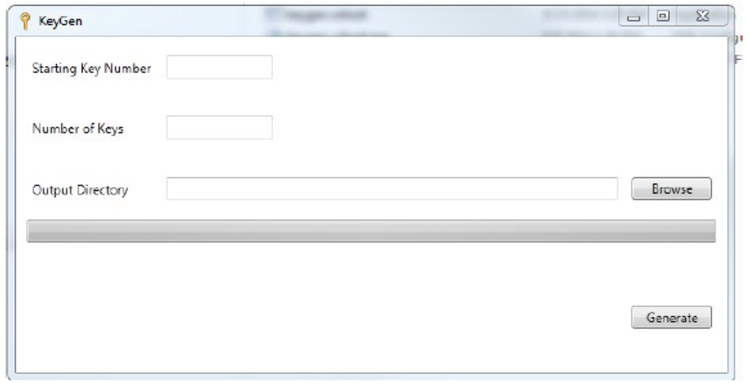
MP

TSS

MSS

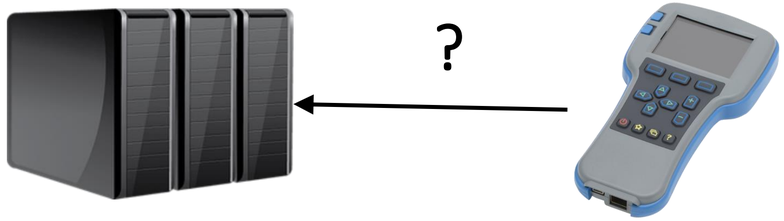
1 maintenance key embedded in fw images, *identical* for all PROTEGO instances
Never erased

1. Keys are generated & written into MP, TSS & MSS fw images



- One 128-bit key per MANPADs
- Identical for MP, TSS & MSS
- MSS never erased
- Suggests AES-128 in ECB mode (since msg is 128-bit)

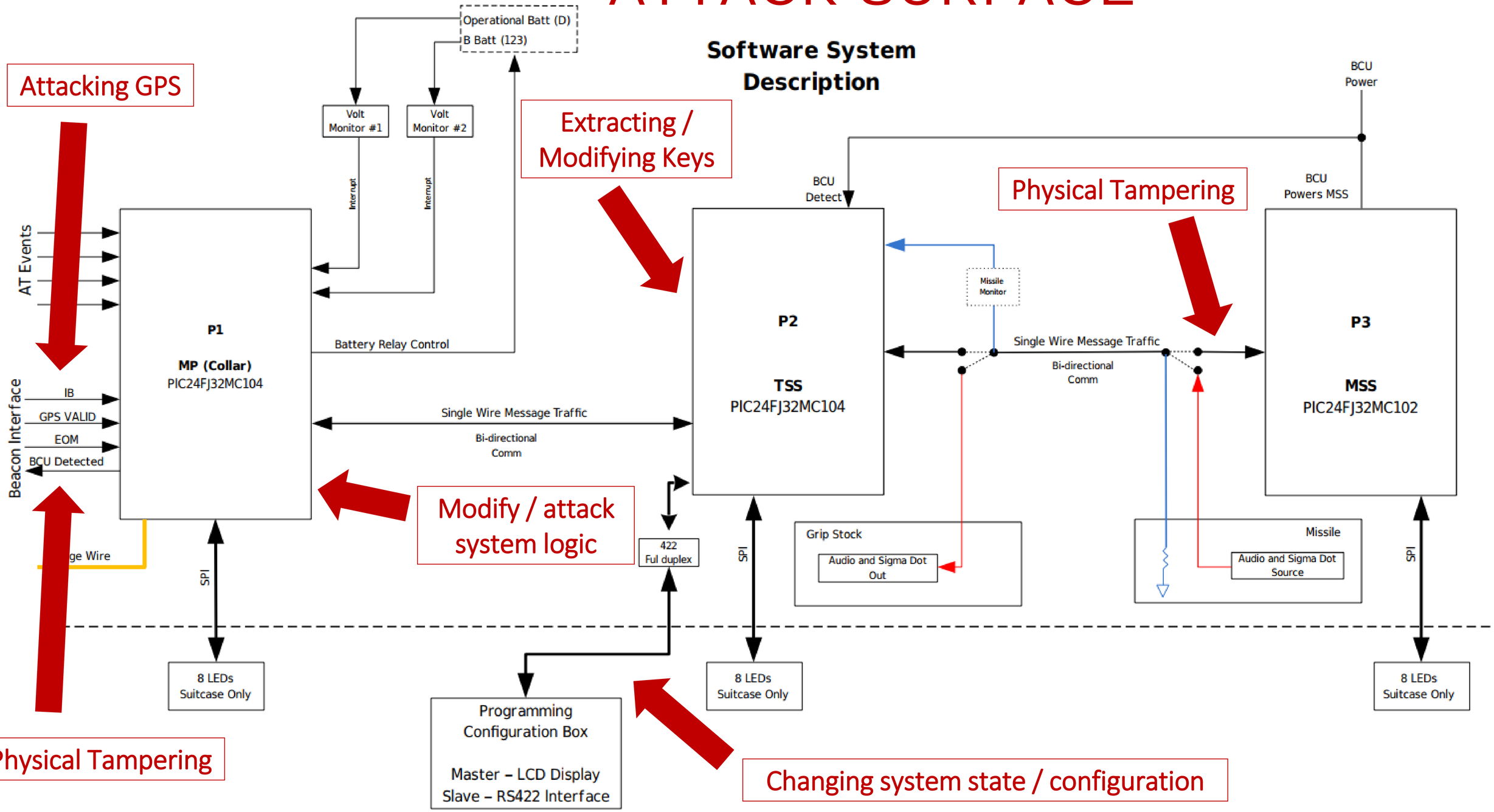
2. Programming box does not contain any keys, possibly queries them from a backend?



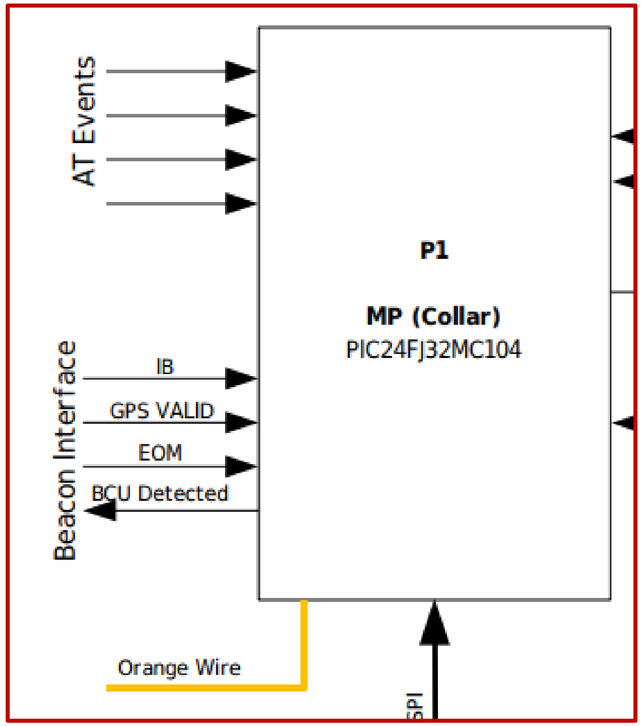
3. Unclear how reconfiguration is done exactly, but after key erasure still need to talk to PROTEGO. Makes sense system falls back to global maintenance key.

