What’s all the fuzz about?

Project Robus

Aegis™ Platform

Adam Crain, Automatak

Chris Sistrunk PE, Mandiant

Project Robus

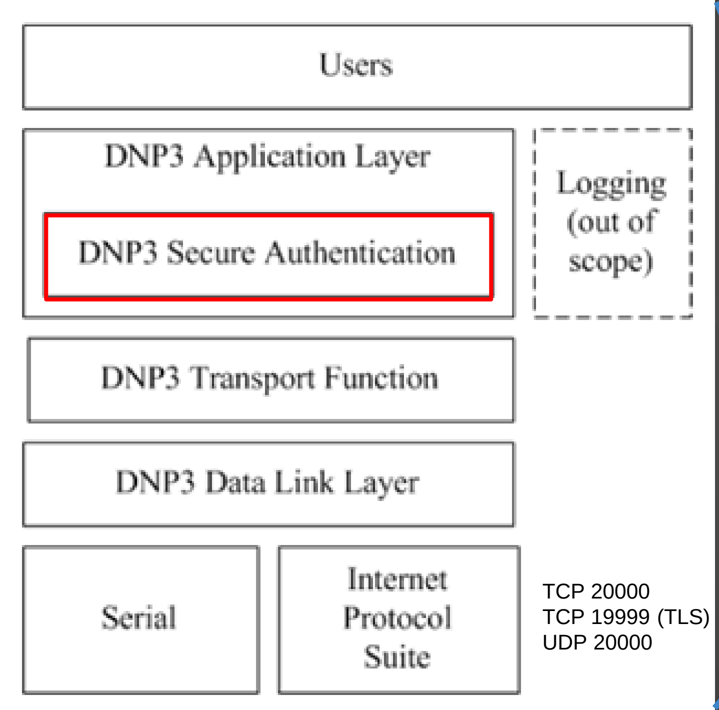
- Started in April 2013
- 17 advisories / 31 tickets
- Mostly DNP3, 1 Modbus
- Only 4 products so far without a detectable issue

www.automatak.com/robus
www.automatak.com/aegis

Vendor Response Matrix

#	ICS-CERT Adv	Company	Bug	Fix	Days	Advisory
1	ICSA-13-161-01	IOServer	4/24	5/24	30	6/10/2013
2	ICSA-13-213-03	IOServer	5/1	7/20	80	8/1/2013
3	ICSA-13-219-01	SEL	5/1	5/30	29	8/7/2013
4	ICSA-13-226-01	Kepware	4/24	6/18	55	8/14/2013
5	ICSA-13-234-02	TOP Server	4/24	6/18	55	8/22/2013
6	ICSA-13-240-01	TMW	4/24	6/17	54	8/28/2013
7	ICSA-13-213-04A	Matrikon	4/24	6/17	54	8/29/2013
8	ICSA-13-252-01	Subnet	4/24	8/30	128	9/9/2013
9	ICSA-13-282-01	Alstom	4/24	6/4	41	10/21/2013
10	ICSA-13-297-01	Catapult	4/24	10/1	160	11/22/2013
11	ICSA-13-297-02	GE IP	S.R.	10/1	n/a	11/22/2013
12	ICSA-13-337-01	Elecsys	9/12	11/4	53	12/3/2013
13	ICSA-13-346-02	Cooper OPC	7/31	None	∞day™	12/12/2013
14	ICSA-13-346-01	Cooper/Cybectec	5/1	12/12	225	12/12/2013
15	ICSA-13-352-01	Novatech	5/1	9/5	127	12/18/2013
16	ICSA-14-014-01	Schneider	8/6	8/23	17	1/14/2014
17	ICSA-14-006-01	Schneider/Telvent	8/29	10/16	48	1/30/2014

Breaking Down DNP3



Users

DNP3 Application Layer

DNP3 Secure Authentication

Logging (out of scope)

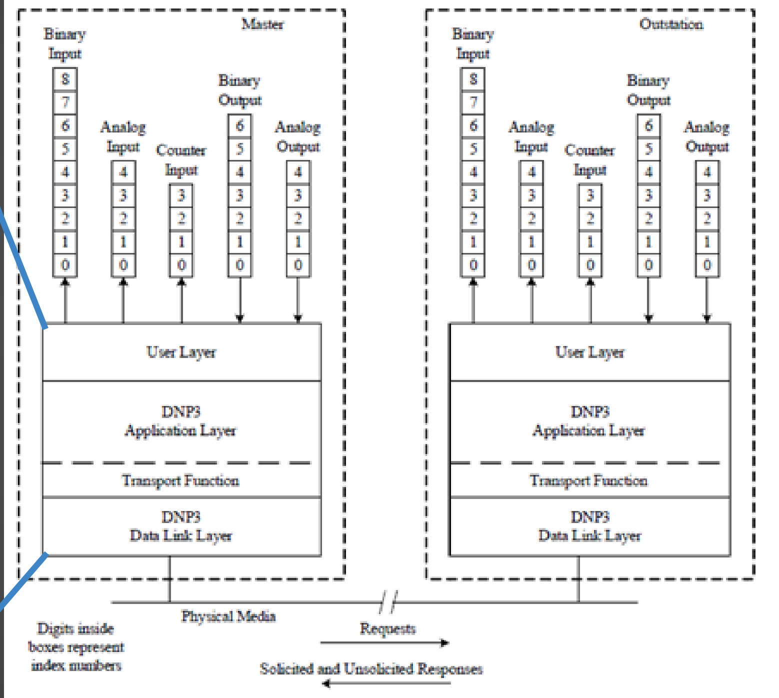
DNP3 Transport Function

DNP3 Data Link Layer

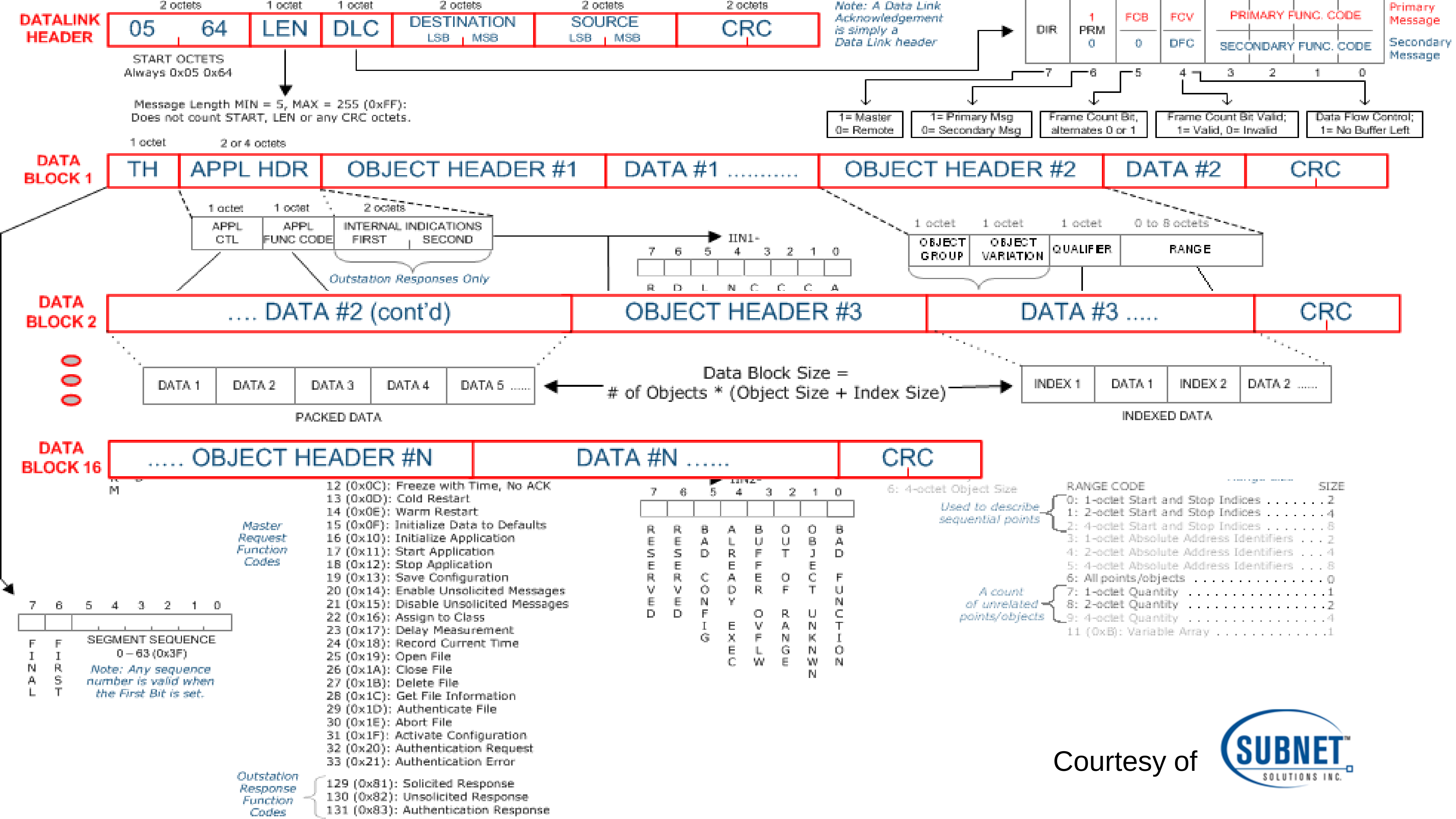
Serial

Internet Protocol Suite

TCP 20000
TCP 19999 (TLS)
UDP 20000



Ref from IEEE Std 1815-2012



Master Request Function Codes

12 (0x0C): Freeze with Time, No ACK
13 (0x0D): Cold Restart
14 (0x0E): Warm Restart
15 (0x0F): Initialize Data to Defaults
16 (0x10): Initialize Application
17 (0x11): Start Application
18 (0x12): Stop Application
19 (0x13): Save Configuration
20 (0x14): Enable Unsolicited Messages
21 (0x15): Disable Unsolicited Messages
22 (0x16): Assign to Class
23 (0x17): Delay Measurement
24 (0x18): Record Current Time
25 (0x19): Open File
26 (0x1A): Close File
27 (0x1B): Delete File
28 (0x1C): Get File Information
29 (0x1D): Authenticate File
30 (0x1E): Abort File
31 (0x1F): Activate Configuration
32 (0x20): Authentication Request
33 (0x21): Authentication Error

