

## Wurldtech Presents:

### From FUD to FACT: A Glimpse Into The Delphi Database

#### Presented By:

Dr. Nate Kube, *CTO*  
Wurldtech Security Technologies



## About The Speaker

### **Dr. Nate Kube – CTO, Wurldtech**

Dr. Kube directs Wurldtech's technology innovation group to improve the safety and security of global critical infrastructure. He is an expert in formal test methods, embedded systems testing, combinatorial generation, and computational complexity theory.

As the creator of the Achilles testing technology and Certification program, Dr. Kube's research efforts have been heavily funded by Canadian, American, and International Government agencies. Kube leads ISA's SP99 Derived Requirements, serves as the Industrial Cyber Security SME for the WIB Plant Security Working Group and has co-authored numerous best practices for industrial cyber security.

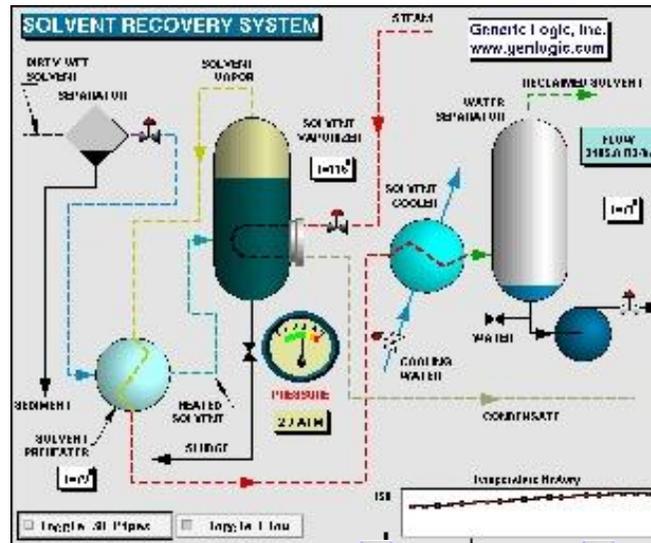
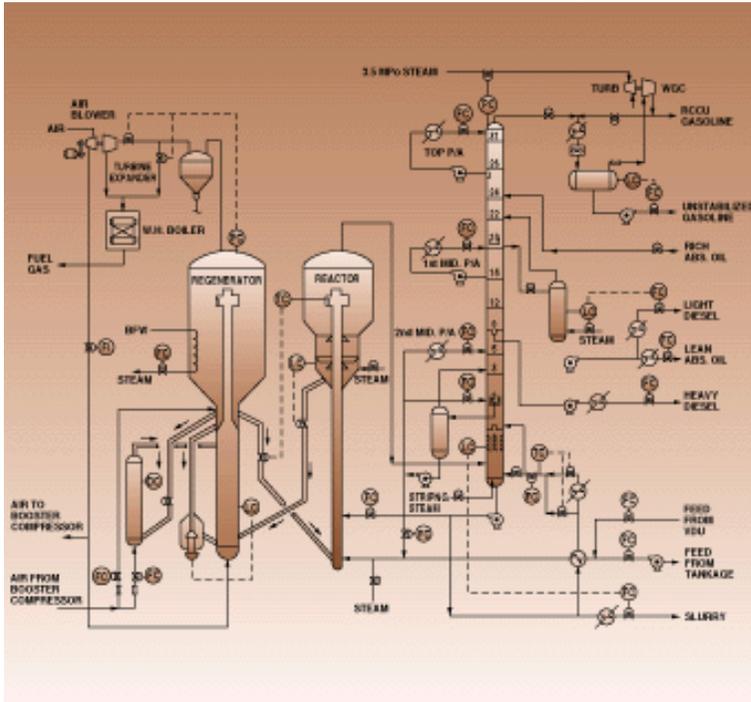
### **Wurldtech**

Founded in 2006 and now trusted worldwide by leading equipment manufacturers, system integrators, and operators of industrial automation systems, Wurldtech provides powerful technology solutions to proactively diagnose, mitigate and manage cyber risks in real-time high availability industrial environments

# Webcast Presentation Outline

- 1. Background: A Problem Statement & Delphi Motivation**
- 2. Introduction Into The Delphi Vulnerability Database Project**
- 3. Delphi Vulnerability Ranking Overview**
- 4. Overview Of Vulnerability Statistics On Embedded Devices**
- 5. What Does This Mean To Industrial Automation Stakeholders?**
- 6. Closing The Loop & Getting Involved**

# Process Control is...



# Process control systems

High level (command) computer systems  
controlling plant & machinery

Lots of display and communication of real time  
information. Measurements may be updated  
every second.

