New York University Abu Dhabi
Modern Microprocessor Architectures Lab
nyuad.nyu.edu/momalab

Automated Reverse Engineering of Industrial Control Systems Binaries

Mihalis Maniatakos

Assistant Professor, NYU Abu Dhabi

@realmomalab

ICS cybersecurity landscape

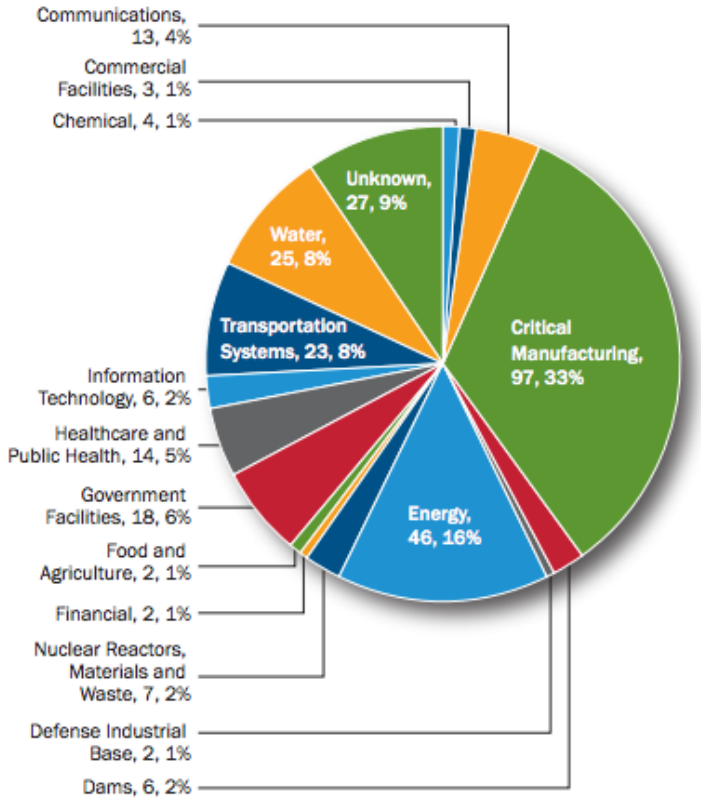
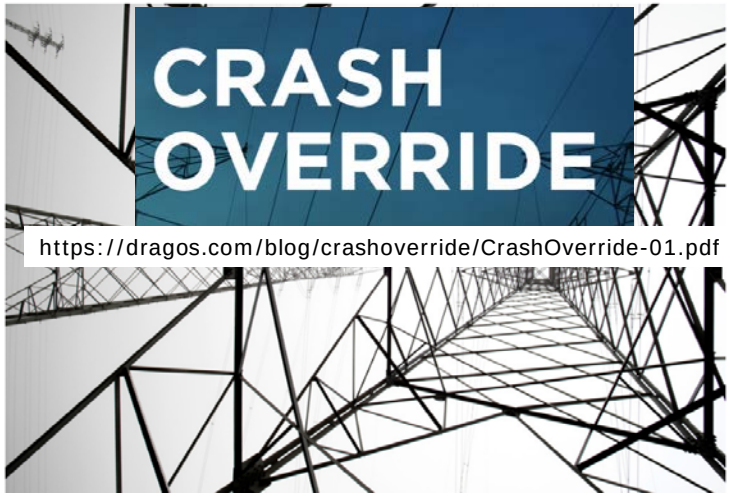


Figure 1. FY 2015 Incidents by Sector, 295 total.

Image Source:
ICS-CERT 2015 report

KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID



https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Why is it becoming worse?

- Advanced (“smart”) features
  - Microprocessor-based devices
- More COTS hardware/software
  - ARM/Linux
- Industrial Protocols

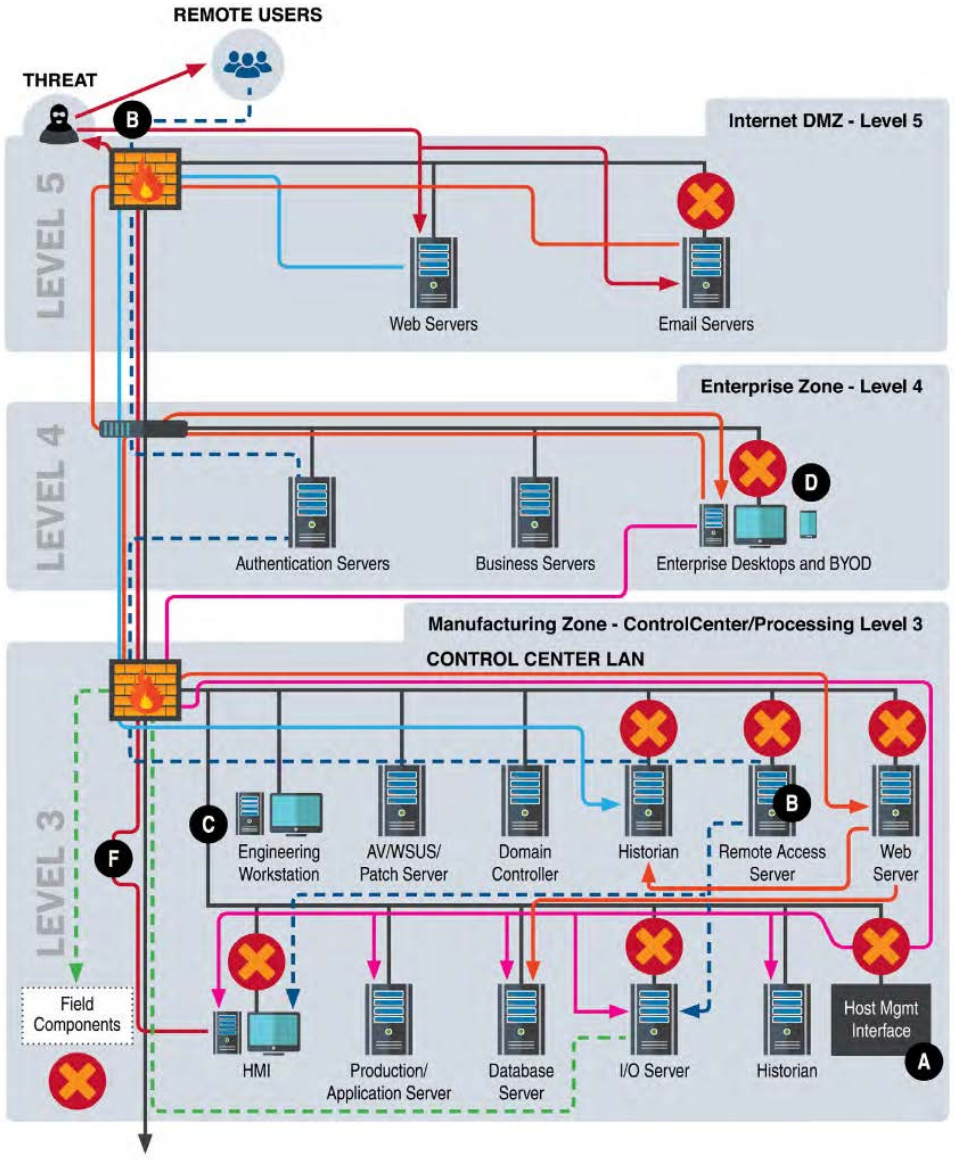
Is it getting worse?