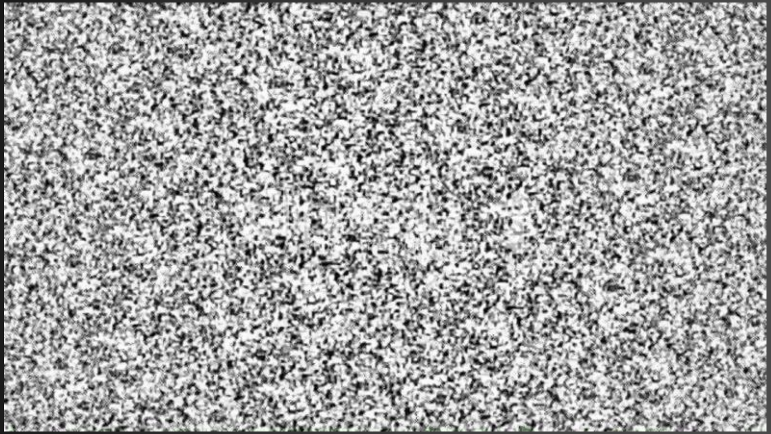
Outstation Response Function Codes

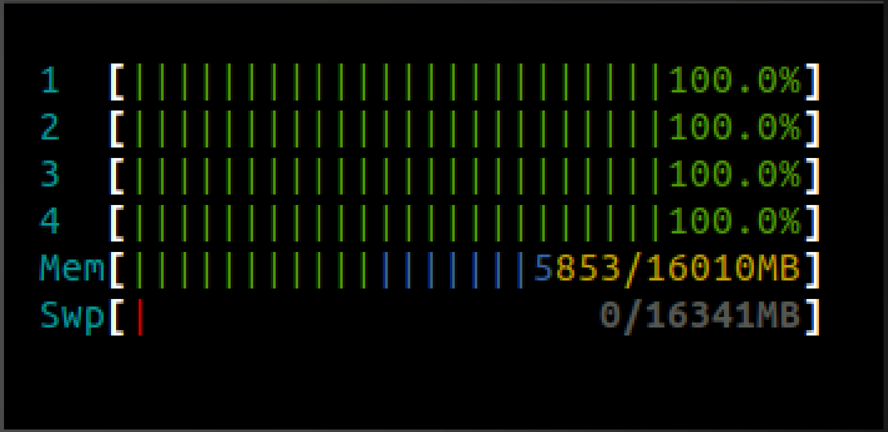
129 (0x81): Solicited Response
130 (0x82): Unsolicited Response
131 (0x83): Authentication Response

	RANGE CODE	SIZE
Used to describe sequential points	0: 1-octet Start and Stop Indices	2
	1: 2-octet Start and Stop Indices	4
	2: 4-octet Start and Stop Indices	8
	3: 1-octet Absolute Address Identifiers	2
	4: 2-octet Absolute Address Identifiers	4
	5: 4-octet Absolute Address Identifiers	8
	6: All points/objects	0
A count of unrelated points/objects	7: 1-octet Quantity	1
	8: 2-octet Quantity	2
	9: 4-octet Quantity	4
	11 (0xB): Variable Array	1

Courtesy of SUBNET™ SOLUTIONS INC.

White Noise Fuzzing

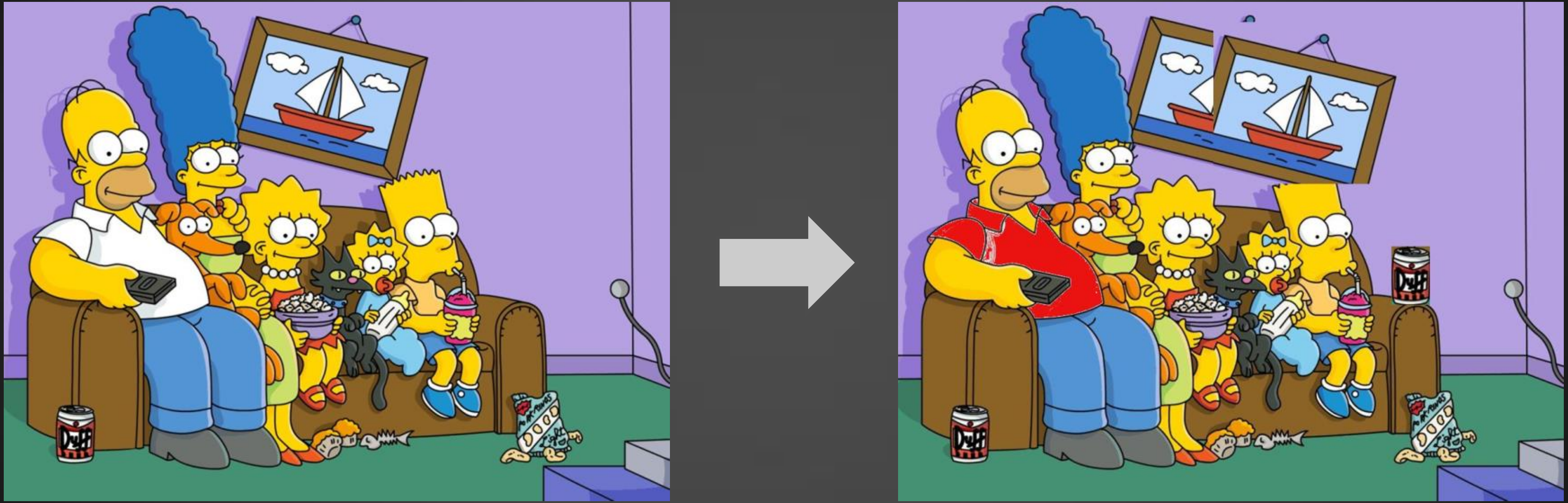




```
1  [||||||||||||||||||||||||100.0%]
2  [||||||||||||||||||||||||100.0%]
3  [||||||||||||||||||||||||100.0%]
4  [||||||||||||||||||||||||100.0%]
Mem[||||||||||||||||||5853/16010MB]
Swp[|                    0/16341MB]
```

#1 random == really “dumb”

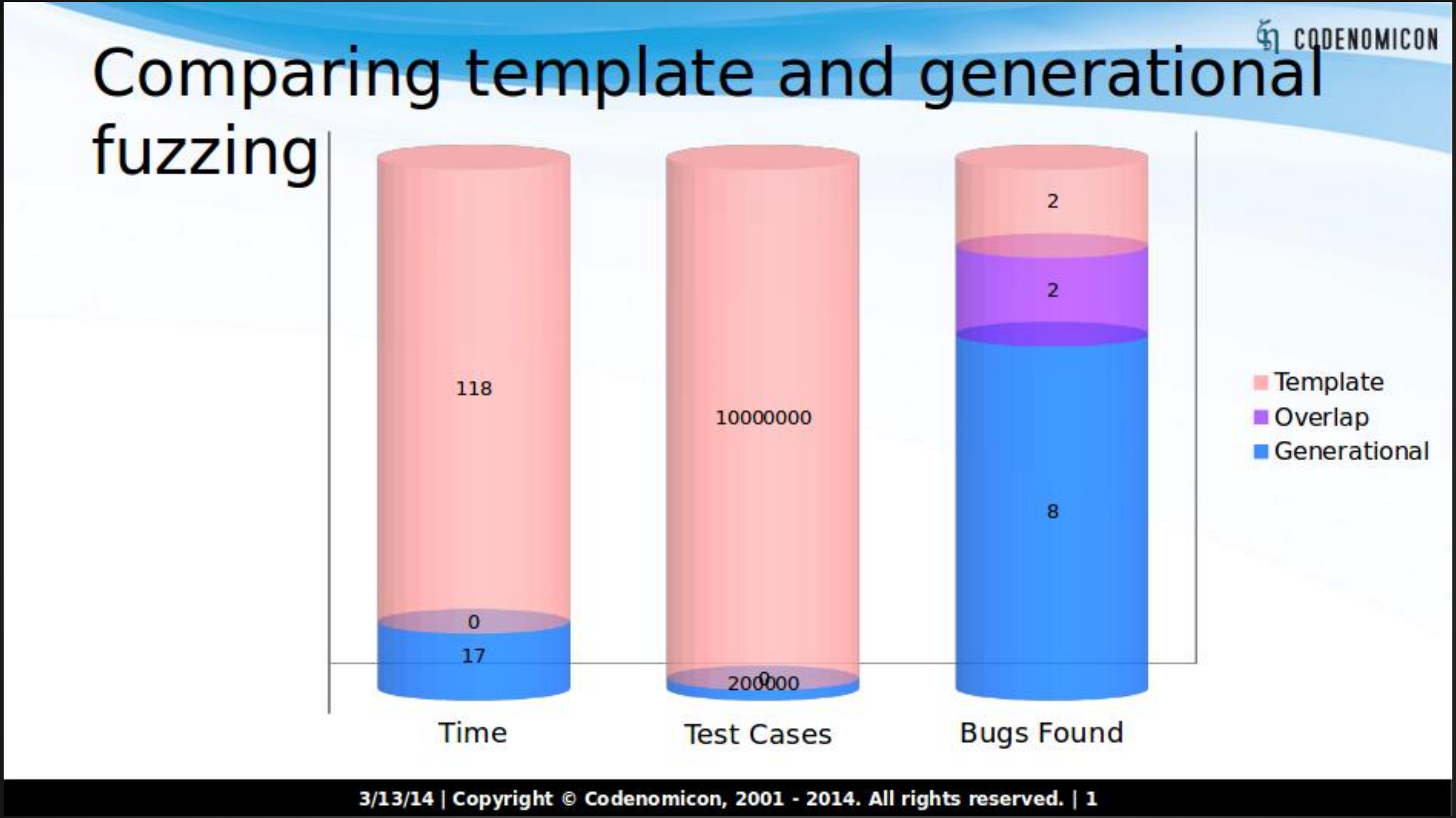
Template (mutational) Fuzzing



Generational “Smart” Fuzzing

Multi-field Anomalies

Generational == most vulns!