SECRET//NOFORN

ATTACK SURFACE

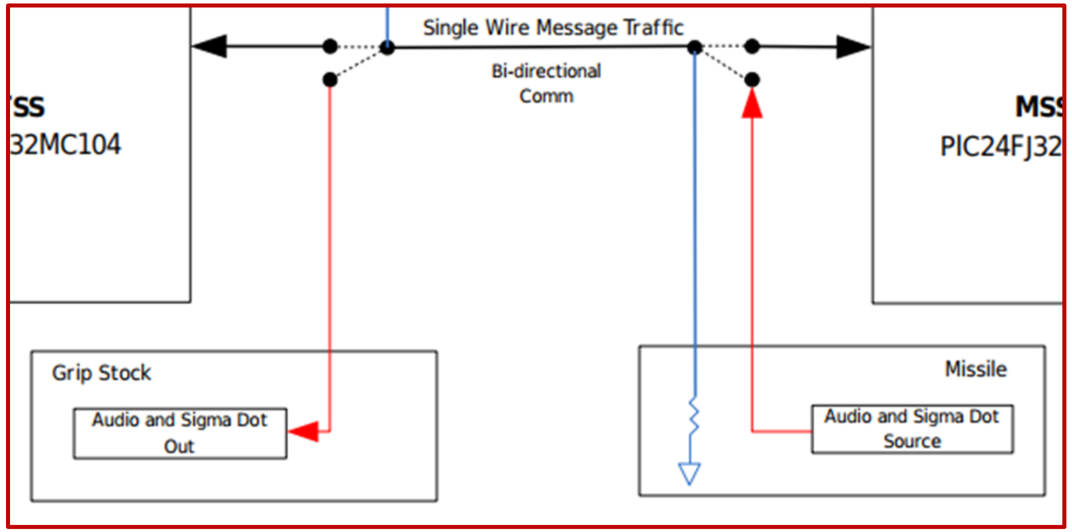


PHYSICAL TAMPERING



Beacon Interface signals

Eg. Cause default-true evaluation



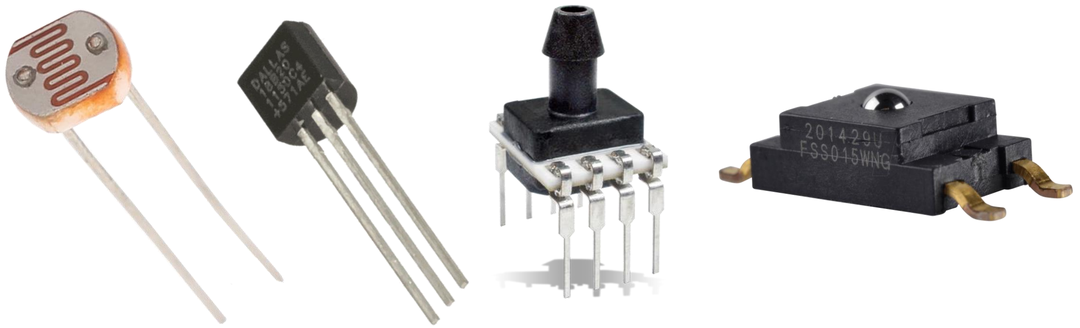
Smart Switch

Eg. Ensure it's normally-closed

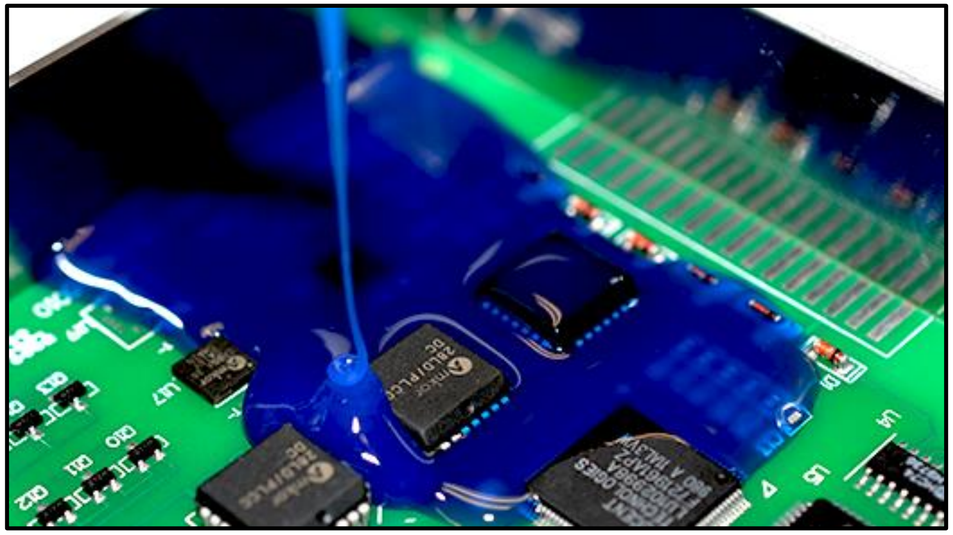
ANTI-TAMPER MEASURES

Metal Shielding

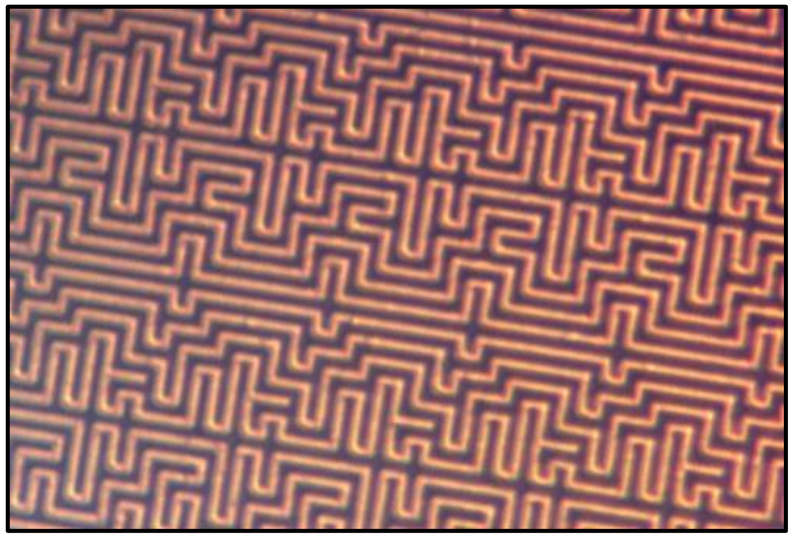
Light/Temp/Pressure/Force Sensors



Encapsulation



Active Meshes



* https://siliconpr0n.org/wiki/doku.php?id=physical_protection, www.cellspare.com, www.chasecorp.com

ANTI-TAMPER MEASURES

- Many well-explored invasive techniques, also via backside*
- Keys stored in flash, not battery-backed SRAM
  - *Attacker who cuts write-enable line might prevent erasure*
- Issues: Knowledge & capital intensive
- Also: there's a warhead there…