ICS-CERT advisories snapshot for since 19th March 2019

- ICSA-19-099-01 : Siemens SIMOCODE pro V EIP
- ICSA-19-099-02 : Siemens Spectrum Power 4.7
- ICSA-19-099-03 : Siemens Industrial Products with OPC UA
- ICSA-19-099-04 : Siemens SINEMA Remote Connect
- ICSA-19-099-05 : Siemens RUGGEDCOM ROX II
- ICSA-19-099-06 : Siemens CP, SIAMTIC, SIMOCODE, SINAMICS, SITOP, and TIM
- ICSA-19-094-01 : Omron CX-Programmer
- ICSA-19-094-02 : Rockwell Automation Stratix 5400/5410/5700 and ArmorStratix 5700
- ICSA-19-094-03 : Rockwell Automation Stratix 5400/5410/5700/8000/8300 and ArmorStratix 5700
- ICSA-19-094-04 : Rockwell Automation Stratix 5950
- ICSA-19-092-01 : Advantech WebAccess/SCADA
- ICSA-19-087-01 : Rockwell Automation PowerFlex 525 AC Drives
- ICSA-19-085-01 : Siemens SCALANCE X
- ICSA-19-085-02 : PHOENIX CONTACT RAD-80211-XD
- ICSA-19-085-03 : ENTTEC Lighting Controllers
- ICSMA-19-080-01 : Medtronic Conexus Radio Frequency Telemetry Protocol
- ICSA-19-078-01 : AVEVA InduSoft Web Studio and InTouch Edge HMI
- ICSA-19-078-02 : Columbia Weather Systems MicroServer

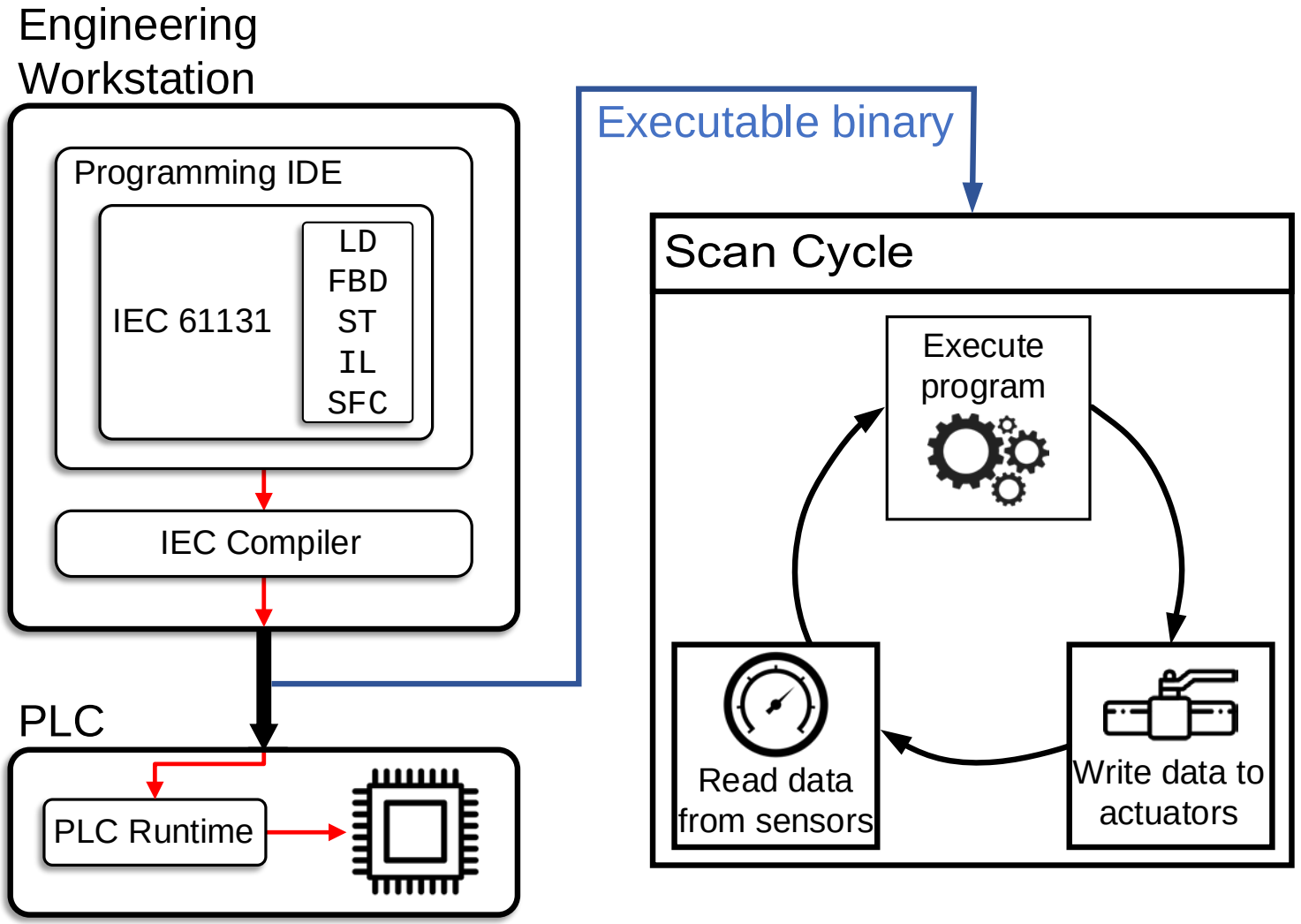
Attack points

https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf



PLC operation in ICS

PLC = Programmable Logic Controller



Why reverse engineer ICS binaries?

- Analyze PLC malware
- Recover lost source code

- Dynamic payload generation
- No need for C2 server (air-gap)

Why are ICS binaries “special”?