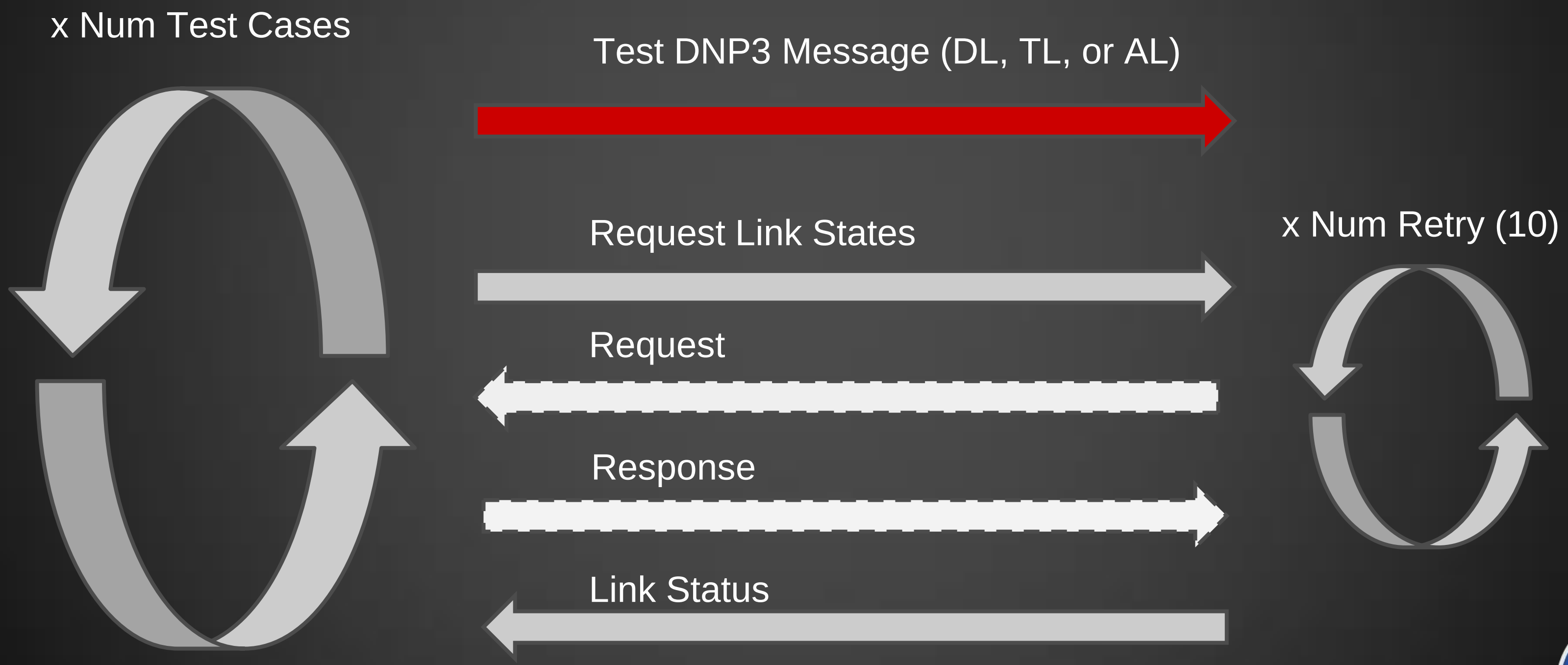


Comparing template and generational fuzzing

Aegis™ Specifics

- Written in Scala www.scala-lang.org
- Currently porting it to C#
- Protocol boundary conditions
- Abstracts physical layer
- Combines aspects of generation and mutation
- Repeatable random seeds
- ~200,000 test cases with one seed

Fuzzer Test Flow



I 0x0564 U...
Y U NO 0x0564
ME BAK ?!

Combinatorics

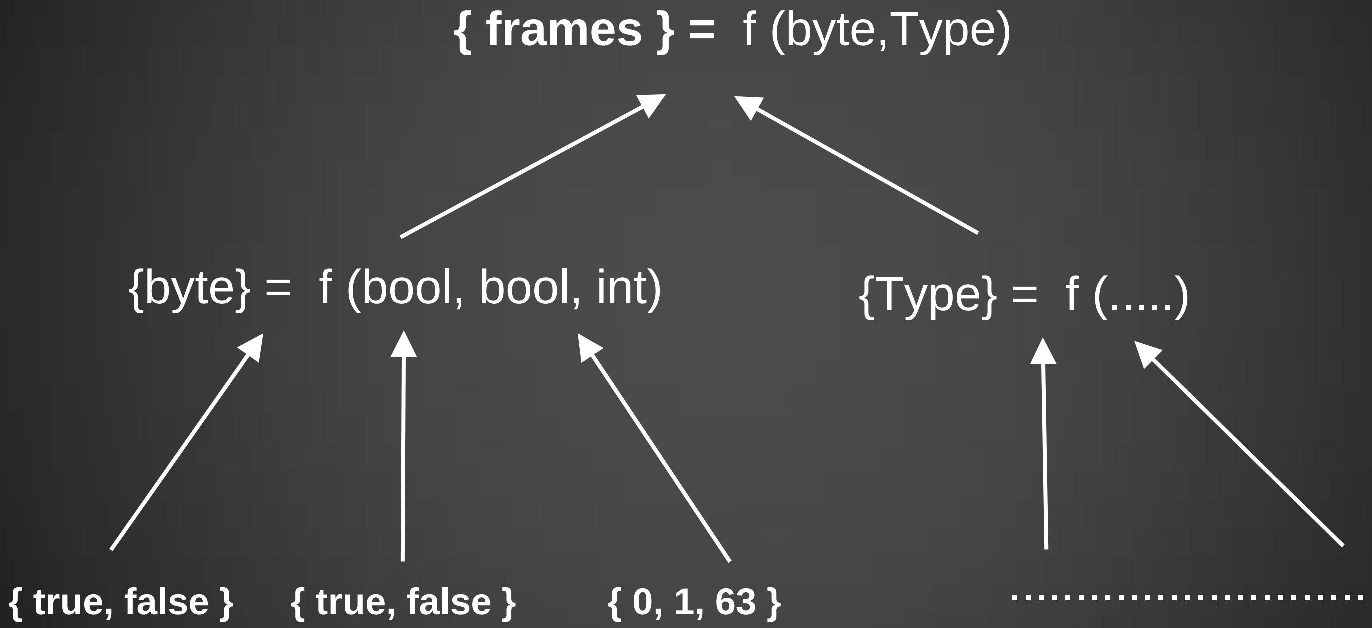
```
val nums = List(1, 3)
val colors = List(“red”,”green”)

// repeat the reversed string num times
def combine(i: Int, s: String) = List.fill(i)(s.reverse).mkString
val result = Cartesian.Transform(colors,nums)(combine)
```

What is result?

Lazy Generator

```
// val nums = List(1, 3)
// val colors = List(“red”,”green”)
> result.foreach(println)
  der
  derderder
  neerg
  neergneergneerg
```

Fuzzing is $O(2^n)$



{ frames } = f (byte,Type)

{byte} = f (bool, bool, int)

{Type} = f (.....)

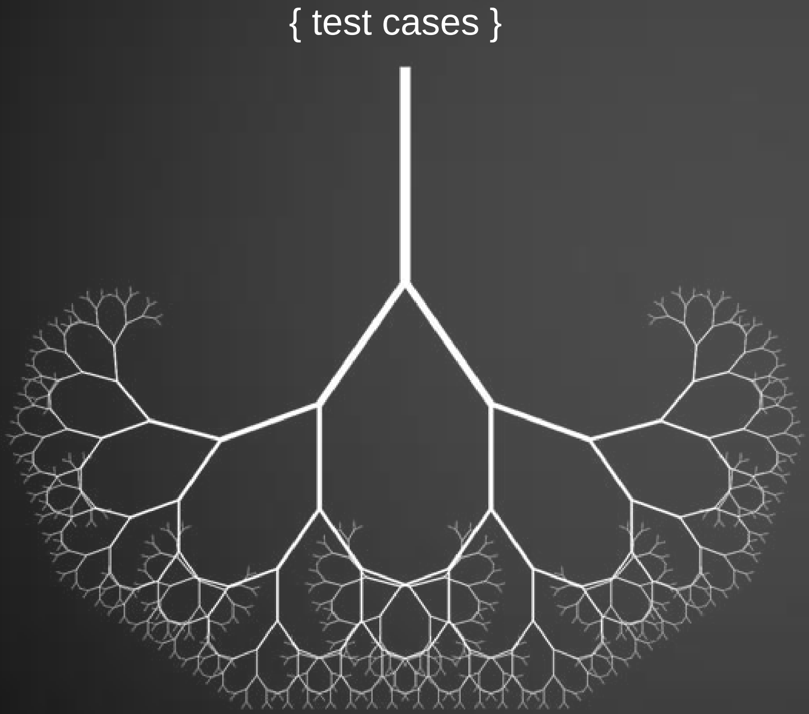
{ true, false }

{ true, false }

{ 0, 1, 63 }

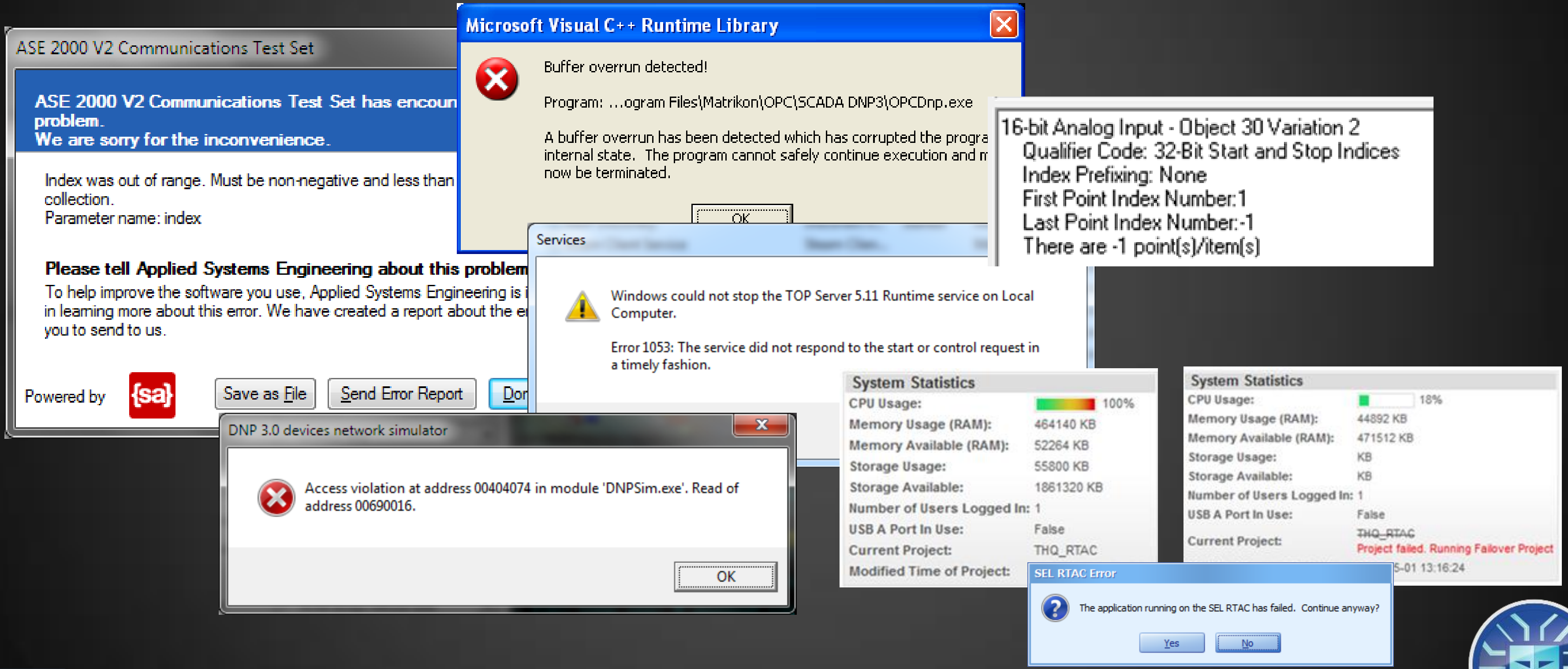
....