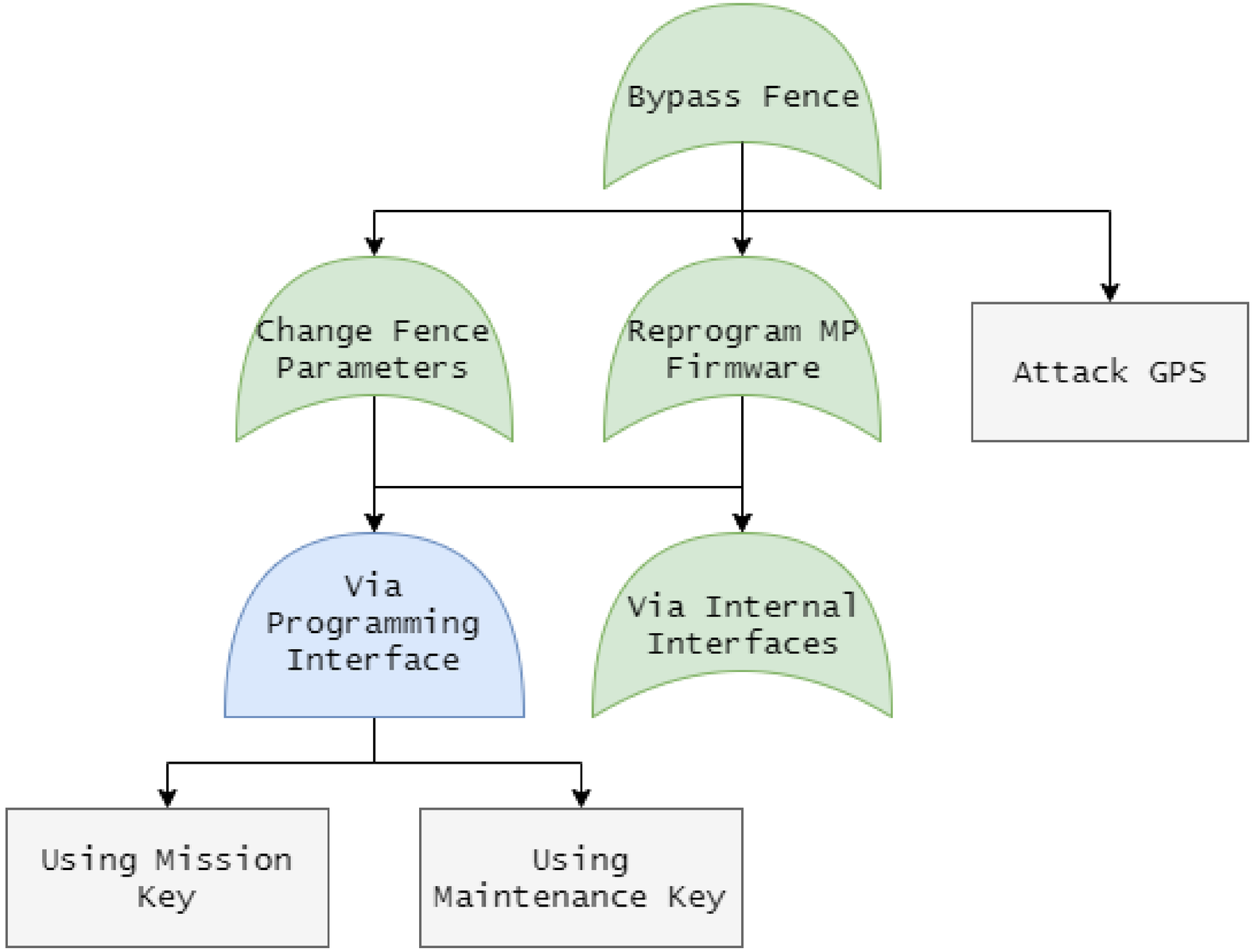
* https://www.blackhat.com/docs/us-15/materials/us-15-Thomas-Advanced-IC-Reverse-Engineering-Techniques-In-Depth-Analysis-Of-A-Modern-Smart-Card.pdf, https://pacsec.jp/psj13/psj2013-day2_Dmitry_starbug_slides_PacSec.pdf

ANTI-TAMPER MEASURES

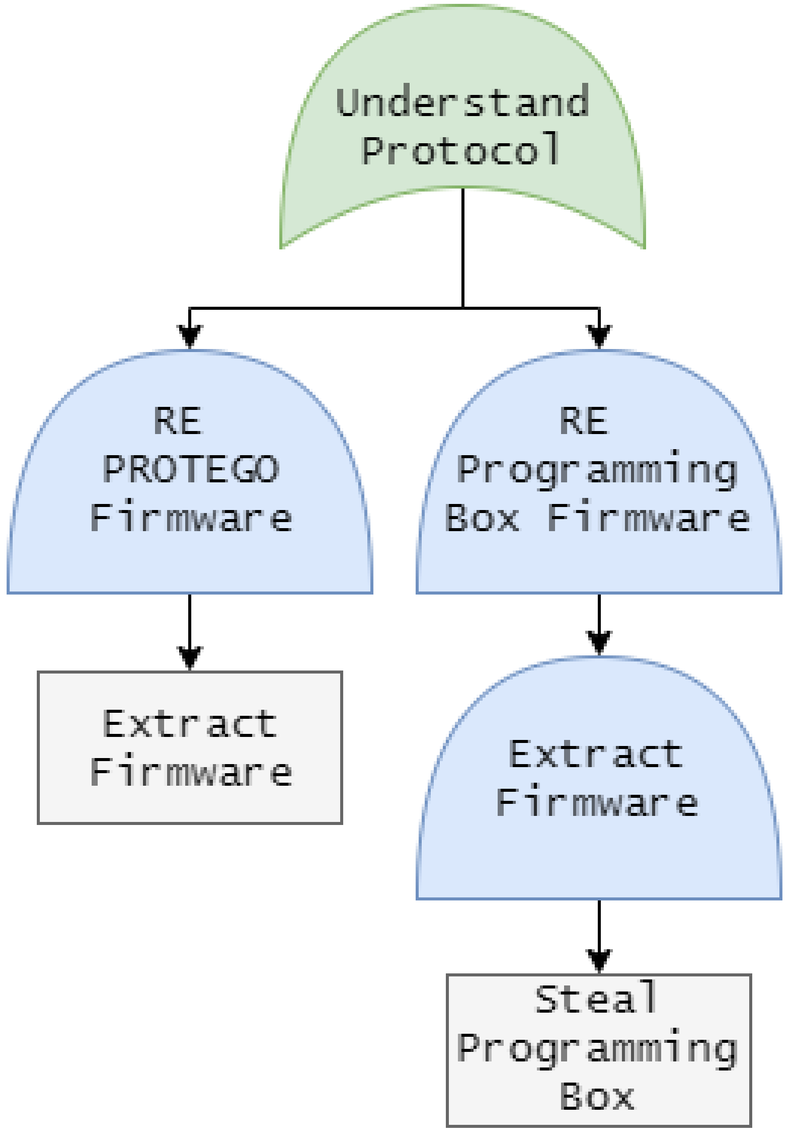
- Bigger issue: unencrypted seeker signals would mean tampered smart switch could render PROTEGO moot
  - *If seeker can get lock-on & fire signal from gripstock, it's over*

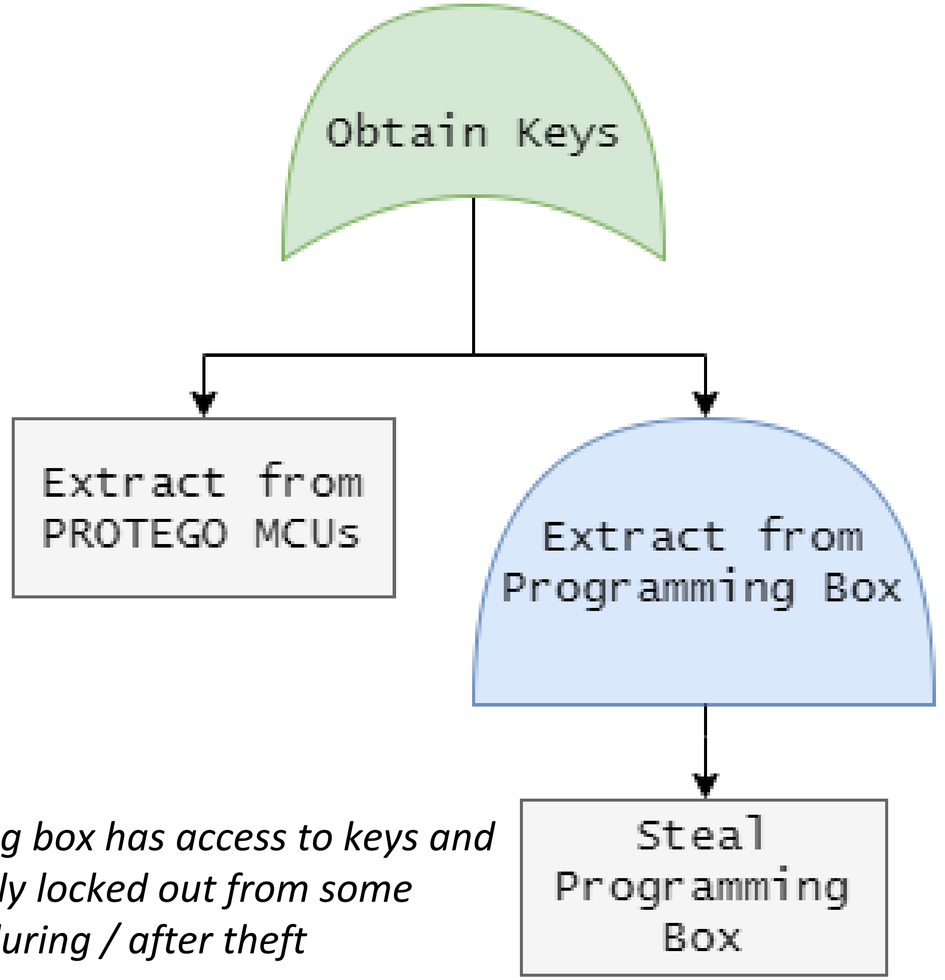
- Don't know if this is the case
- Don't know how hard tampering with that switch is