- Execution model
  - Scan cycle
- I/O operations
  - How and where are I/O operations?
- File formats
  - Custom & Proprietary
- Optimizations
  - Or lack thereof …

Methodology

- Phase 1:
  1. Binary format reverse engineering
  2. Build knowledge databases
- One-time cost
  - Small number of platforms
  - Manual or semi-automated analysis
- Phase 2:
  - Binary Analysis
- Automated
  - At-scale analyses
- Dissect binaries
- Reconstruct CFG
- Visualize and interact with results

ICSREF instantiation: CODESYS

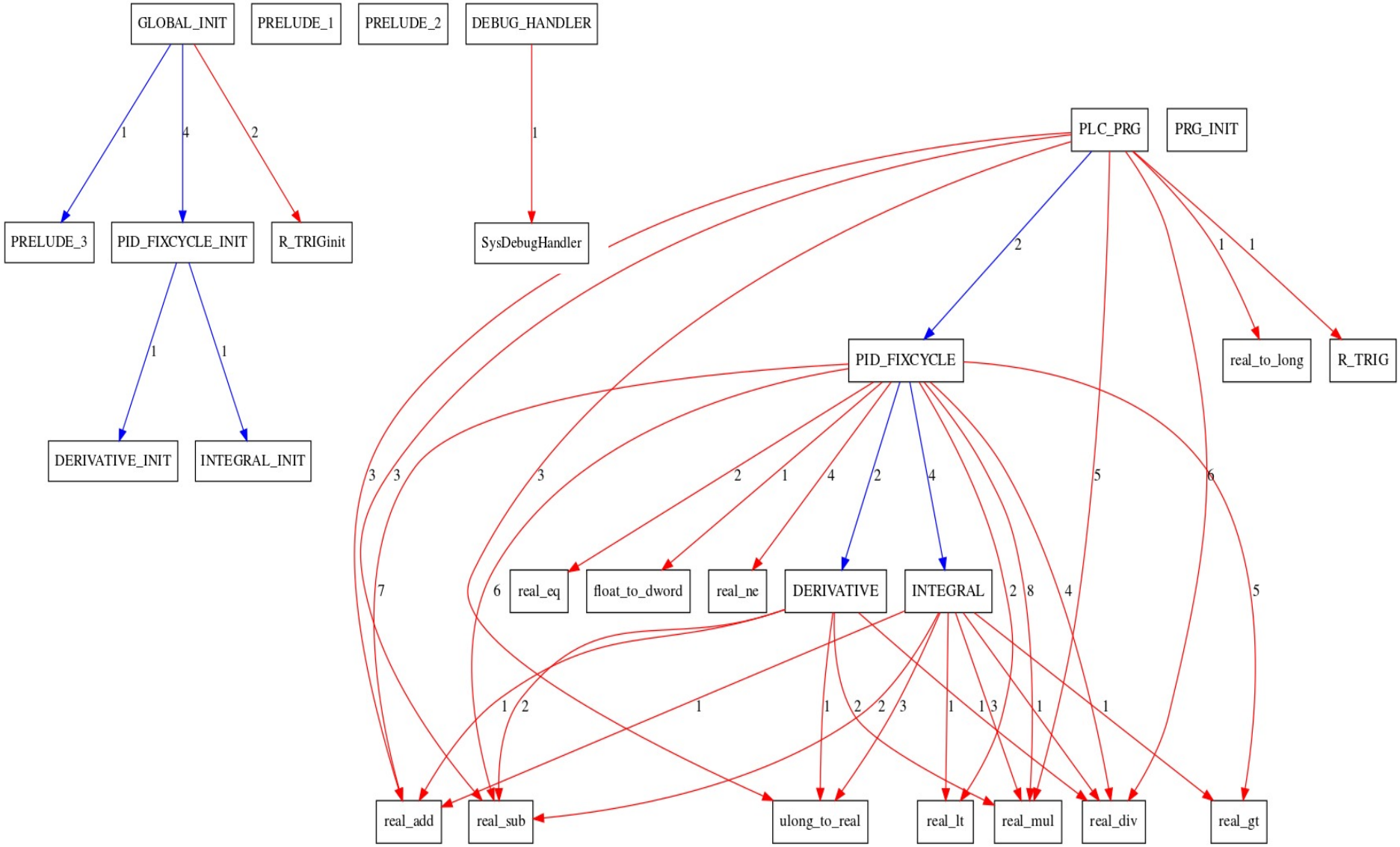
github.com/momalab/ICSREF

```
(icsref) me@example:$ ./icsref.py

ICS Reverse Engineering Framework

    _________________ ____  _____________
   /  _/ ____/ ___// __ \/ ____/ ____/
   / // /    \__ \/ /_/ / __/ / /_
 _/ // /___ ___/ / _, _/ /___/ __/
/___/\____//____/_/ |_/_____/_/

author: Tasos Keliris (@koukouviou)
Type <help> if you need a nudge
reversing@icsref:$
reversing@icsref:$ help

Documented commands (type help <topic>):
========================================
__changepid         changepid       exp_pid_match  history  pyscript  set
__replace_callname  cleanup         graphbuilder   load     quit      shell
_relative_load      cmdenvironment  hashmatch      pidargs  run       shortcuts
analyze             edit            help           py       save      show
```