Generators can get large!



- Many function codes
- Many objects
- Header types
- Many field values

Types of Vulnerabilities



ASE 2000 V2 Communications Test Set

ASE 2000 V2 Communications Test Set has encoun
problem.
We are sorry for the inconvenience.

Index was out of range. Must be non-negative and less than
collection.
Parameter name: index

Please tell Applied Systems Engineering about this problem
To help improve the software you use, Applied Systems Engineering is i
in learning more about this error. We have created a report about the er
you to send to us.

Powered by {sa} Save as File Send Error Report Don

Microsoft Visual C++ Runtime Library

Buffer overrun detected!

Program: ...ogram Files\Matrikon\OPC\SCADA DNP3\OPCDnp.exe

A buffer overrun has been detected which has corrupted the progra
internal state. The program cannot safely continue execution and m
now be terminated.

OK

16-bit Analog Input - Object 30 Variation 2
Qualifier Code: 32-Bit Start and Stop Indices
Index Prefixing: None
First Point Index Number:1
Last Point Index Number:-1
There are -1 point(s)/item(s)

Services

Windows could not stop the TOP Server 5.11 Runtime service on Local Computer.

Error 1053: The service did not respond to the start or control request in a timely fashion.

DNP 3.0 devices network simulator

Access violation at address 00404074 in module 'DNPSim.exe'. Read of address 00690016.

OK

System Statistics
CPU Usage: 100%
Memory Usage (RAM): 464140 KB
Memory Available (RAM): 52264 KB
Storage Usage: 55800 KB
Storage Available: 1861320 KB
Number of Users Logged In: 1
USB A Port In Use: False
Current Project: THQ_RTAC
Modified Time of Project:

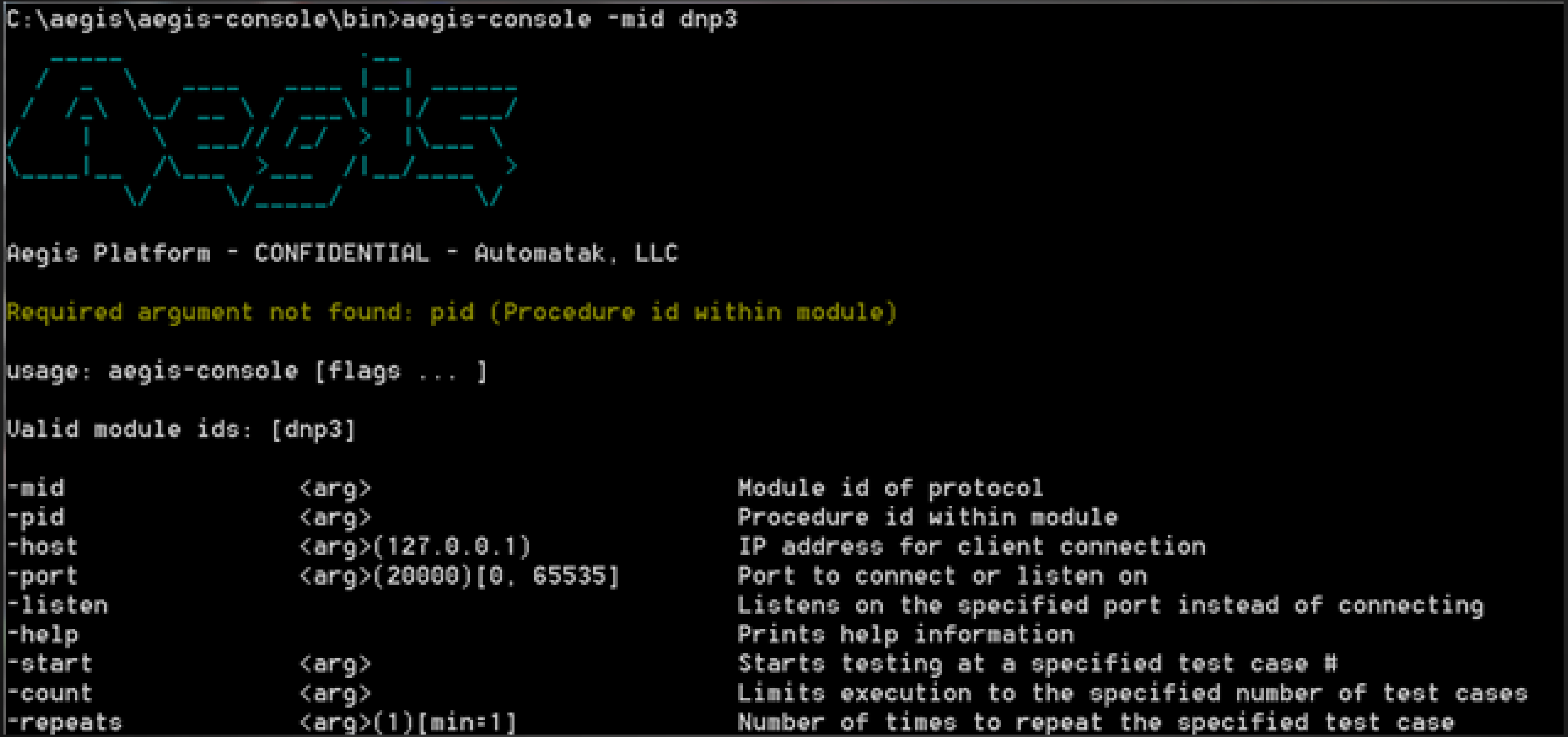
System Statistics
CPU Usage: 18%
Memory Usage (RAM): 44892 KB
Memory Available (RAM): 471512 KB
Storage Usage: KB
Storage Available: KB
Number of Users Logged In: 1
USB A Port In Use: False
Current Project: ~~THQ_RTAC~~
Project failed. Running Failover Project
5-01 13:16:24

SEL RTAC Error

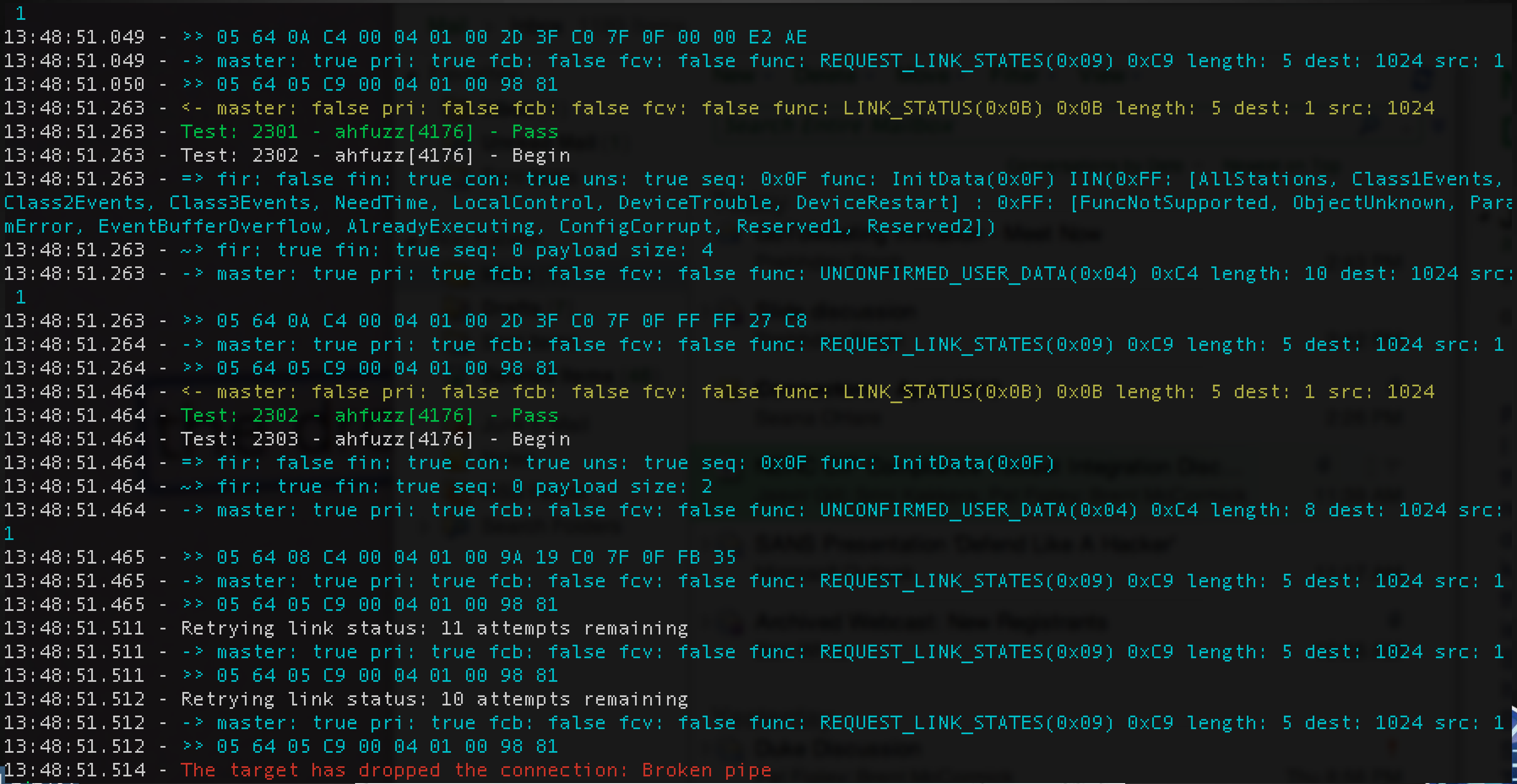
The application running on the SEL RTAC has failed. Continue anyway?