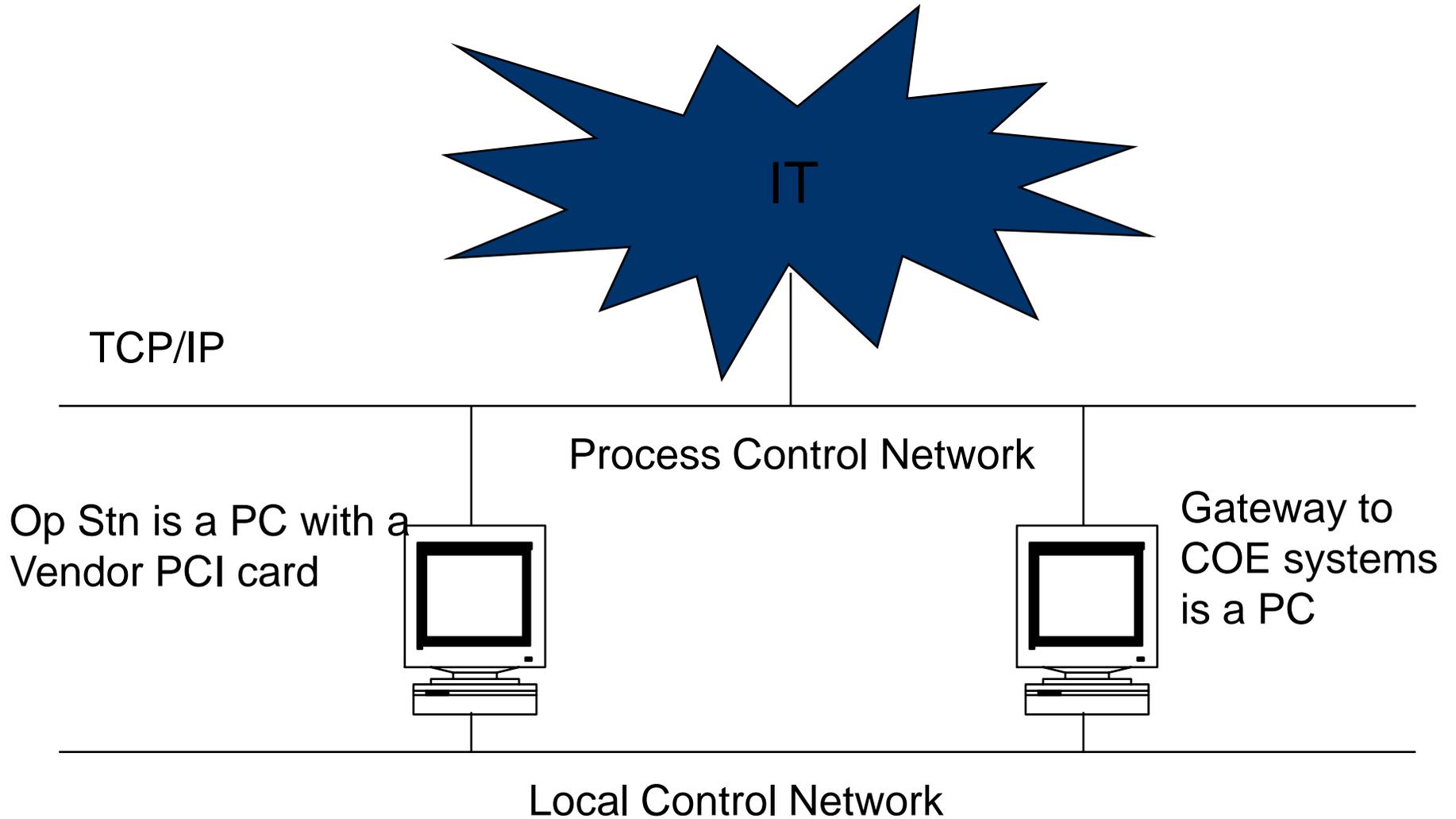
Supervisory Control and Data Acquisition Systems  
(SCADA)

Distributed Control Systems (DCS)