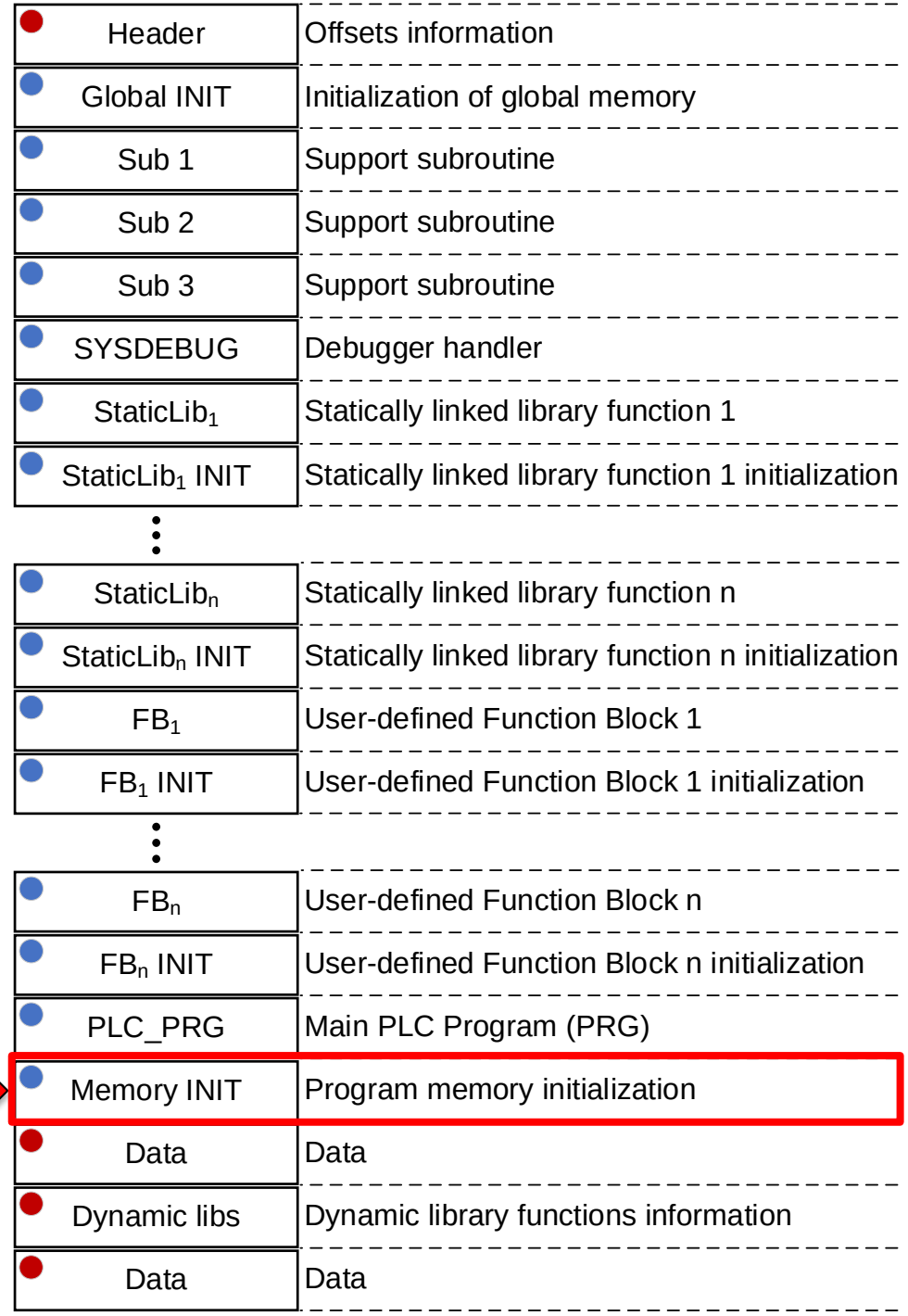
Before ICSREF

```
00000000 03 00 00 00 AA 33 00 00 50 01 00 00 DB 02 00 00 32 00 00 00 10 00 00 00 80 00 00 00 00 00 00 00 4C 2E 00 00 08 00 00 00 04 10 00 00
0000002c 40 31 00 00 FC FF 07 00 05 00 00 00 93 9A 17 00 FF 03 00 00 01 00 00 00 9C 33 00 00 00 00 00 00 00 00 00 00 0D C0 A0 E1 00 58 2D E9
00000058 0C B0 A0 E1 FF 5F 2D E9 B4 8D 9F E5 00 00 C8 E5 00 10 D8 E5 04 00 2D E5 04 90 2D E5 9C 2D 9F E5 02 90 88 E0 01 00 A0 E1 04 10 2D E5
00000084 04 90 2D E5 04 80 2D E5 04 E0 2D E5 7C 8D 9F E5 00 80 98 E5 0F E0 A0 E1 08 F0 A0 E1 00 00 A0 E1 04 E0 9D E4 04 80 9D E4 04 90 9D E4
000000b0 04 10 9D E4 04 90 9D E4 04 00 9D E4 00 10 A0 E1 01 10 48 E5 00 10 D8 E5 04 00 2D E5 04 90 2D E5 38 2D 9F E5 02 90 88 E0 01 00 A0 E1
000000dc 04 10 2D E5 04 90 2D E5 04 80 2D E5 04 E0 2D E5 20 8D 9F E5 00 80 98 E5 0F E0 A0 E1 08 F0 A0 E1 00 00 A0 E1 04 E0 9D E4 04 80 9D E4
00000108 04 90 9D E4 04 10 9D E4 04 90 9D E4 04 00 9D E4 00 10 A0 E1 01 10 48 E5 00 10 D8 E5 04 00 2D E5 DC 2C 9F E5 02 00 88 E0 04 90 2D E5
00000134 04 80 2D E5 04 E0 2D E5 C4 8C 9F E5 00 80 98 E5 0F E0 A0 E1 08 F0 A0 E1 00 00 A0 E1 04 E0 9D E4 04 80 9D E4 04 90 9D E4 04 00 9D E4
00000160 00 10 A0 E1 01 10 48 E5 00 10 A0 E3 17 12 48 E5 00 10 A0 E3 16 12 48 E5 84 1C 9F E5 55 13 08 E5 78 1C 9F E5 51 13 08 E5 6C 1C 9F E5
0000018c 4D 13 08 E5 68 1C 9F E5 49 13 08 E5 58 1C 9F E5 45 13 08 E5 4C 1C 9F E5 41 13 08 E5 40 1C 9F E5 3D 13 08 E5 34 1C 9F E5 39 13 08 E5
000001b8 28 1C 9F E5 35 13 08 E5 2C 1C 9F E5 31 13 08 E5 00 10 A0 E3 2D 13 08 E5 0C 1C 9F E5 29 13 08 E5 00 1C 9F E5 25 13 08 E5 0C 1C 9F E5
000001e4 21 13 08 E5 00 10 A0 E3 1D 13 08 E5 E4 1B 9F E5 19 13 08 E5 00 10 A0 E3 D4 2B 9F E5 B2 10 88 E1 01 10 A0 E3 C4 2B 9F E5 B2 10 88 E1
00000210 02 10 A0 E3 B4 2B 9F E5 B2 10 88 E1 03 10 A0 E3 A4 2B 9F E5 B2 10 88 E1 04 10 A0 E3 94 2B 9F E5 B2 10 88 E1 05 10 A0 E3 84 2B 9F E5
0000023c B2 10 88 E1 06 10 A0 E3 74 2B 9F E5 B2 10 88 E1 00 10 A0 E3 64 2B 9F E5 B2 10 88 E1 01 10 A0 E3 54 2B 9F E5 B2 10 88 E1 02 10 A0 E3
00000268 44 2B 9F E5 B2 10 88 E1 03 10 A0 E3 34 2B 9F E5 B2 10 88 E1 04 10 A0 E3 24 2B 9F E5 B2 10 88 E1 05 10 A0 E3 14 2B 9F E5 B2 10 88 E1
00000294 06 10 A0 E3 04 2B 9F E5 B2 10 88 E1 07 10 A0 E3 F4 2A 9F E5 B2 10 88 E1 08 10 A0 E3 E4 2A 9F E5 B2 10 88 E1 09 10 A0 E3 D4 2A 9F E5
000002c0 B2 10 88 E1 0A 10 A0 E3 C4 2A 9F E5 B2 10 88 E1 0B 10 A0 E3 B4 2A 9F E5 B2 10 88 E1 0C 10 A0 E3 A4 2A 9F E5 B2 10 88 E1 0D 10 A0 E3
000002ec 94 2A 9F E5 B2 10 88 E1 0E 10 A0 E3 84 2A 9F E5 B2 10 88 E1 0F 10 A0 E3 74 2A 9F E5 B2 10 88 E1 10 10 A0 E3 64 2A 9F E5 B2 10 88 E1
00000318 11 10 A0 E3 54 2A 9F E5 B2 10 88 E1 12 10 A0 E3 44 2A 9F E5 B2 10 88 E1 13 10 A0 E3 34 2A 9F E5 B2 10 88 E1 14 10 A0 E3 24 2A 9F E5
00000344 B2 10 88 E1 15 10 A0 E3 14 2A 9F E5 B2 10 88 E1 16 10 A0 E3 04 2A 9F E5 B2 10 88 E1 17 10 A0 E3 F4 29 9F E5 B2 10 88 E1 18 10 A0 E3
00000370 E4 29 9F E5 B2 10 88 E1 19 10 A0 E3 D4 29 9F E5 B2 10 88 E1 1A 10 A0 E3 C4 29 9F E5 B2 10 88 E1 1B 10 A0 E3 B4 29 9F E5 B2 10 88 E1