Yes No

Using Aegis



```
C:\aegis\aegis-console\bin>aegis-console -mid dnp3
   _____                .__
  /  _  \   ____   ____ |__| ______
 /  /_\  \_/ __ \ / ___\|  |/  ___/
/    |    \  ___// /_/  >  |\___ \
\____|__  /\___  >___  /|__/____  >
        \/     \/_____/         \/

Aegis Platform - CONFIDENTIAL - Automatak, LLC

Required argument not found: pid (Procedure id within module)

usage: aegis-console [flags ... ]

Valid module ids: [dnp3]

-mid                <arg>                        Module id of protocol
-pid                <arg>                        Procedure id within module
-host               <arg>(127.0.0.1)             IP address for client connection
-port               <arg>(20000)[0, 65535]       Port to connect or listen on
-listen                                          Listens on the specified port instead of connecting
-help                                            Prints help information
-start              <arg>                        Starts testing at a specified test case #
-count              <arg>                        Limits execution to the specified number of test cases
-repeats            <arg>(1)[min=1]              Number of times to repeat the specified test case
```



```
 1
13:48:51.049 - >> 05 64 0A C4 00 04 01 00 2D 3F C0 7F 0F 00 00 E2 AE
13:48:51.049 - -> master: true pri: true fcb: false fcv: false func: REQUEST_LINK_STATES(0x09) 0xC9 length: 5 dest: 1024 src: 1
13:48:51.050 - >> 05 64 05 C9 00 04 01 00 98 81
13:48:51.263 - <- master: false pri: false fcb: false fcv: false func: LINK_STATUS(0x0B) 0x0B length: 5 dest: 1 src: 1024
13:48:51.263 - Test: 2301 - ahfuzz[4176] - Pass
13:48:51.263 - Test: 2302 - ahfuzz[4176] - Begin
13:48:51.263 - => fir: false fin: true con: true uns: true seq: 0x0F func: InitData(0x0F) IIN(0xFF: [AllStations, Class1Events,
Class2Events, Class3Events, NeedTime, LocalControl, DeviceTrouble, DeviceRestart] : 0xFF: [FuncNotSupported, ObjectUnknown, Para
mError, EventBufferOverflow, AlreadyExecuting, ConfigCorrupt, Reserved1, Reserved2])
13:48:51.263 - ~> fir: true fin: true seq: 0 payload size: 4
13:48:51.263 - -> master: true pri: true fcb: false fcv: false func: UNCONFIRMED_USER_DATA(0x04) 0xC4 length: 10 dest: 1024 src:
 1
13:48:51.263 - >> 05 64 0A C4 00 04 01 00 2D 3F C0 7F 0F FF FF 27 C8
13:48:51.264 - -> master: true pri: true fcb: false fcv: false func: REQUEST_LINK_STATES(0x09) 0xC9 length: 5 dest: 1024 src: 1
13:48:51.264 - >> 05 64 05 C9 00 04 01 00 98 81
13:48:51.464 - <- master: false pri: false fcb: false fcv: false func: LINK_STATUS(0x0B) 0x0B length: 5 dest: 1 src: 1024
13:48:51.464 - Test: 2302 - ahfuzz[4176] - Pass
13:48:51.464 - Test: 2303 - ahfuzz[4176] - Begin
13:48:51.464 - => fir: false fin: true con: true uns: true seq: 0x0F func: InitData(0x0F)
13:48:51.464 - ~> fir: true fin: true seq: 0 payload size: 2
13:48:51.464 - -> master: true pri: true fcb: false fcv: false func: UNCONFIRMED_USER_DATA(0x04) 0xC4 length: 8 dest: 1024 src:
1
13:48:51.465 - >> 05 64 08 C4 00 04 01 00 9A 19 C0 7F 0F FB 35
13:48:51.465 - -> master: true pri: true fcb: false fcv: false func: REQUEST_LINK_STATES(0x09) 0xC9 length: 5 dest: 1024 src: 1
13:48:51.465 - >> 05 64 05 C9 00 04 01 00 98 81
13:48:51.511 - Retrying link status: 11 attempts remaining
13:48:51.511 - -> master: true pri: true fcb: false fcv: false func: REQUEST_LINK_STATES(0x09) 0xC9 length: 5 dest: 1024 src: 1
13:48:51.511 - >> 05 64 05 C9 00 04 01 00 98 81
13:48:51.512 - Retrying link status: 10 attempts remaining
13:48:51.512 - -> master: true pri: true fcb: false fcv: false func: REQUEST_LINK_STATES(0x09) 0xC9 length: 5 dest: 1024 src: 1
13:48:51.512 - >> 05 64 05 C9 00 04 01 00 98 81
13:48:51.514 - The target has dropped the connection: Broken pipe
```

Examples

Run 10 link layer test cases starting at #123

```
$ aegis-console -mid dnp3 -pid lfuzz -start 123 -count 10
```

Unsolicited response fuzzing of a master listening on default port 20000 with master address of 0 and an outstation address of 1

```
$ aegis-console -mid dnp3 -pid aufuzz -dest 0 -src 1 -master -listen
```

Outstation link layer fuzzing test case #100 only

```
$ aegis-console -mid dnp3 -pid lfuzz -start 100 -count 1
```

Outstation application object fuzzing against 192.168.1.55:20001 with default addressing

```
$ aegis-console -mid dnp3 -id aofuzz -host 192.168.1.55 -port 20001
```

Recorded Demos

Video 1: a DNP3 outstation

-pid aofuzz

Video 2: a DNP3 master

-pid aufuzz -listen -master -seed 1

White-box vs. Black-box Testing

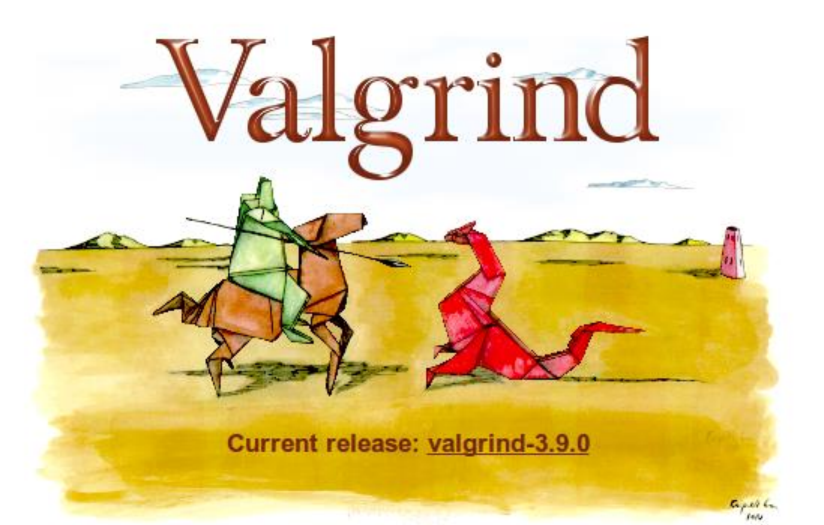
- Defender has the advantage, but has to choose to exercise it.
- Software-based solutions allow developers to test continually.

There are many OSS tools of the trade.

Code Coverage with gcov

- If you don’t run a line of code, you’ll never find a bug in it
- Important metric, but not a guarantee of success