LOGICAL TAMPERING



LOGICAL TAMPERING



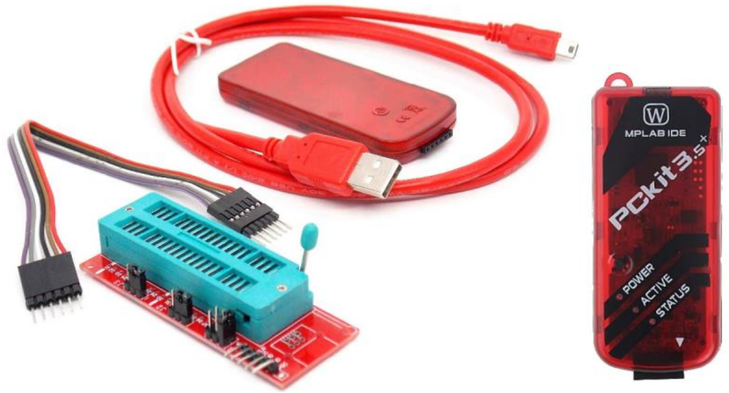


** Assuming box has access to keys and isn't rapidly locked out from some backend during / after theft*

Most approaches will likely require 'sacrificing' at least 1 MANPADs for research

EXTRACTING AND/OR MODIFYING KEYS & FIRMWARE

Debugging Interfaces



Side-Channel Analysis

Invasive Attacks

Software Bugs

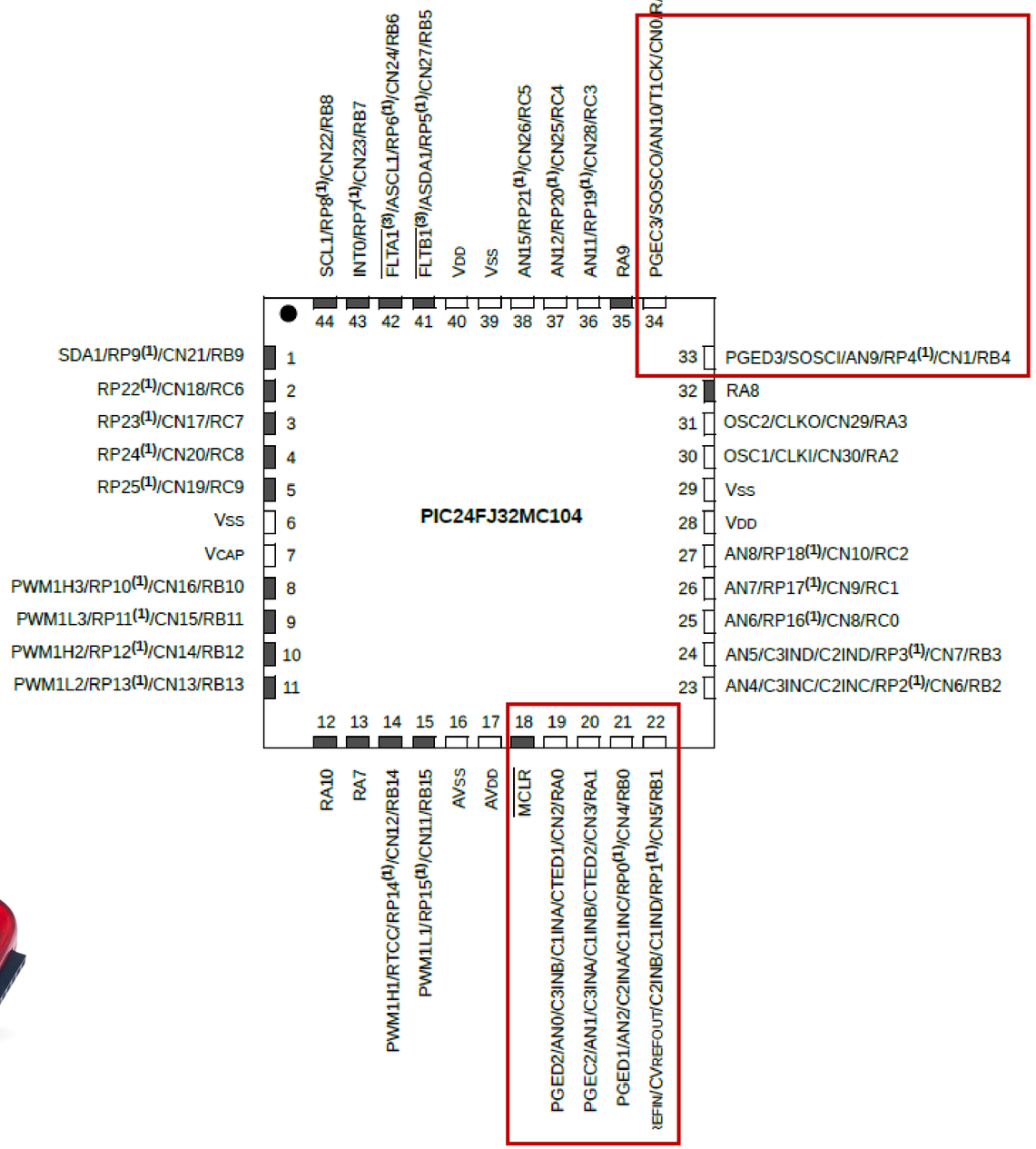
These approaches might trigger AT

BUT: maintenance key is never erased!

DEBUGGING INTERFACES

In-Circuit Serial Programming (ICSP)