0000039c 1C 10 A0 E3 A4 29 9F E5 B2 10 88 E1 1D 10 A0 E3 94 29 9F E5 B2 10 88 E1 1E 10 A0 E3 84 29 9F E5 B2 10 88 E1 1F 10 A0 E3 74 29 9F E5
000003c8 B2 10 88 E1 20 10 A0 E3 64 29 9F E5 B2 10 88 E1 21 10 A0 E3 54 29 9F E5 B2 10 88 E1 22 10 A0 E3 44 29 9F E5 B2 10 88 E1 23 10 A0 E3
000003f4 34 29 9F E5 B2 10 88 E1 28 19 9F E5 20 29 9F E5 B2 10 88 E1 14 19 9F E5 0C 29 9F E5 B2 10 88 E1 00 19 9F E5 F8 28 9F E5 B2 10 88 E1
00000420 EC 18 9F E5 E4 28 9F E5 B2 10 88 E1 D8 18 9F E5 D0 28 9F E5 B2 10 88 E1 C4 18 9F E5 BC 28 9F E5 B2 10 88 E1 B0 18 9F E5 A8 28 9F E5
0000044c B2 10 88 E1 9C 18 9F E5 94 28 9F E5 B2 10 88 E1 88 18 9F E5 80 28 9F E5 B2 10 88 E1 74 18 9F E5 6C 28 9F E5 B2 10 88 E1 60 18 9F E5
00000478 58 28 9F E5 B2 10 88 E1 4C 18 9F E5 44 28 9F E5 B2 10 88 E1 38 18 9F E5 30 28 9F E5 B2 10 88 E1 24 18 9F E5 1C 28 9F E5 B2 10 88 E1
000004a4 10 18 9F E5 08 28 9F E5 B2 10 88 E1 FC 17 9F E5 F4 27 9F E5 B2 10 88 E1 E8 17 9F E5 E0 27 9F E5 B2 10 88 E1 D4 17 9F E5 CC 27 9F E5
000004d0 B2 10 88 E1 C0 17 9F E5 B8 27 9F E5 B2 10 88 E1 AC 17 9F E5 A4 27 9F E5 B2 10 88 E1 98 17 9F E5 90 27 9F E5 B2 10 88 E1 84 17 9F E5
000004fc 7C 27 9F E5 B2 10 88 E1 70 17 9F E5 68 27 9F E5 B2 10 88 E1 5C 17 9F E5 54 27 9F E5 B2 10 88 E1 00 10 A0 E3 44 27 9F E5 B2 10 88 E1
00000528 01 10 A0 E3 34 27 9F E5 B2 10 88 E1 02 10 A0 E3 24 27 9F E5 B2 10 88 E1 04 10 A0 E3 14 27 9F E5 B2 10 88 E1 08 10 A0 E3 04 27 9F E5
00000554 B2 10 88 E1 10 10 A0 E3 F4 26 9F E5 B2 10 88 E1 11 10 A0 E3 E4 26 9F E5 B2 10 88 E1 12 10 A0 E3 D4 26 9F E5 B2 10 88 E1 00 10 A0 E3
00000580 C4 26 9F E5 B2 10 88 E1 01 10 A0 E3 B4 26 9F E5 B2 10 88 E1 02 10 A0 E3 A4 26 9F E5 B2 10 88 E1 03 10 A0 E3 94 26 9F E5 B2 10 88 E1
000005ac 04 10 A0 E3 84 26 9F E5 B2 10 88 E1 03 10 A0 E3 74 26 9F E5 B2 10 88 E1 10 10 A0 E3 64 26 9F E5 B2 10 88 E1 01 10 A0 E3 54 26 9F E5
000005d8 B2 10 88 E1 02 10 A0 E3 44 26 9F E5 B2 10 88 E1 04 10 A0 E3 34 26 9F E5 B2 10 88 E1 05 10 A0 E3 24 26 9F E5 B2 10 88 E1 06 10 A0 E3
00000604 14 26 9F E5 B2 10 88 E1 07 10 A0 E3 04 26 9F E5 B2 10 88 E1 0F 10 A0 E3 F4 25 9F E5 B2 10 88 E1 17 10 A0 E3 E4 25 9F E5 B2 10 88 E1
00000630 16 10 A0 E3 D4 25 9F E5 B2 10 88 E1 C8 15 9F E5 5D 12 08 E5 BC 15 9F E5 59 12 08 E5 00 10 A0 E3 AC 25 9F E5 B2 10 88 E1 01 10 A0 E3
0000065c 9C 25 9F E5 B2 10 88 E1 01 10 A0 E3 8C 25 9F E5 B2 10 88 E1 02 10 A0 E3 7C 25 9F E5 B2 10 88 E1 03 10 A0 E3 6C 25 9F E5 B2 10 88 E1
00000688 04 10 A0 E3 5C 25 9F E5 B2 10 88 E1 05 10 A0 E3 4C 25 9F E5 B2 10 88 E1 06 10 A0 E3 3C 25 9F E5 B2 10 88 E1 07 10 A0 E3 2C 25 9F E5
000006b4 B2 10 88 E1 07 10 A0 E3 1C 25 9F E5 B2 10 88 E1 08 10 A0 E3 0C 25 9F E5 B2 10 88 E1 09 10 A0 E3 FC 24 9F E5 B2 10 88 E1 0A 10 A0 E3
000006e0 EC 24 9F E5 B2 10 88 E1 0B 10 A0 E3 DC 24 9F E5 B2 10 88 E1 0C 10 A0 E3 CC 24 9F E5 B2 10 88 E1 0D 10 A0 E3 BC 24 9F E5 B2 10 88 E1
0000070c 0E 10 A0 E3 AC 24 9F E5 B2 10 88 E1 0F 10 A0 E3 9C 24 9F E5 B2 10 88 E1 10 10 A0 E3 8C 24 9F E5 B2 10 88 E1 11 10 A0 E3 7C 24 9F E5
```