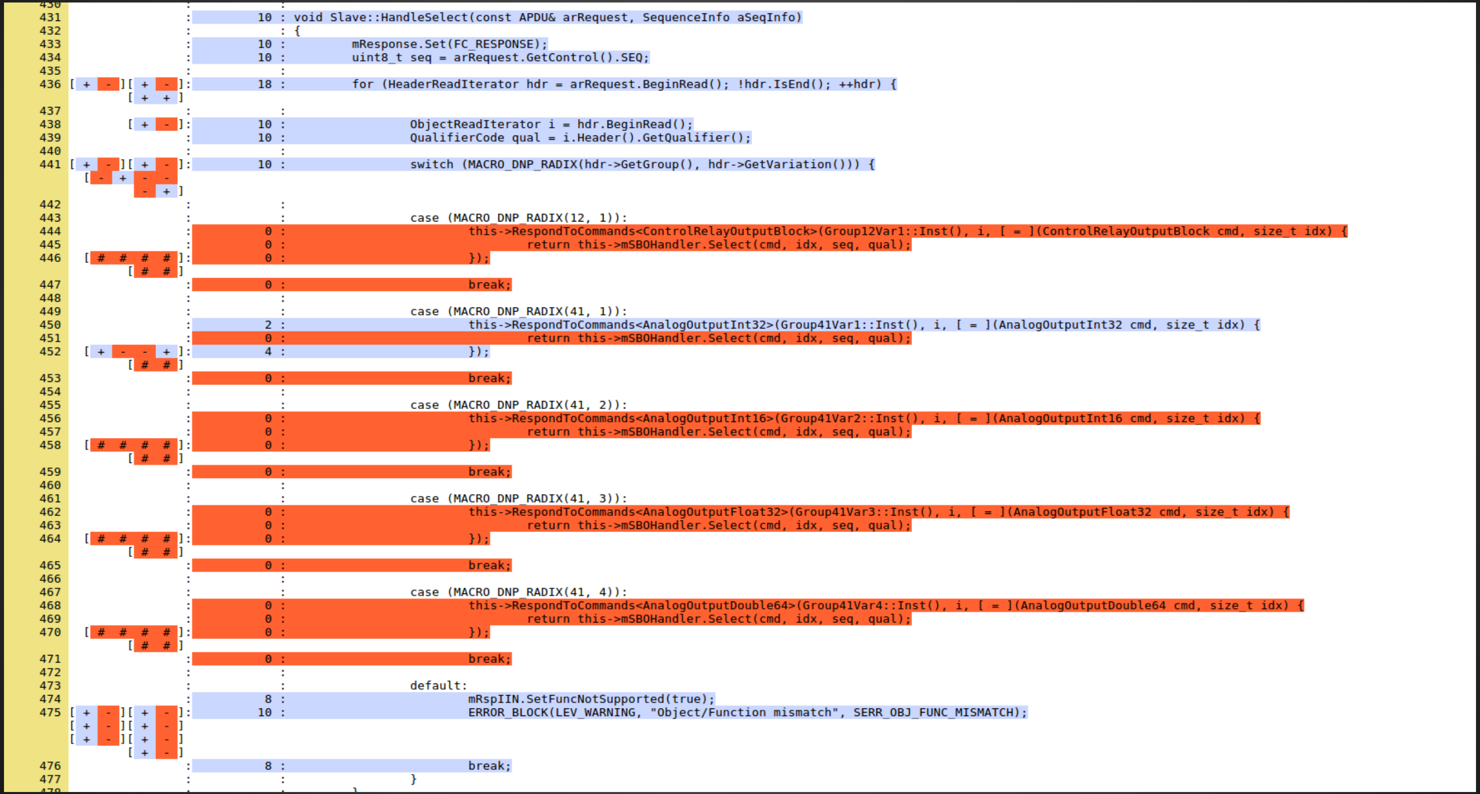
Dynamic Analysis with Valgrind



valgrind.org

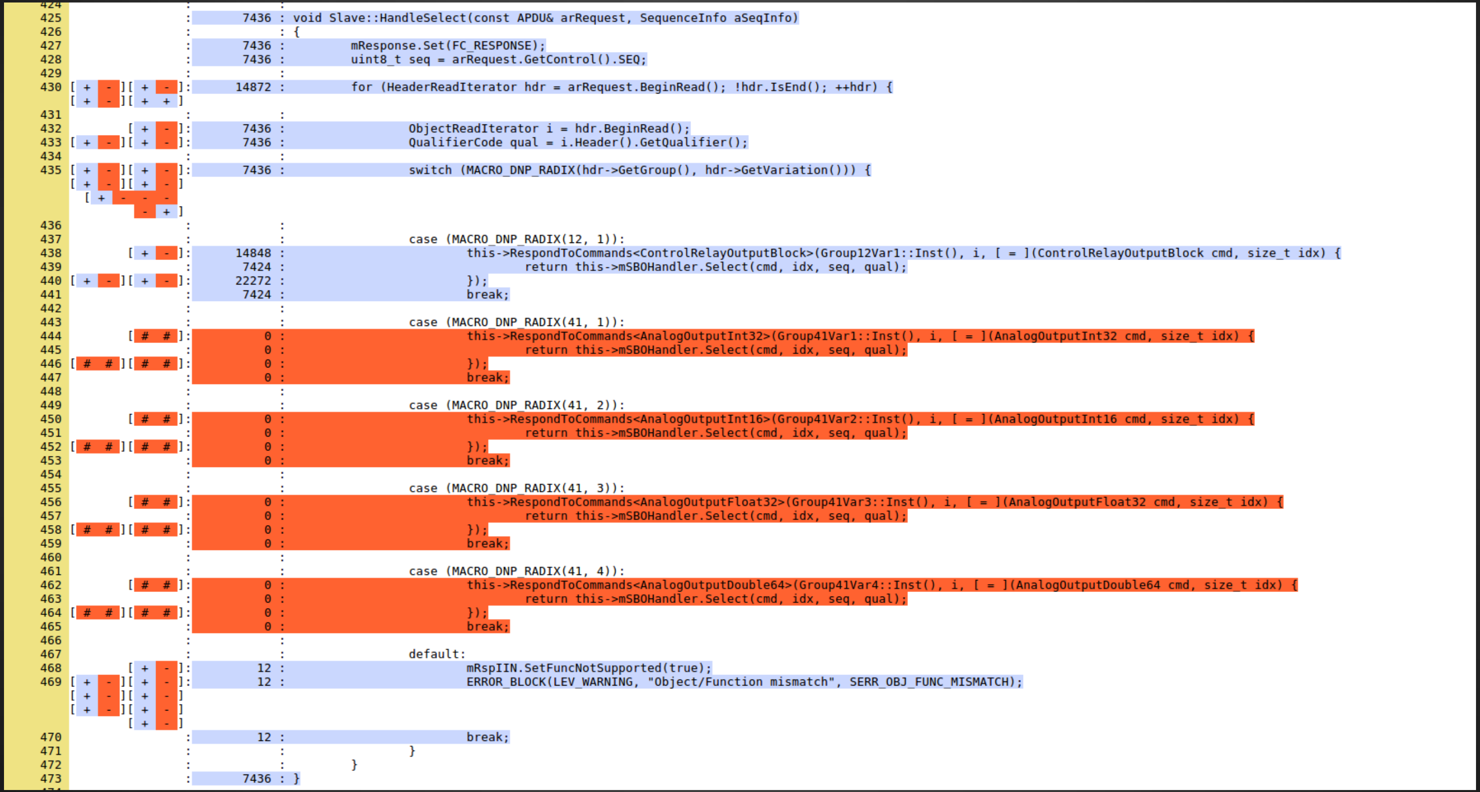
- Virtualized binary execution
  - hooks system calls
- memcheck is your friend
  - leaks
  - overrun / underrun
  - user after free
- callgrind
  - find true bottlenecks

Wurldtech Achilles - opendnp3 outstation - SELECT code coverage



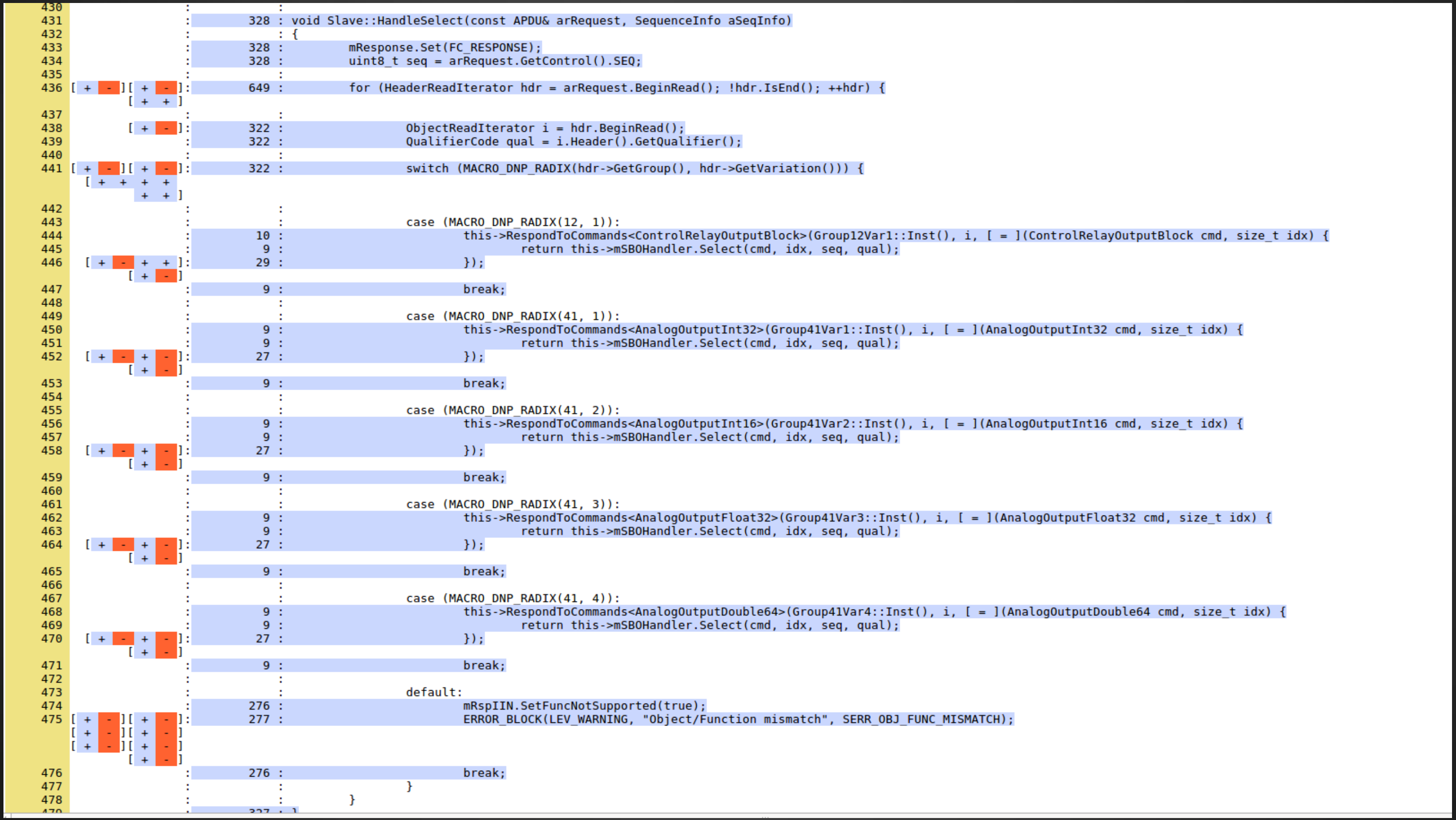
```
                :         :
                :      10 : void Slave::HandleSelect(const APDU& arRequest, SequenceInfo aSeqInfo)
                :         : {
                :      10 :         mResponse.Set(FC_RESPONSE);
                :      10 :         uint8_t seq = arRequest.GetControl().SEQ;
                :         :
[ + - ][ + - ]:      18 :         for (HeaderReadIterator hdr = arRequest.BeginRead(); !hdr.IsEnd(); ++hdr) {
        [ + + ]
                :         :
        [ + - ]:      10 :                 ObjectReadIterator i = hdr.BeginRead();
                :      10 :                 QualifierCode qual = i.Header().GetQualifier();
                :         :
[ + - ][ + - ]:      10 :                 switch (MACRO_DNP_RADIX(hdr->GetGroup(), hdr->GetVariation())) {
  [ - + - -
          - + ]
                :         :
                :         :                 case (MACRO_DNP_RADIX(12, 1)):
                :       0 :                         this->RespondToCommands<ControlRelayOutputBlock>(Group12Var1::Inst(), i, [ = ](ControlRelayOutputBlock cmd, size_t idx) {
                :       0 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
  [ # # # # ]:       0 :                         });
        [ # # ]
                :       0 :                         break;
                :         :
                :         :                 case (MACRO_DNP_RADIX(41, 1)):
                :       2 :                         this->RespondToCommands<AnalogOutputInt32>(Group41Var1::Inst(), i, [ = ](AnalogOutputInt32 cmd, size_t idx) {
                :       0 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
  [ + - - + ]:       4 :                         });
        [ # # ]
                :       0 :                         break;
                :         :
                :         :                 case (MACRO_DNP_RADIX(41, 2)):
                :       0 :                         this->RespondToCommands<AnalogOutputInt16>(Group41Var2::Inst(), i, [ = ](AnalogOutputInt16 cmd, size_t idx) {
                :       0 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
  [ # # # # ]:       0 :                         });
        [ # # ]
                :       0 :                         break;
                :         :
                :         :                 case (MACRO_DNP_RADIX(41, 3)):
                :       0 :                         this->RespondToCommands<AnalogOutputFloat32>(Group41Var3::Inst(), i, [ = ](AnalogOutputFloat32 cmd, size_t idx) {
                :       0 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
  [ # # # # ]:       0 :                         });
        [ # # ]
                :       0 :                         break;
                :         :
                :         :                 case (MACRO_DNP_RADIX(41, 4)):
                :       0 :                         this->RespondToCommands<AnalogOutputDouble64>(Group41Var4::Inst(), i, [ = ](AnalogOutputDouble64 cmd, size_t idx) {
                :       0 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
  [ # # # # ]:       0 :                         });
        [ # # ]
                :       0 :                         break;
                :         :
                :         :                 default:
                :       8 :                         mRspIIN.SetFuncNotSupported(true);
[ + - ][ + - ]:      10 :                         ERROR_BLOCK(LEV_WARNING, "Object/Function mismatch", SERR_OBJ_FUNC_MISMATCH);
[ + - ][ + - ]
[ + - ][ + - ]
        [ + - ]
                :       8 :                         break;
                :         :                 }
                :         :         }
```