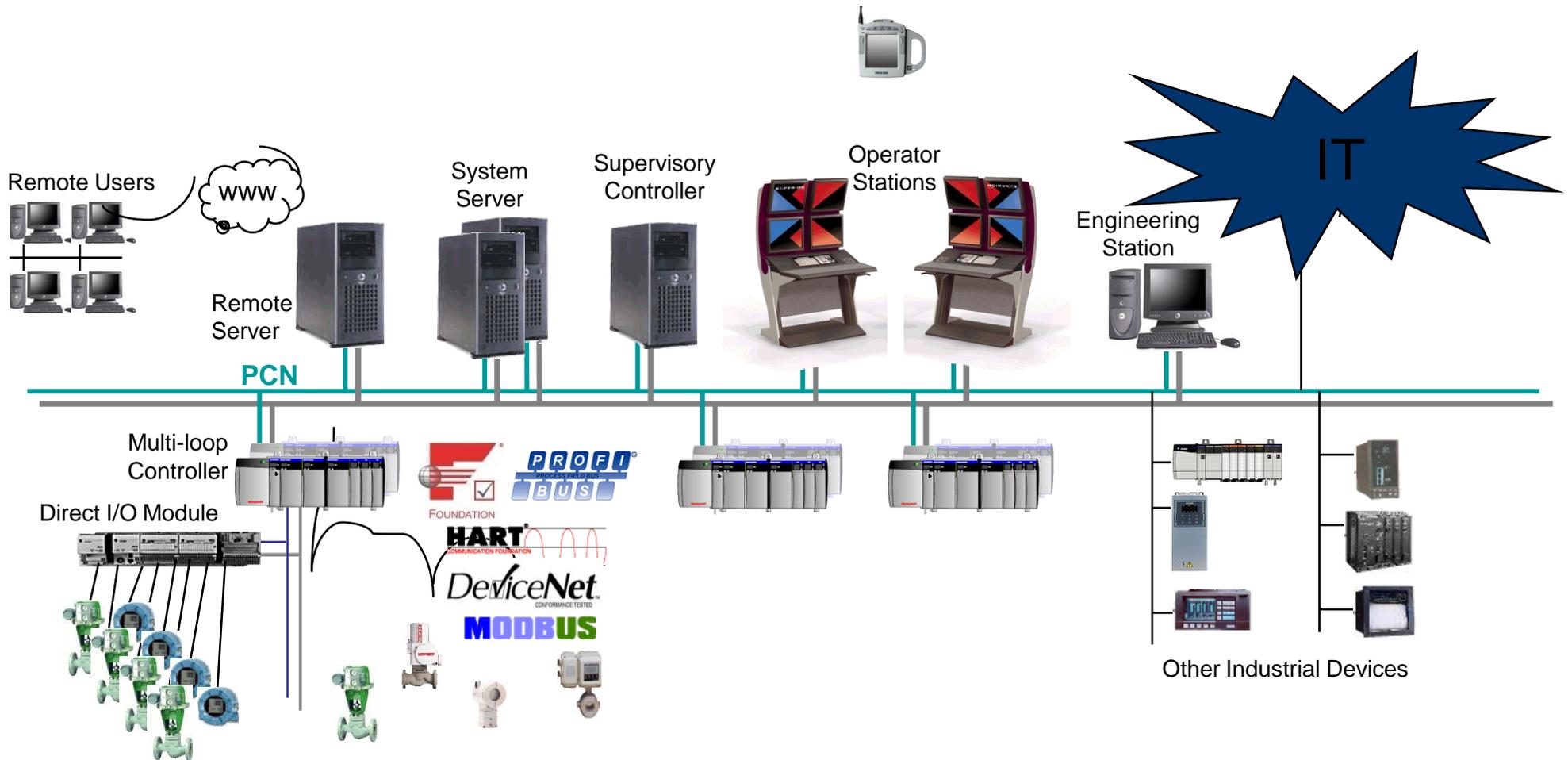
Also low level controllers



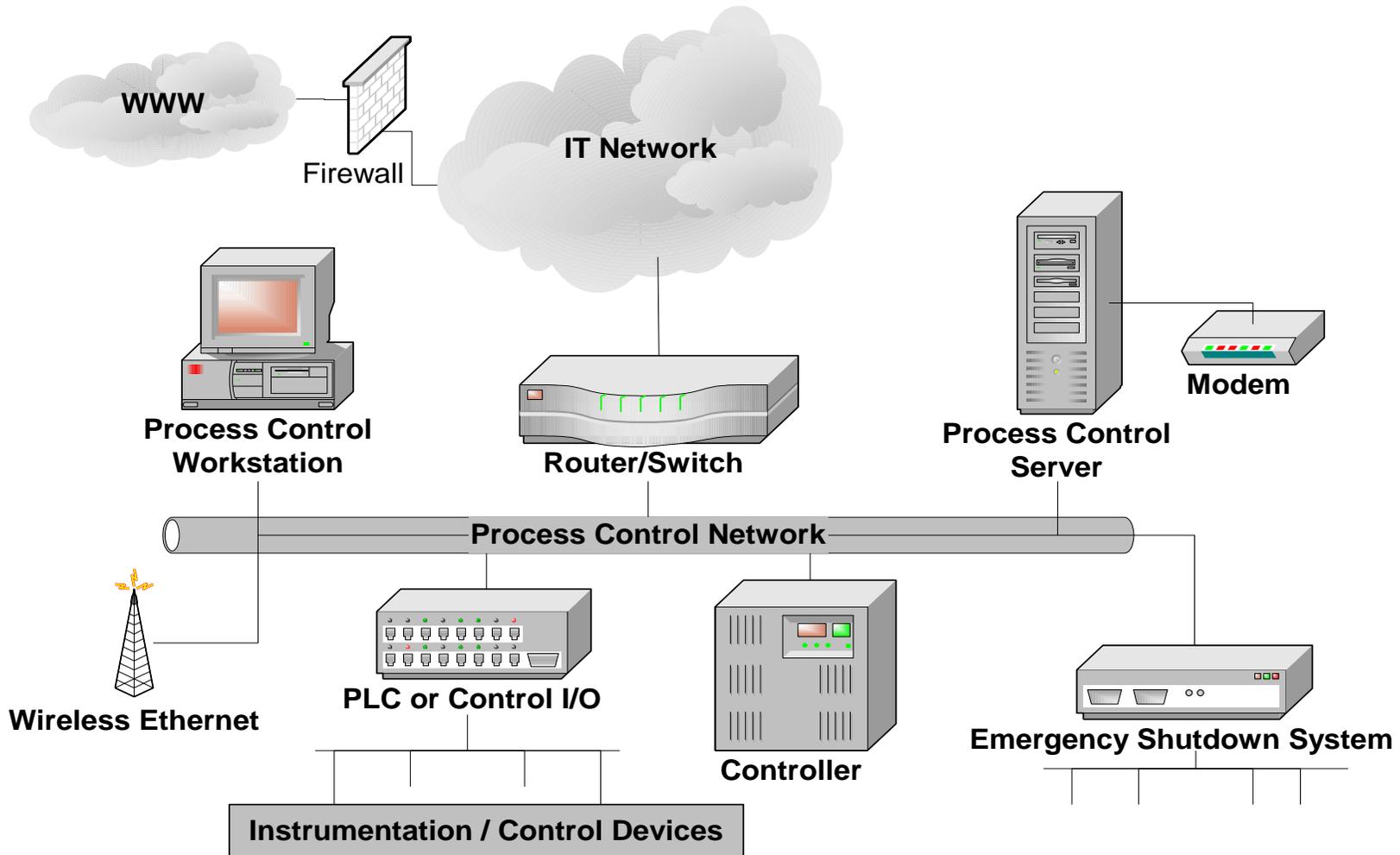
## Evolution: 1990's COTS arrive on the scene



# Evolution: 2000's Everything connected!



# Typical Control System Architecture



# The Pain: What Our Customers Tell Us

## The Evolution Of The Industrial Automation Industry

- Heavy focus on energy CIP, alt energy demand increasing, global pain, disruption attractive
- Regulation challenges & frustration (NERC / CIP)

## Emerging Industrial Automation Technologies & Infrastructure

- Emerging technologies (smart grid) not security tested, demand is growing, suppliers increasing
- No domain-driven conformance testing, interoperability unclear, impacts & risks unknown
- Current public labs are insufficiently focused and ineffective at commercialization

## Disjointed Standards & Compliance Efforts

- Too many working groups, regional representation, part-time contributors, slow progress
- Asymmetric information, no private leadership, confused end-users, not technology-driven

# The Pain: What Our Customers Tell Us

## Insufficient Cyber Security Data & Business Metrics

- No data to support business cases for security improvements & without ROI security is non-starter
- Today's solutions are anecdotal & not driven by end user demand

## Limited Knowledge Base & Subject Matter Expertise

- No central & shared repository or distribution channel to streamline intelligence
- Too few, but at the same time too many “Pundits” with dated expertise & technology experience
- Trust diminishing amongst cyber security professionals & distrust increasing with operators