1. Master Clear (MCLR)
2. Power (Vdd)
3. Ground (Vss)
4. Data (PGD)
5. Clock (PGC)

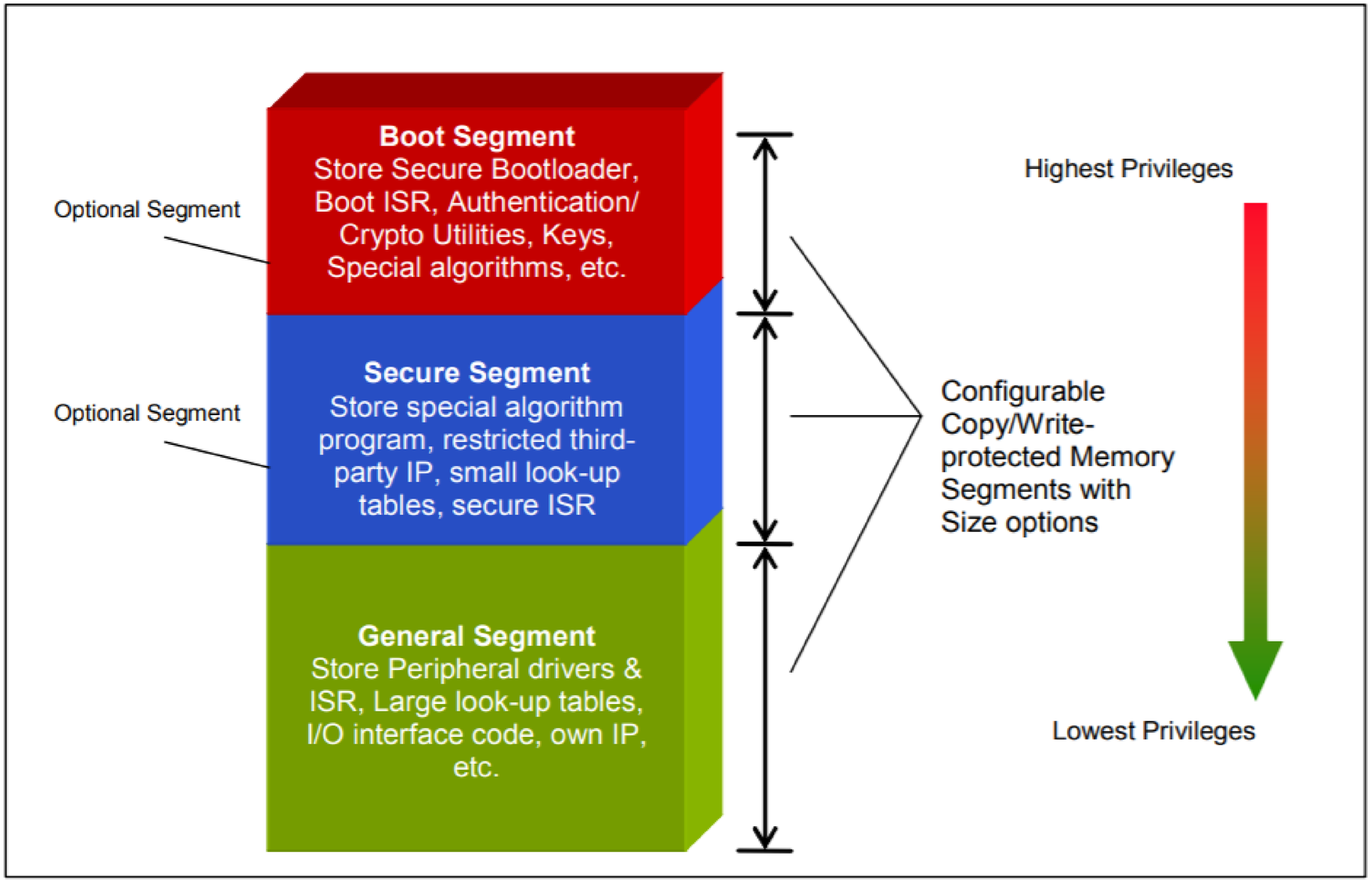


ISSUE: MICROCHIP CODEGUARD

Read-out & Write Protection

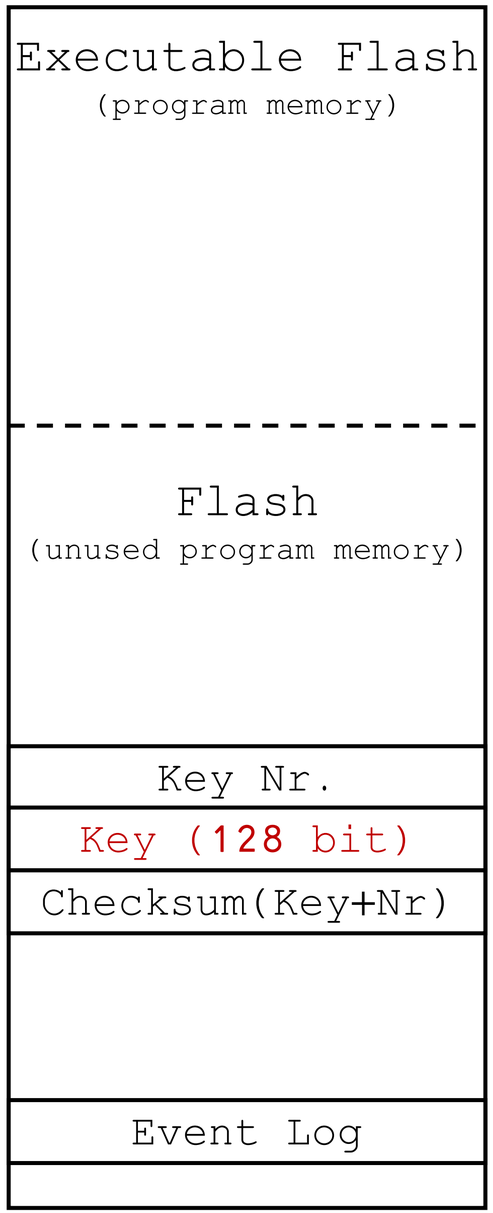
Configured via Configuration Words (CW)

Violation triggers Security Reset



* http://ww1.microchip.com/downloads/en/DeviceDoc/70179B.pdf, http://cs-people.bu.edu/rmancuso/courses/cs454_654-sp19/material/docs/dsPIC33F.23%20-%20CodeGuard%20Security.pdf

PROTEGO MCU MEMORY LAYOUT



1. Version Number
2. 16-bit image CRC calculated at startup

No mention of firmware authentication

No mention of hardware root of trust or secure element

Nothing beyond CodeGuard

If checksum does not match, key will not be loaded

Probably holds AT events that can be read out by programmer

CODEGUARD DISCLAIMER

Note the following details of the code protection feature on Microchip devices:

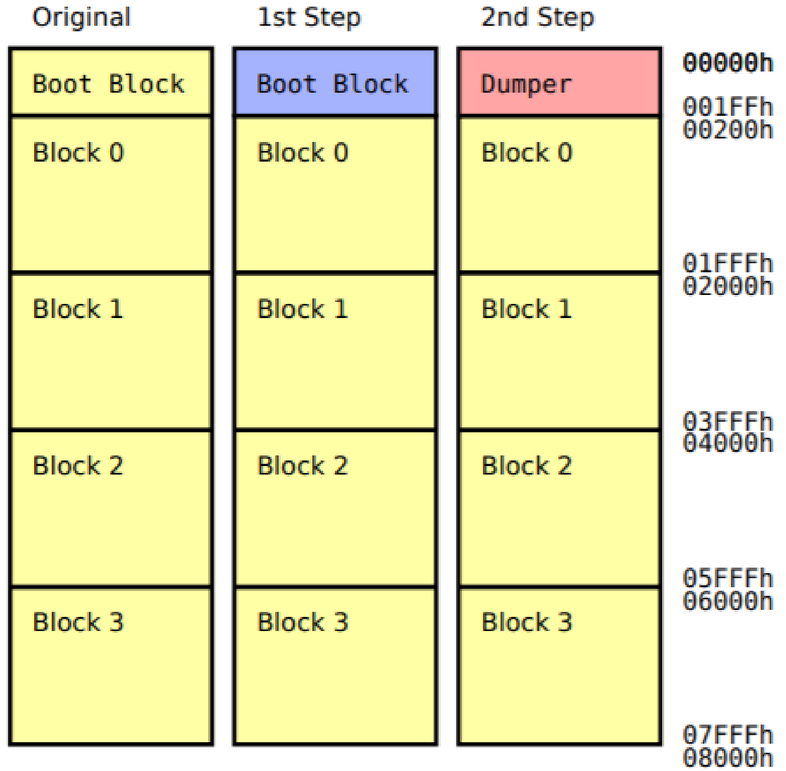
- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

CODEGUARD BASIC

Device Family	CodeGuard™ Security Implementation Type	Maximum Memory Segment Size (Bytes)		
		Boot Segment	Secure Segment	General Segment
All PIC24F devices	Basic	—	—	All on-chip Flash memory

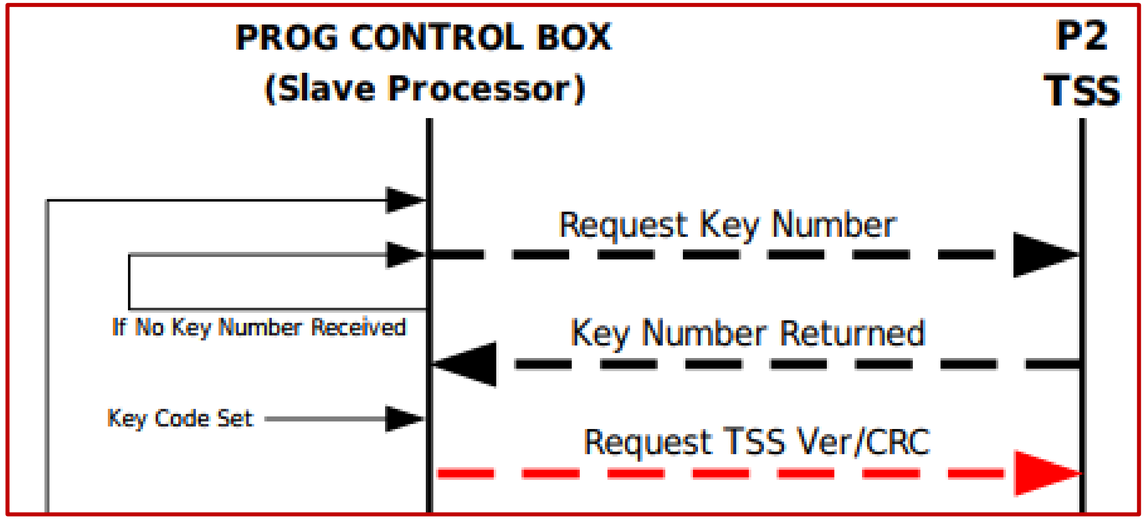
- Only support for *General Segment* Code & Write Protect
- No separate segments for bootloader or keys
- PIC18FXX2/XX8 suffered from '*heart of darkness*' attack, unclear whether similar attack applies to PIC24F