Mu4000 - opendnp3 outstation - SELECT code coverage

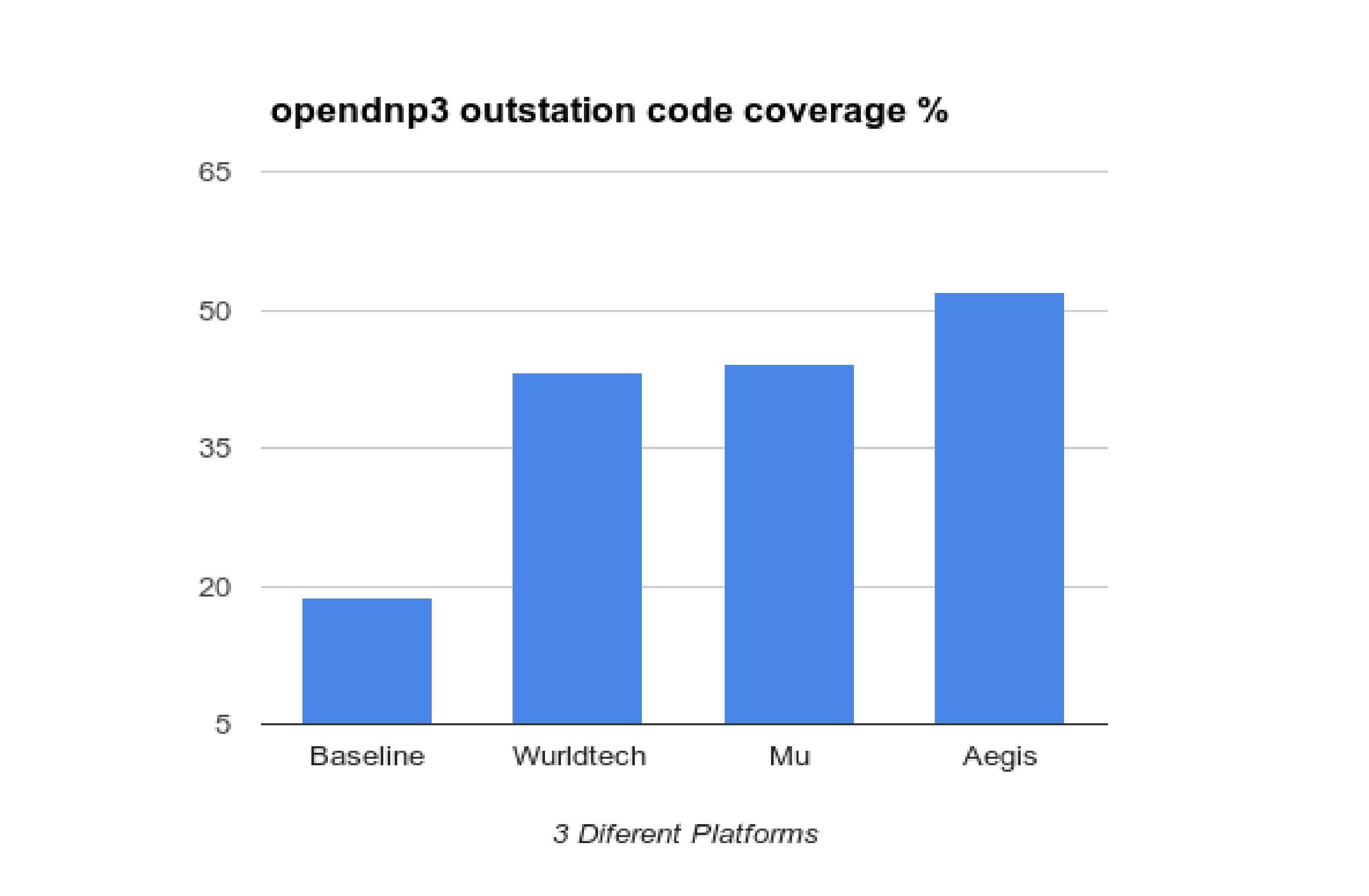


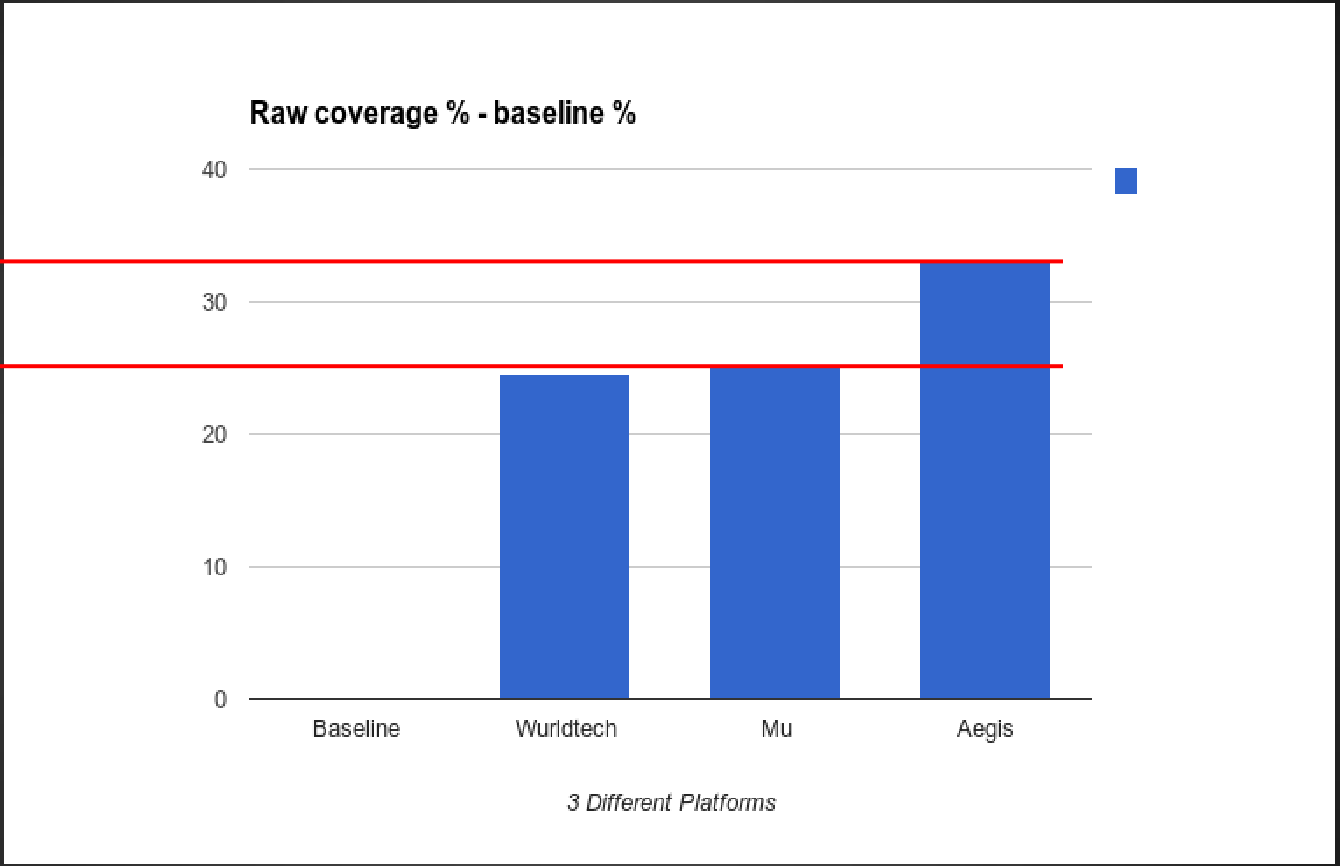
```
                       :                :
                       :       7436 : void Slave::HandleSelect(const APDU& arRequest, SequenceInfo aSeqInfo)
                       :            : {
                       :       7436 :         mResponse.Set(FC_RESPONSE);
                       :       7436 :         uint8_t seq = arRequest.GetControl().SEQ;
                       :            :
[ +  - ][ +  - ]:      14872 :         for (HeaderReadIterator hdr = arRequest.BeginRead(); !hdr.IsEnd(); ++hdr) {
[ +  - ][ +  + ]
                       :            :
        [ +  - ]:       7436 :                 ObjectReadIterator i = hdr.BeginRead();
[ +  - ][ +  - ]:       7436 :                 QualifierCode qual = i.Header().GetQualifier();
                       :            :
[ +  - ][ +  - ]:       7436 :                 switch (MACRO_DNP_RADIX(hdr->GetGroup(), hdr->GetVariation())) {
[ +  - ][ +  - ]
  [ +  -  -  -
            -  + ]
                       :            :
                       :            :                 case (MACRO_DNP_RADIX(12, 1)):
        [ +  - ]:      14848 :                         this->RespondToCommands<ControlRelayOutputBlock>(Group12Var1::Inst(), i, [ = ](ControlRelayOutputBlock cmd, size_t idx) {
                       :       7424 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
[ +  - ][ +  - ]:      22272 :                         });
                       :       7424 :                         break;
                       :            :
                       :            :                 case (MACRO_DNP_RADIX(41, 1)):
        [ #  # ]:          0 :                         this->RespondToCommands<AnalogOutputInt32>(Group41Var1::Inst(), i, [ = ](AnalogOutputInt32 cmd, size_t idx) {
                       :          0 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
[ #  # ][ #  # ]:          0 :                         });
                       :          0 :                         break;
                       :            :
                       :            :                 case (MACRO_DNP_RADIX(41, 2)):
        [ #  # ]:          0 :                         this->RespondToCommands<AnalogOutputInt16>(Group41Var2::Inst(), i, [ = ](AnalogOutputInt16 cmd, size_t idx) {
                       :          0 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
[ #  # ][ #  # ]:          0 :                         });
                       :          0 :                         break;
                       :            :
                       :            :                 case (MACRO_DNP_RADIX(41, 3)):
        [ #  # ]:          0 :                         this->RespondToCommands<AnalogOutputFloat32>(Group41Var3::Inst(), i, [ = ](AnalogOutputFloat32 cmd, size_t idx) {
                       :          0 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
[ #  # ][ #  # ]:          0 :                         });
                       :          0 :                         break;
                       :            :
                       :            :                 case (MACRO_DNP_RADIX(41, 4)):
        [ #  # ]:          0 :                         this->RespondToCommands<AnalogOutputDouble64>(Group41Var4::Inst(), i, [ = ](AnalogOutputDouble64 cmd, size_t idx) {
                       :          0 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
[ #  # ][ #  # ]:          0 :                         });
                       :          0 :                         break;
                       :            :
                       :            :                 default:
        [ +  - ]:         12 :                         mRspIIN.SetFuncNotSupported(true);
[ +  - ][ +  - ]:         12 :                         ERROR_BLOCK(LEV_WARNING, "Object/Function mismatch", SERR_OBJ_FUNC_MISMATCH);
[ +  - ][ +  - ]
[ +  - ][ +  - ]
        [ +  - ]
                       :         12 :                         break;
                       :            :                 }
                       :            :         }
                       :       7436 : }
```