After ICSREF



File format: Memory map



Legend
- Code
- Data

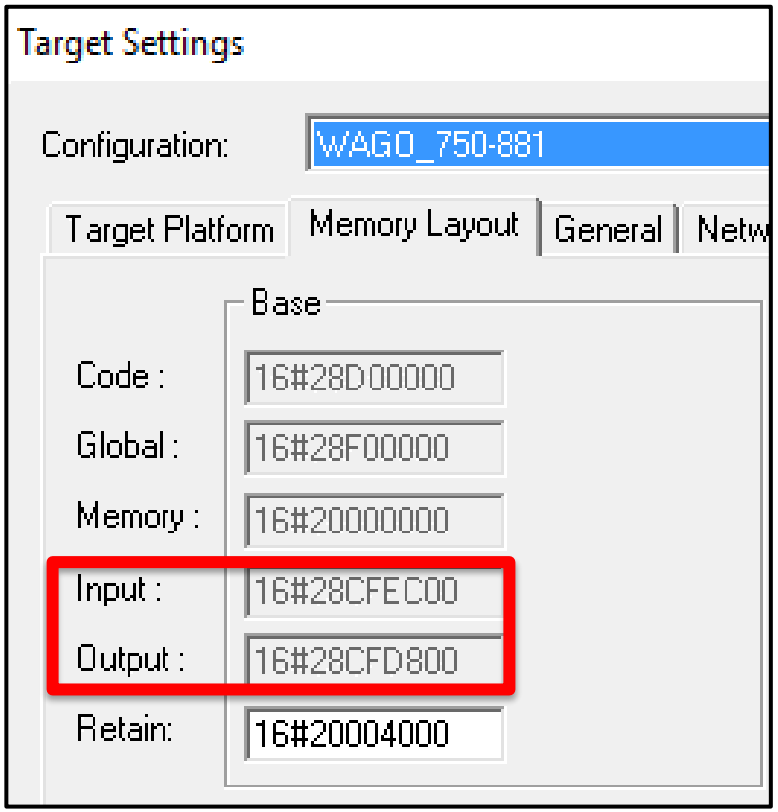
```
# Subroutine entry point
   MOV     R12, SP
   STMFD   SP!, {R11,R12,LR}
# Code
   ...
   ...
```

```
# Code
   ...
   ...
# Call other subroutine
   STR     Ri, [SP,#-4]!
   STR     LR, [SP,#-4]!
   LDR     Ri, =SUB_OFFSET
   LDR     Ri, [Ri]
   MOV     LR, PC
   MOV     PC, Ri
   NOP
   LDR     LR, [SP],#4
   LDR     Ri, [SP],#4
# Code
   ...
   ...
# Data section in code
   B       loc_Y
# Data
   0xCAFEBABE
   0xDEADBEEF
   ...
   ...
```

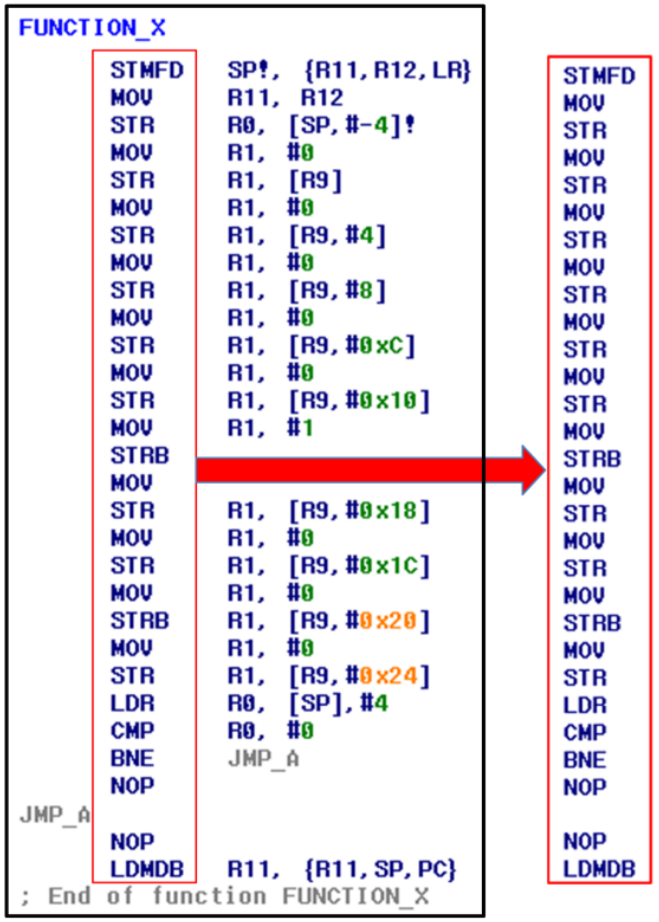
```
loc_Y:
# Code
   ...
   ...
# Subroutine exit
   LDMDB   R11, {R11,SP,PC}
# Data
   0xCAFEBABE
   0xDEADBEEF
   ...
   ...
```

Knowledge databases

- I/O memory maps

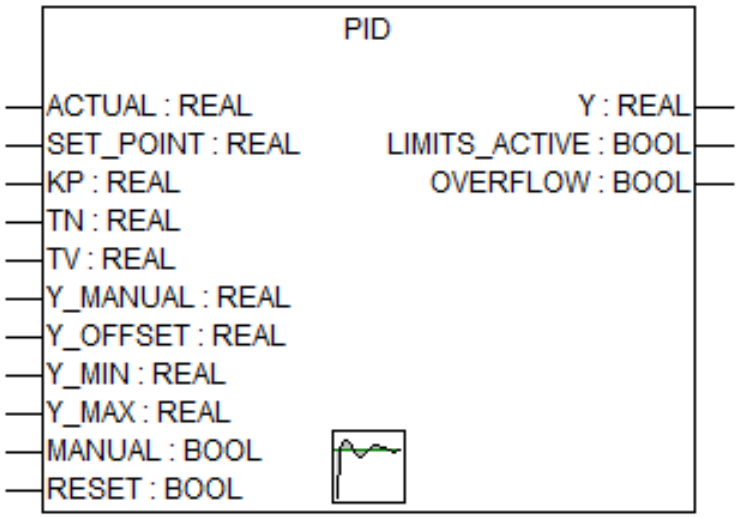


- Function signatures



Finding function arguments

- Arguments passed on the stack
- Symbolic execution
  - Extract parameters




```
LDR     R0, [R8,#0xA4]  ; R0=[0x3408] SIM_xmeas07
STR     R0, [R8,#-0xF4] ; [0x3270]=SIM_xmeas07
LDR     R0, [R8,#-0x350] ; R0=[0x3014] Pressure_Setpoint
STR     R0, [R8,#-0xF0] ; [0x3274]=Pressure_Setpoint
LDR     R0, [R8,#-0x34C] ; R0=[0x3018] Pressure_KP
STR     R0, [R8,#-0xEC] ; [0x3278]=Pressure_KP
LDR     R0, [R8,#-0x348] ; R0=[0x301C] Pressure_KI
STR     R0, [R8,#-0xE8] ; [0x327C]=Pressure_KI
MOV     R0, #0          ; R0=0.0
STR     R0, [R8,#-0xE4] ; [0x3280]=0.0 (Derivative term)
LDR     R0, [R8,#0x9C]  ; R0=[0x3400] Pressure_Manual
STR     R0, [R8,#-0xE0] ; [0x3284]=Pressure_Manual
LDR     R0, [R8,#-0x340] ; R0=[0x3024] Pressure_Output_Min
STR     R0, [R8,#-0xD8] ; [0x328C]=Pressure_Output_Min
LDR     R0, [R8,#-0x344] ; R0=[0x3020] Pressure_Output_Max
STR     R0, [R8,#-0xD4] ; [0x3290]=Pressure_Output_Max
LDR     R1, =0x28CFEC04 ; Load from Memory
LDRB    R2, [R1]        ; R2=[0x28CFEC04] AP_plc_reset
AND     R0, R2, #1      ; Rd = Op1 & Op2
STRB    R0, [R8,#-0xCF] ; [0x3295]=AP_plc_reset
LDR     R0, [R8,#-0x32C] ; R0=[0x3038] Cycle_Time
STR     R0, [R8,#-0xCC] ; [0x3298]=Cycle_Time
NOP                     ; No Operation
STR     R9, [SP,#-4]!   ; Store to Memory
LDR     R0, =0xFFFFFEAC ; Load from Memory
ADD     R9, R8, R0      ; R9=0x3210
STR     R9, [SP,#-4]!   ; Store to Memory
STR     R8, [SP,#-4]!   ; Store to Memory
STR     LR, [SP,#-4]!   ; Store to Memory
LDR     R8, =0x128      ; PID_FIXCYCLE
LDR     R8, [R8]        ; Load from Memory
MOV     LR, PC          ; Rd = Op2
```