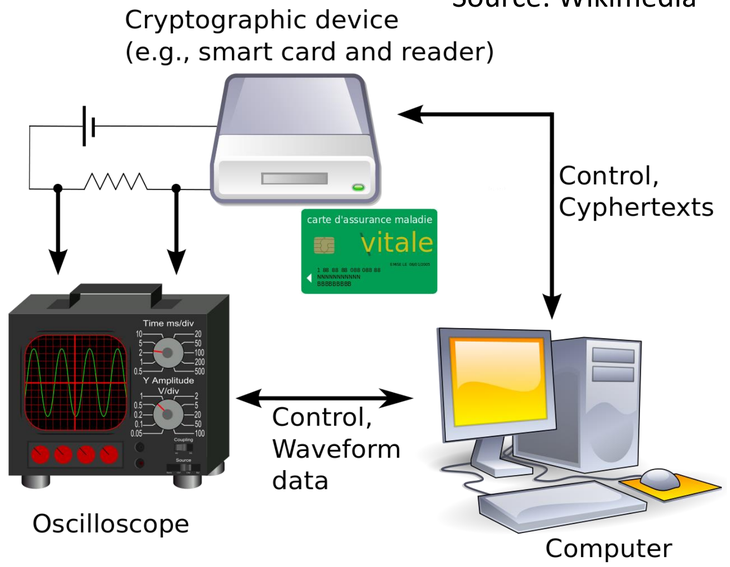
* https://www.openpcd.org/images/HID-iCLASS-security.pdf

SIDE-CHANNEL ATTACKS (SPA/DPA/CPA)

No hardware crypto, no SCA counter-measures



Source: Wikimedia

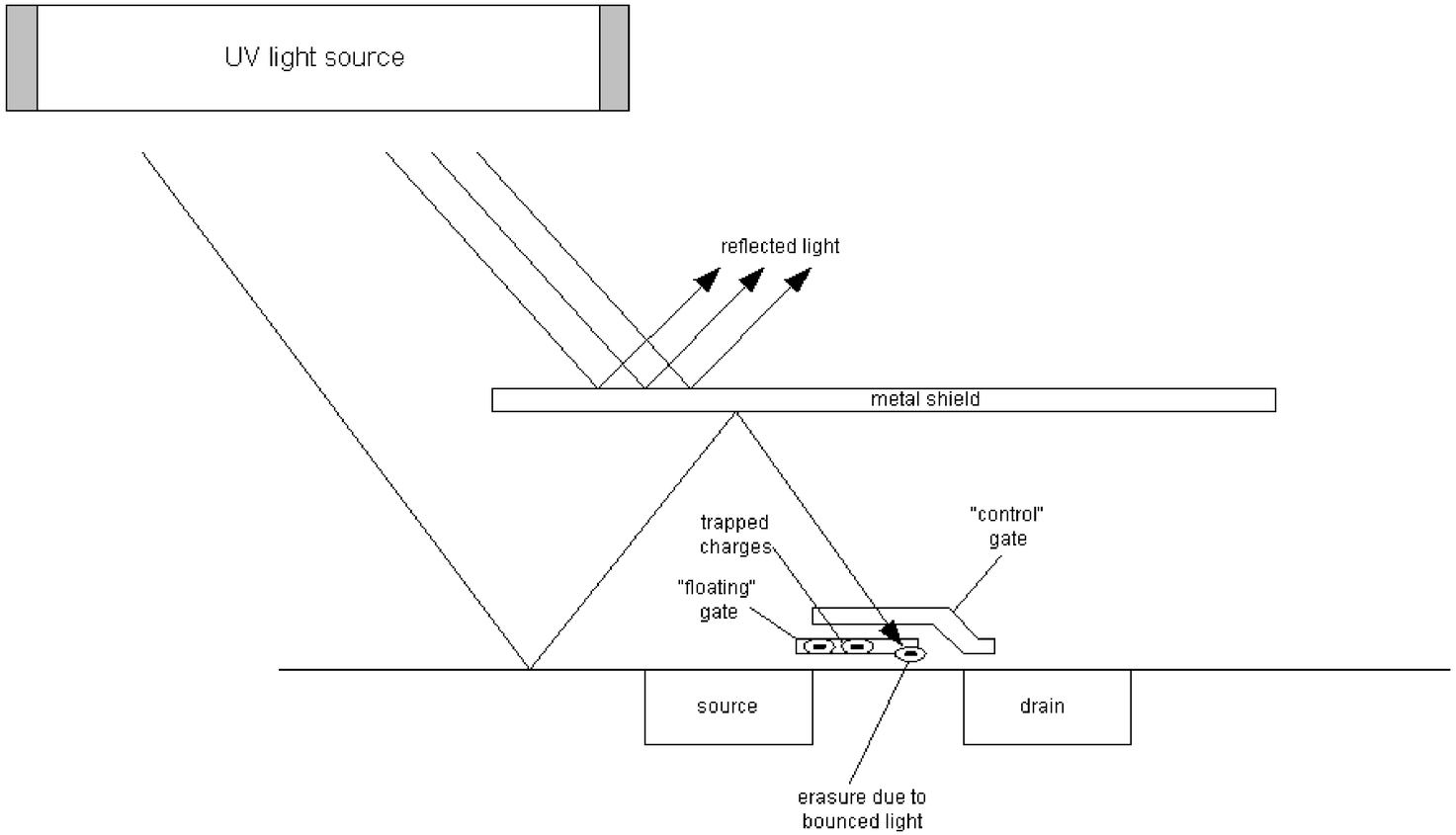


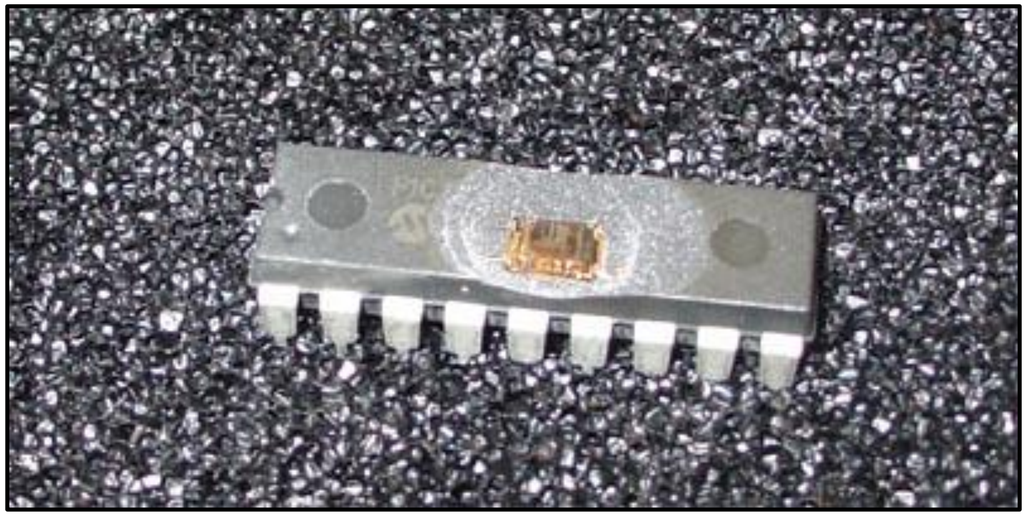
Probably no SW C-Ms in PROTEGO FW

Might affect power consumption adversely

Target maintenance key, extract & apply to different MANPADS

INVASIVE ATTACKS





PIC24FJ2 Series Microcontrollers MCU Code Extraction Crack,Break,Unlock

PIC24FJ32GB002	PIC24FJ32GB004	PIC24FJ32MC101	PIC24FJ32MC102
PIC24FJ32MC104	PIC24FJ48GA002	PIC24FJ48GA004	PIC24FJ64GA002

* http://siliconexposed.blogspot.com/2011/03/microchip-pic12f683-teardown.html, https://www.bunniestudios.com/blog/?page_id=40, http://www.unlock-ic.com/