Aegis™ 0.1.0 - opendnp3 outstation - SELECT code coverage



```
                :           :
                :       328 : void Slave::HandleSelect(const APDU& arRequest, SequenceInfo aSeqInfo)
                :           : {
                :       328 :         mResponse.Set(FC_RESPONSE);
                :       328 :         uint8_t seq = arRequest.GetControl().SEQ;
                :           :
[ + - ][ + - ]:       649 :         for (HeaderReadIterator hdr = arRequest.BeginRead(); !hdr.IsEnd(); ++hdr) {
        [ + + ]
                :           :
        [ + - ]:       322 :                 ObjectReadIterator i = hdr.BeginRead();
                :       322 :                 QualifierCode qual = i.Header().GetQualifier();
                :           :
[ + - ][ + - ]:       322 :                 switch (MACRO_DNP_RADIX(hdr->GetGroup(), hdr->GetVariation())) {
  [ +  +  +  +
           + + ]
                :           :
                :           :                 case (MACRO_DNP_RADIX(12, 1)):
                :        10 :                         this->RespondToCommands<ControlRelayOutputBlock>(Group12Var1::Inst(), i, [ = ](ControlRelayOutputBlock cmd, size_t idx) {
                :         9 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
  [ + - + + ]:        29 :                         });
        [ + - ]
                :         9 :                         break;
                :           :
                :           :                 case (MACRO_DNP_RADIX(41, 1)):
                :         9 :                         this->RespondToCommands<AnalogOutputInt32>(Group41Var1::Inst(), i, [ = ](AnalogOutputInt32 cmd, size_t idx) {
                :         9 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
  [ + - + - ]:        27 :                         });
        [ + - ]
                :         9 :                         break;
                :           :
                :           :                 case (MACRO_DNP_RADIX(41, 2)):
                :         9 :                         this->RespondToCommands<AnalogOutputInt16>(Group41Var2::Inst(), i, [ = ](AnalogOutputInt16 cmd, size_t idx) {
                :         9 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
  [ + - + - ]:        27 :                         });
        [ + - ]
                :         9 :                         break;
                :           :
                :           :                 case (MACRO_DNP_RADIX(41, 3)):
                :         9 :                         this->RespondToCommands<AnalogOutputFloat32>(Group41Var3::Inst(), i, [ = ](AnalogOutputFloat32 cmd, size_t idx) {
                :         9 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
  [ + - + - ]:        27 :                         });
        [ + - ]
                :         9 :                         break;
                :           :
                :           :                 case (MACRO_DNP_RADIX(41, 4)):
                :         9 :                         this->RespondToCommands<AnalogOutputDouble64>(Group41Var4::Inst(), i, [ = ](AnalogOutputDouble64 cmd, size_t idx) {
                :         9 :                                 return this->mSBOHandler.Select(cmd, idx, seq, qual);
  [ + - + - ]:        27 :                         });
        [ + - ]
                :         9 :                         break;
                :           :
                :           :                 default:
                :       276 :                         mRspIIN.SetFuncNotSupported(true);
[ + - ][ + - ]:       277 :                         ERROR_BLOCK(LEV_WARNING, "Object/Function mismatch", SERR_OBJ_FUNC_MISMATCH);
[ + - ][ + - ]
[ + - ][ + - ]
        [ + - ]
                :       276 :                         break;
                :           :                 }
                :           :         }
                :       327 : }
```

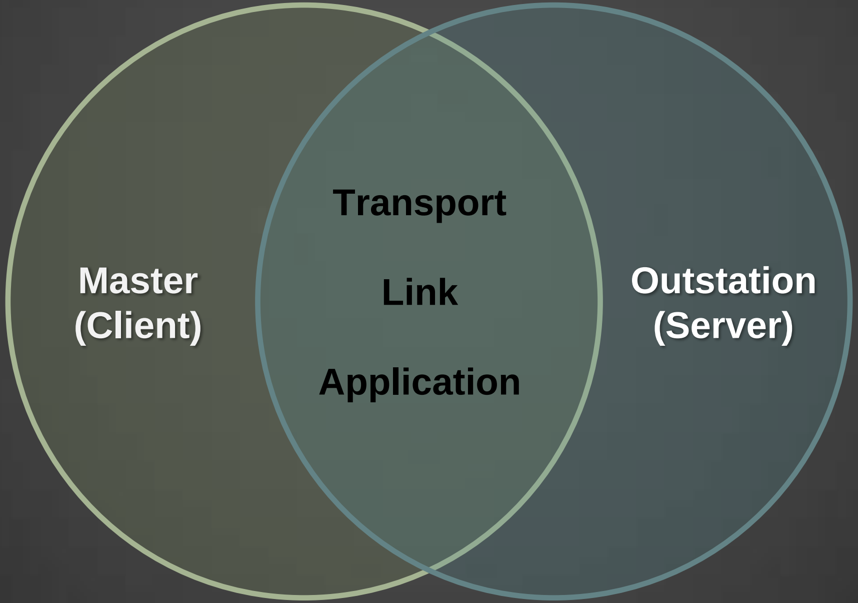

opendnp3 outstation code coverage %
65
50
35
20
5
Baseline
Wurldtech
Mu
Aegis
3 Diferent Platforms



8%

33% more relative to others

Total code coverage



More Fuzzers are Better

- Aegis fuzzing with every release
- In-memory fuzzing
- Checks from Codenomicon, Wurldtech, Mu

opendnp3

SANS

Fuzzing is just another tool

- Unit test coverage in excess of 90%
- Valgrind for dynamic analysis
- Open source conformance test harness
- Static analysis using Clang / Coverity / CppCheck

opendnp3

SANS

Security!

HOST Grant

- Adding authentication (SAv5)
- Adding encryption (TLS)

http://investments.opencybersecurity.org/

opendnp3

SHODAN update

Probably default configs

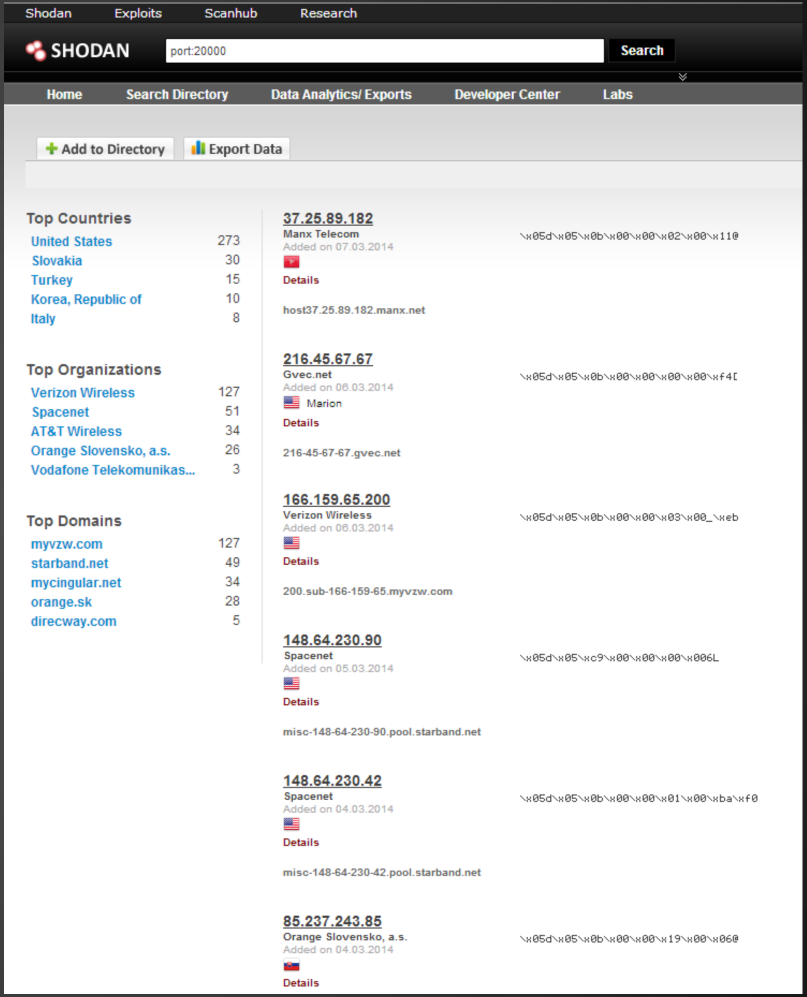
- Many similar responses
- Same DNP Addresses

```
python shell
>>> " ".join("%02x" % ord(i) for
  i in "DNP3 paste from shodan”)
```

Unsolicited Response, IIN Restart & Need Time Synch

Unsolicited Response with Binary and Analog Data

Class 1/2/3/0 Poll!!!



Top Countries	
United States	273
Slovakia	30
Turkey	15
Korea, Republic of	10
Italy	8

Top Organizations	
Verizon Wireless	127
Spacenet	51
AT&T Wireless	34
Orange Slovensko, a.s.	26
Vodafone Telekomunikas...	3

Top Domains	
myvzw.com	127
starband.net	49
mycingular.net	34
orange.sk	28
direcway.com	5

37.25.89.182
Manx Telecom
Added on 07.03.2014
Details
host37.25.89.182.manx.net

```
\x05d\x05\x0b\x00\x00\x02\x00\x11@
```

216.45.67.67
Gvec.net
Added on 06.03.2014
Marion
Details
216-45-67-67.gvec.net

```
\x05d\x05\x0b\x00\x00\x00\x00\xf4[
```

166.159.65.200
Verizon Wireless
Added on 06.03.2014
Details
200.sub-166-159-65.myvzw.com

```
\x05d\x05\x0b\x00\x00\x03\x00_\xeb
```

148.64.230.90
Spacenet
Added on 05.03.2014
Details
misc-148-64-230-90.pool.starband.net

```
\x05d\x05\xc9\x00\x00\x00\x006L
```

148.64.230.42
Spacenet
Added on 04.03.2014
Details
misc-148-64-230-42.pool.starband.net

```
\x05d\x05\x0b\x00\x00\x01\x00\xba\xf0
```

85.237.243.85
Orange Slovensko, a.s.
Added on 04.03.2014
Details

```
\x05d\x05\x0b\x00\x00\x19\x00\x06@
```

Conclusions

- DNP3 is not a special case, other protocols same fate

Modbus, IEC 60870, IEC 61850, ICCP, EtherNet/IP…

- Early testing both slave/server AND master/client sides of the protocol are important!
- Compliance != Security, but the culture is important
- Don’t have to be a nation/state or large firm to do this
- A few good folks can make a difference in the industry

Go fuzz yourself before ☞ does...

Questions?

@jadamcrain
@chrissistrunk