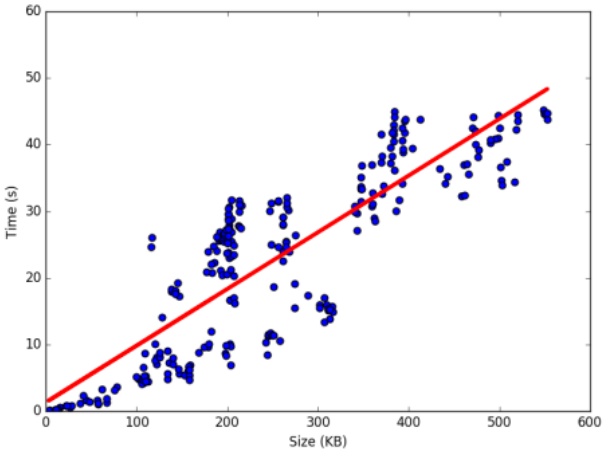
ICSREF correctness evaluation

- In-house binaries
- GitHub
  - 55 users
  - 127 repositories
  - 471 source code and binaries
- 266 binaries used for testing
  - The other projects are code stubs or corrupted

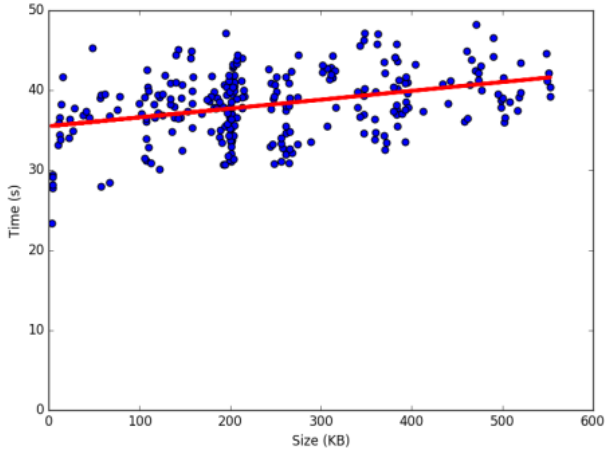
Vendor	Number of projects
Wago	320
BECKHOFF	71
OWEN	33
STW	24
CODESYS SoftPLC	7
ALTUS	7
TTCONTROL	2
ifm electronic	2
LENZE	1
Googol	1
FESTO	1
Bosch Rexroth	1
BERGHOF	1
Total	471

ICSREF performance

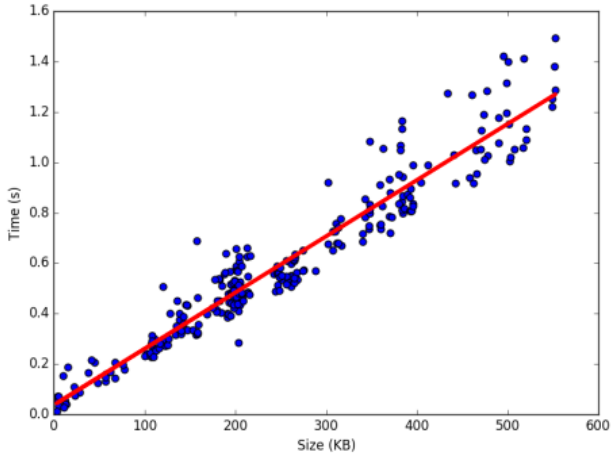
Dell XPS 9360: Intel i7-7500U CPU, 16 GB RAM, Ubuntu 16.04