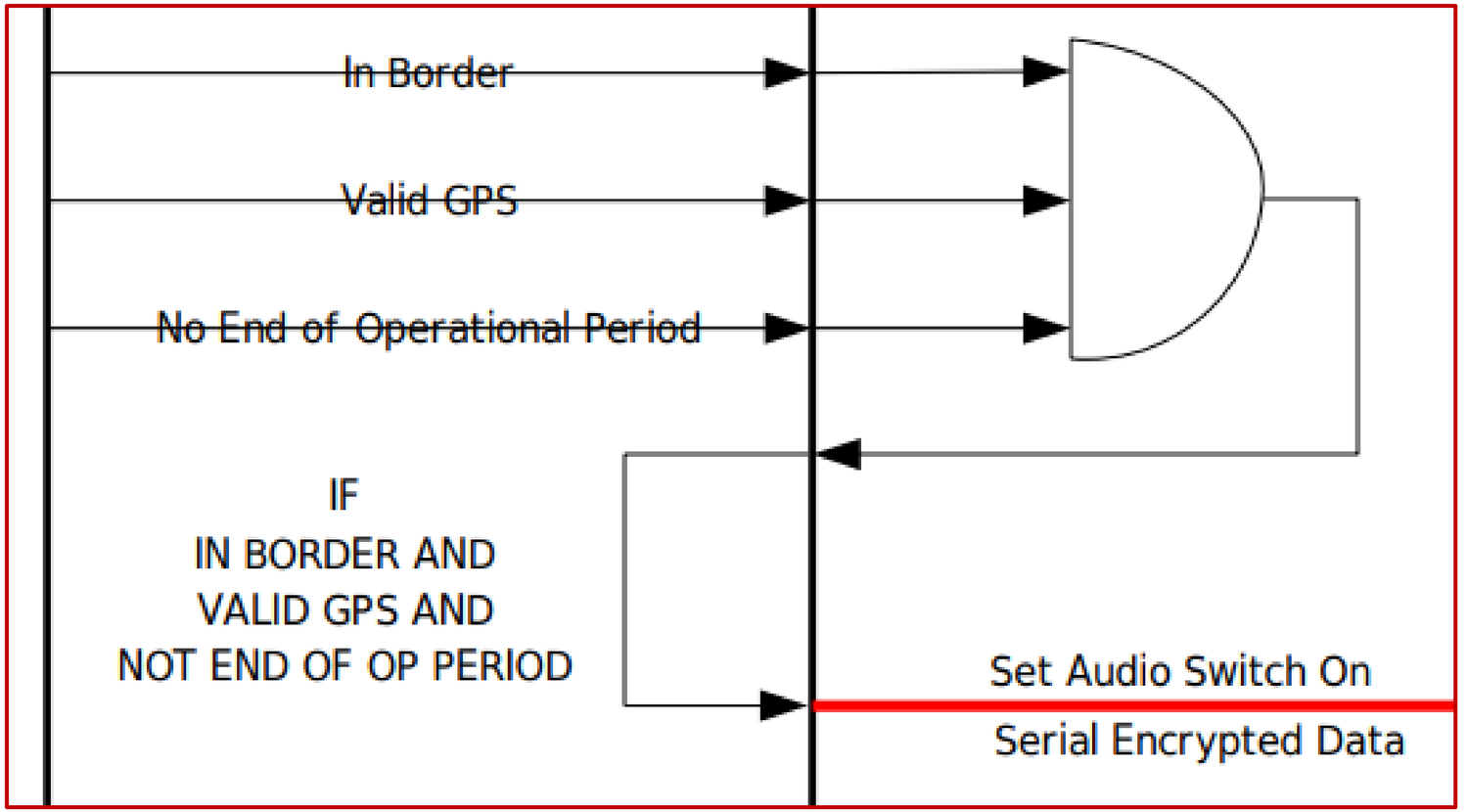
SOFTWARE VULNERABILITIES

ID	Summary
20	During an erase on MP and TSS turn off all unnecessary interrupts
40	When UART is connected, the state of MP Master is stale
41	MP and TSS were going to sleep when erase condition existed
42	Configuring Beacon Only Works Once in Tactical Mode
43	HW - SW Add control of AND2 (OB after being in once)
46	When BCU power is applied and them missing missile is activate, erase does not occur

- Memory corruption or State machine logic bugs
- Exploit a vuln to send a *smart switch close* command or exfiltrate keys
- Issue #1: tiny attack surface exposure over programming interface
- Issue #2: full-blackbox VR & XD is hellish, need firmware extraction

ATTACKING GPS

PROTEGO core security decision based on GPS-derived info (location & time)



GPS 101

- Global Navigation Satellite System (GNSS)

  GPS, GLONASS, Galileo, Beidou

- PROTEGO probably uses plain C/A codes from civilian signal

Band	Freq.	Description
L1	1575.42 MHz	Coarse acquisition (C/A) & encrypted precision (P(Y)) codes Civilian (L1C) & Military (M) codes on future block III satellites
L2	1227.60 MHz	P(Y) code, L2C & military codes on Block IIR-M and newer
L3	1381.05 MHz	Nuclear detonation detection (NUDET)
L4	1379.913 MHz	Studied for ionospheric correction
L5	1176.45 MHz	Proposed civilian Safety-of-Life (SoL) signal

GPS JAMMING

- If GPS is unavailable: MANPADS won’t fire.
- If GPS is unavailable: Possibly no key erasure

- Naïve approach: overpowering noise on L1 & L2 bands

- Jamming might be detected (signal anomalies)
- And corrected for (multi-src correlation, noise filtering)
- Or trigger key erasure

GPS JAMMING

* Effects of GNSS jammers and potential mitigation approaches - H. Kuusniemi
  A look at the threat of systematic jamming of GNSS - J. Curran et al.

- Smarter approach:
  combine jammer with GNSS info
- Trigger short & sparse bursts aligned with specific msg portions