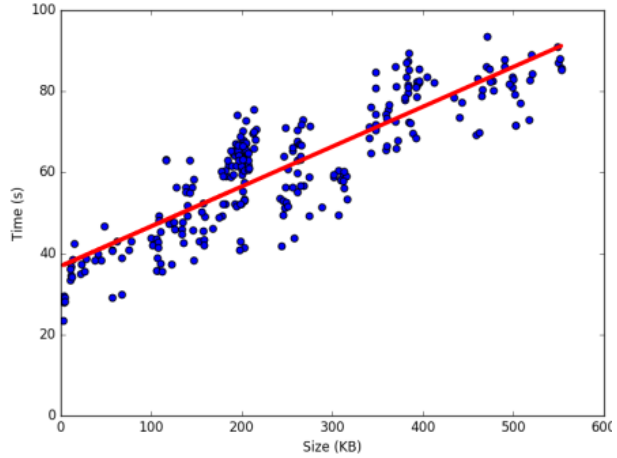
(a) radare2 time



(b) angr time



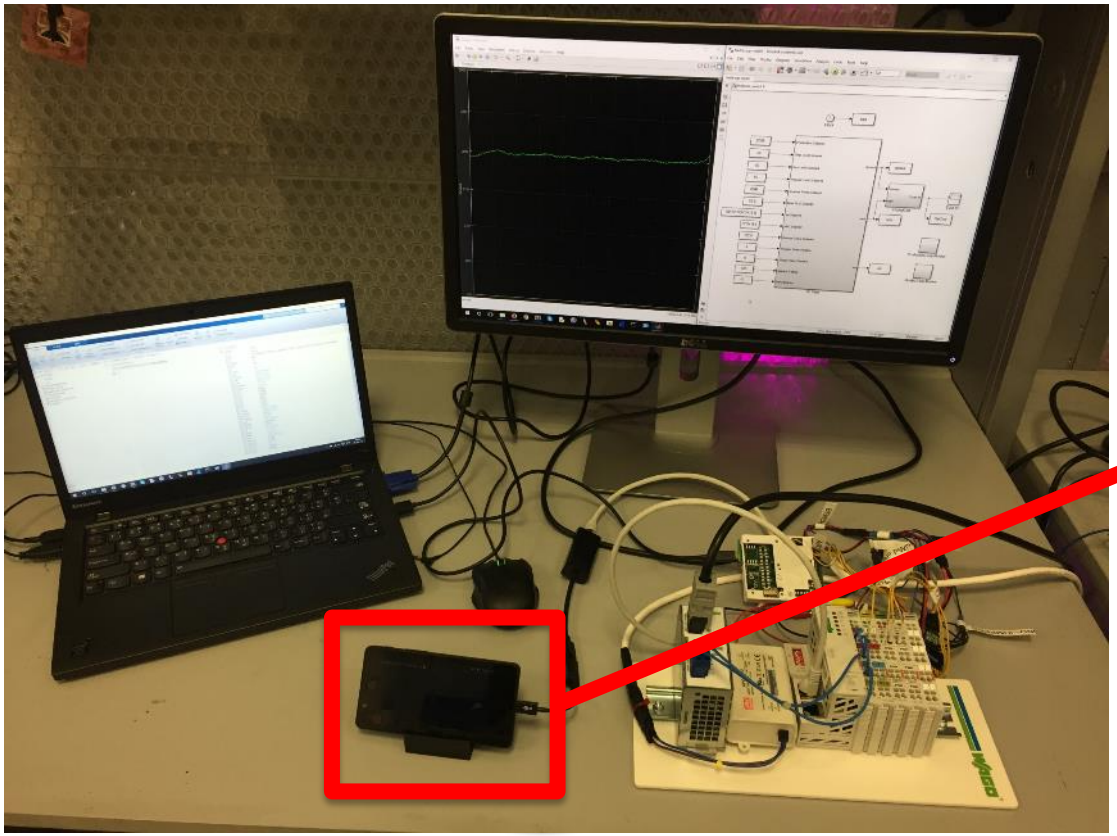
(c) Other operations

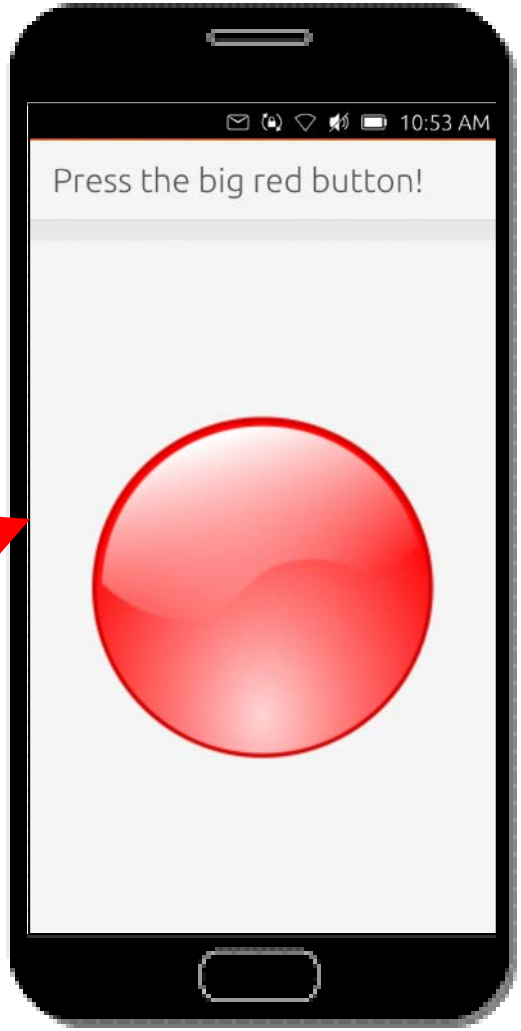


(d) Total time

Case study

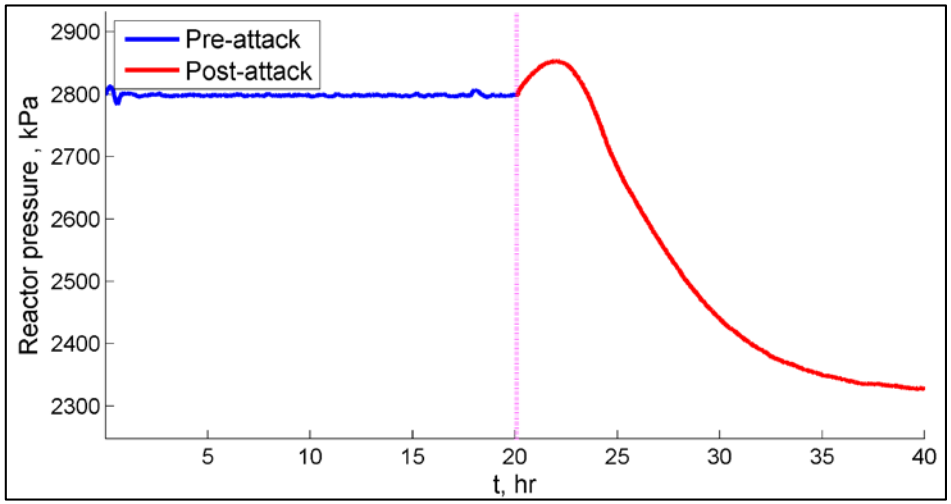
Automated payload delivery with ICSREF

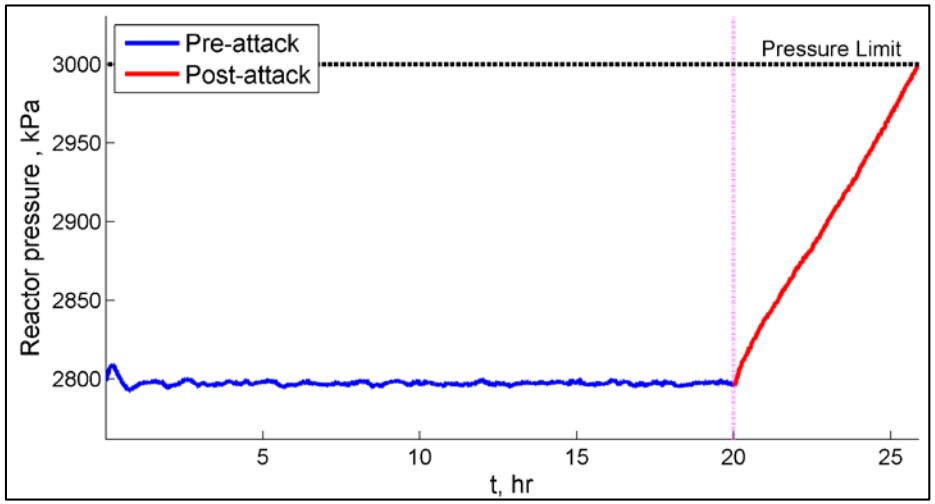




Process-aware attack results

Tennessee Eastman chemical process – Reactor pressure





Proportional gain attack

Integral gain attack

Conclusion

- Methodology for reverse engineering leveraging characteristics of ICS binaries
- github.com/momalab/ICSREF
  - Automated reverse engineering for CODESYS binaries
  - Binary and source code samples for experimentation

NYU Abu Dhabi CCS smart city testbed

http://sites.nyuad.nyu.edu/ccs-ad/smart-city-testbed/

- Testbed incorporates various smart processes
  - Smart grid
  - Industrial IoT
  - Intelligent transportation
  - Smart house
  - Smart building

- Questions?
  - Follow me @realmomalab