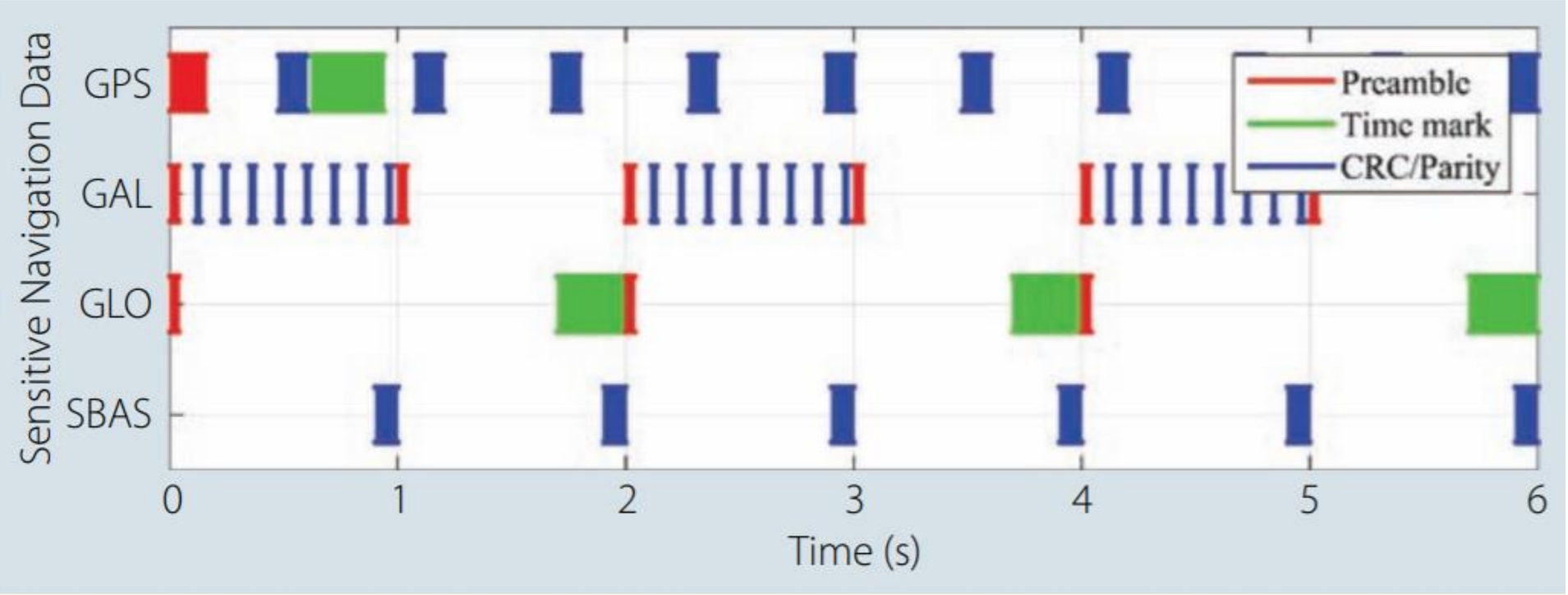


FIGURE 2 Position in time of various portions of sensitive data contained in each of the GPS, Galileo and GLONASS

GPS SPOOFING

- GPS is unauthenticated, weak signal
- Allows for signal replay / forging
- Commercial / SDR solutions have made this pretty accessible
- Collect in-fence signal, move MANPADS in Faraday cage, replay loop

* Another Place, Another Time - S. Gerling
Time and Position Spoofing with Open Source Projects - K. Wang et al.
Targeted GPS spoofing - B. Hermans et al.
https://www.gpsworld.com/defensesecurity-surveillanceassessing-spoofing-threat-3171/
https://github.com/osqzss/gps-sdr-sim

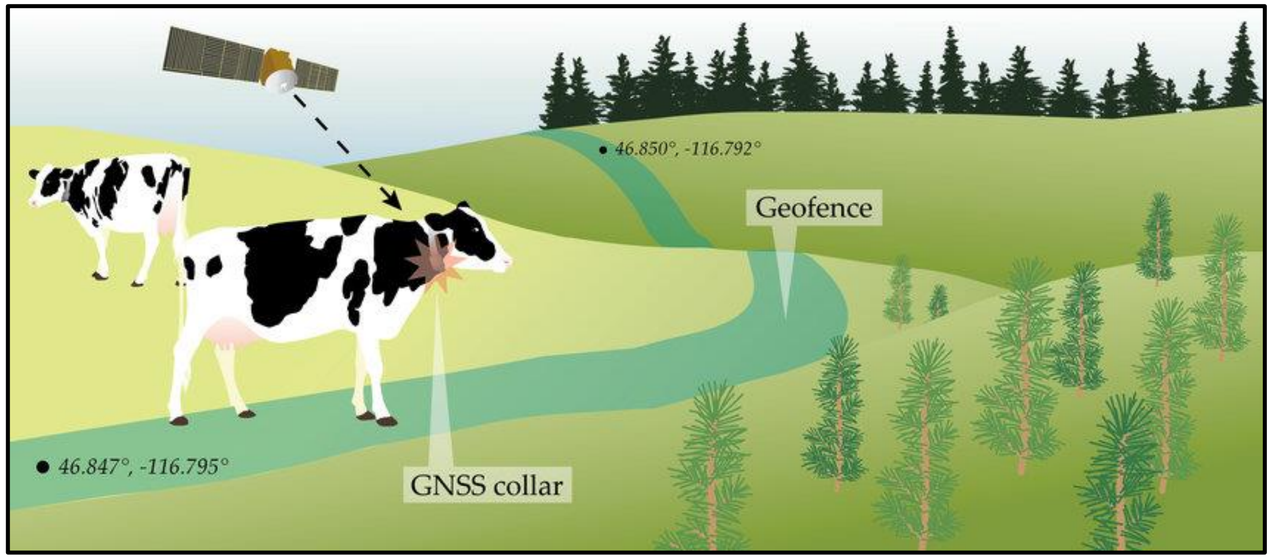
GPS SPOOFING

- Counter-Measures:
  anomaly detection: signal strength, latency, loss of lock, etc.
  multi-source correlation
  internal reference clock
  etc.
- Issue: active counter-measures drain power, not likely in PROTEGO
- Carry-off attack: carefully align spoofed signal, gradually increase power and take over while avoiding loss of lock or triggering CMs

CONCLUSION

SIMILAR SYSTEMS = SIMILAR ATTACKS

- Theft prevention (eg. Armored trucks)
- Ankle monitors
- Smart guns
- UAV area denial
- Autonomous driving
- Employee monitoring
- Livestock management (cyberpunk cattle rustlers?)



IS THIS STUFF ATTACKED IN PRACTICE?

Yes, especially through GPS jamming

Feds arrest rogue trucker after GPS jamming borks New Jersey airport test

Car thieves using GPS 'jammers'

'Jammers' overwhelm anti-theft devices on cars and lorries – and later versions could be used to disrupt air traffic

Organised crime 'routinely jamming GPS'

GPS Under Attack as Crooks, Rogue Workers Wage Electronic War

TLP: GREEN

FBI CYBER DIVISION

Private Industry Notification

DATE: 2 October 2014

PIN #: 141002-001

(U) Cargo Thieves use GPS Jammers to Mask GPS Trackers

(U) This Private Industry Notification (PIN) highlights the use of Global Positioning Systems (GPS) jammers by criminals to thwart law enforcement response and investigation into cargo thefts in the United States. Since at least February 2012, various law enforcement and private sector partners have reported that GPS tracking devices have been jammed by criminals engaged in nefarious activity including cargo theft and illicit shipping of goods. Although banned by federal law, the jammers are readily available over the Internet and easy to employ.

(U) GPS Jammers are Small and Unobtrusive

(U) GPS jammers are transmitters that block tracking devices from acquiring GPS broadcast signals by transmitting electromagnetic interference[a] (noise) on the same frequency[b]. They come in many shapes and sizes, with varying capabilities. Plugged into a standard cigarette lighter jack, a small jammer (pictured right) operating in the vehicle will disrupt GPS logging or GPS tracking systems for a radius of up to five yards. Mid-sized and larger jammers typically block a combination of GPS, cellphone, Wi-Fi, and other signals and thus also prevent the tracker from wirelessly reporting any location or status data. In a test conducted by a federal law enforcement agency, GPS jamming devices were determined to be effective to approximately 65 feet. A large GPS jammer can disrupt any tracking device or receiver within a radius of several hundred yards.

UNCLASSIFIED

(U) An example of a GPS Jammer

(U) Source: Los Angeles Sheriff's

* https://publicintelligence.net/fbi-cargo-thieves-gps-jammers/

CONCLUSION

- PROTEGO: Not a GPS-guided aircraft assassination module
- But likely MANPADS geofencing for covert arms supply
- Unclear where, when or if ever fielded. TIMBER SYCAMORE?
- Utilizes COTS technology in similar fashion to commercial systems

  A geofence is a geofence

- **Possible Achilles heels**:
  - Unencrypted seeker signals?
  - Lack of secure boot & firmware authentication
  - Global maintenance key
  - Reliance on civilian GPS without clear EW counter-measures

QUESTIONS?

@S4MVARTAKA

WWW.MIDNIGHTBLUELABS.COM