## So What Is A Solution? Data & Distribution

- Data (More, Better, Faster & Frequent)
- Distribution (Centralized, Symmetric, & Efficient)

# The Wurldtech Industrial Cyber Security Lifecycle

**Data**      **Translation**      **Distribution**



**Vendors**



**Operators**



**Delphi Database**



**Achilles Inside**



**Wurldtech Labs /  
BCIT COE**

# Where It All Starts - The Achilles Satellite



## Domain Specific Design

- Physical Layer Support For Common Industrial Control Requirements (OPC, Digital I/O)
- Common Industrial Protocols & Available Proprietary Protocol Test Suites

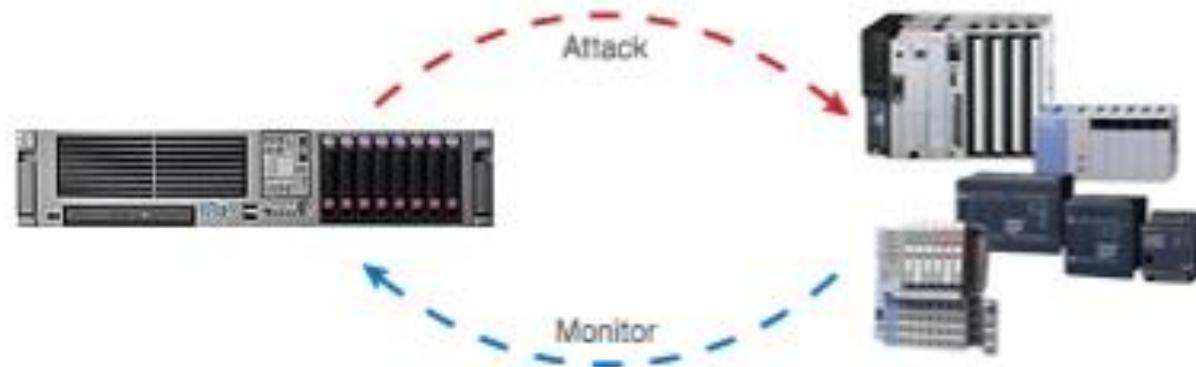
## Innovative Test Framework & Packet Generation

- Automated Grammar-based Testing & Stateful Packet Generation
- Third Party Test Tool Integration & Customizable Test Case Creation (Nessus, Codenomicon)

# Why Does Wurldtech Have So Much Data?

Testing Technology, Access Depth, Strong Partnerships & Industry Trust

Standard Test Methodology



Single Controller Test Bench



# Collect, Characterize & Build Resilience Profiles

## So What Is Delphi?

- Information Architecture Designed To Centralize & Distribute IA Cyber Risk Information
- The Delphi Program Is An Ongoing Effort Led By Wurldtech Labs & Industry Partners To Create A Centralized Repository Of Resilience Profiles For IACS Components.
- IACS components are categorized in Delphi according to SP99 Derived Requirements model: Applications, Network devices, Host devices, Embedded devices

## What Is The Point? Try To Secure A Building Without A Blueprint

- Understanding The Actual Risk Posture Of The Industry (No FUD Please!)
- Constructing Measures That Accurately Mitigate Present Weaknesses (Rule-sets, Sigs)
- Quantifying ROI On Security Technology Investments
- Enabling Informed Decisions!

# Today's Focus: Early Results - Embedded Devices

## What Is An Embedded Device?

- Embedded device is a device containing embedded software that communicates over a network interface which directly monitors, controls or actuates an industrial process e.g. PLC, RTU, DCS controller, SIS PLC

## What Is An Embedded Device Resilience Profile?

- A Resilience Profile For An Embedded Device Reflects A Device's Ability To:
  - *Resist Systematic Failure, &*
  - *Maintain Safe And Consistent Control Of A Process*

## This Resilience Profile Contains Properties Including:

- Vulnerabilities, Their Trigger, And Rank (Based On Impact To Key Functionalities)
- Effective Mitigation Strategies (Firewall Rulesets/IDS-IPS Signatures)
- Stable Operating Parameters (Resource Limits)

# Vulnerability Ranking

## LoV, PLoV, LoC, PLoC

- Yes, & Many More...Vulnerabilities Can Be Ranked Based On Their Impact To Key Embedded Device Functionalities Such As Available And Control

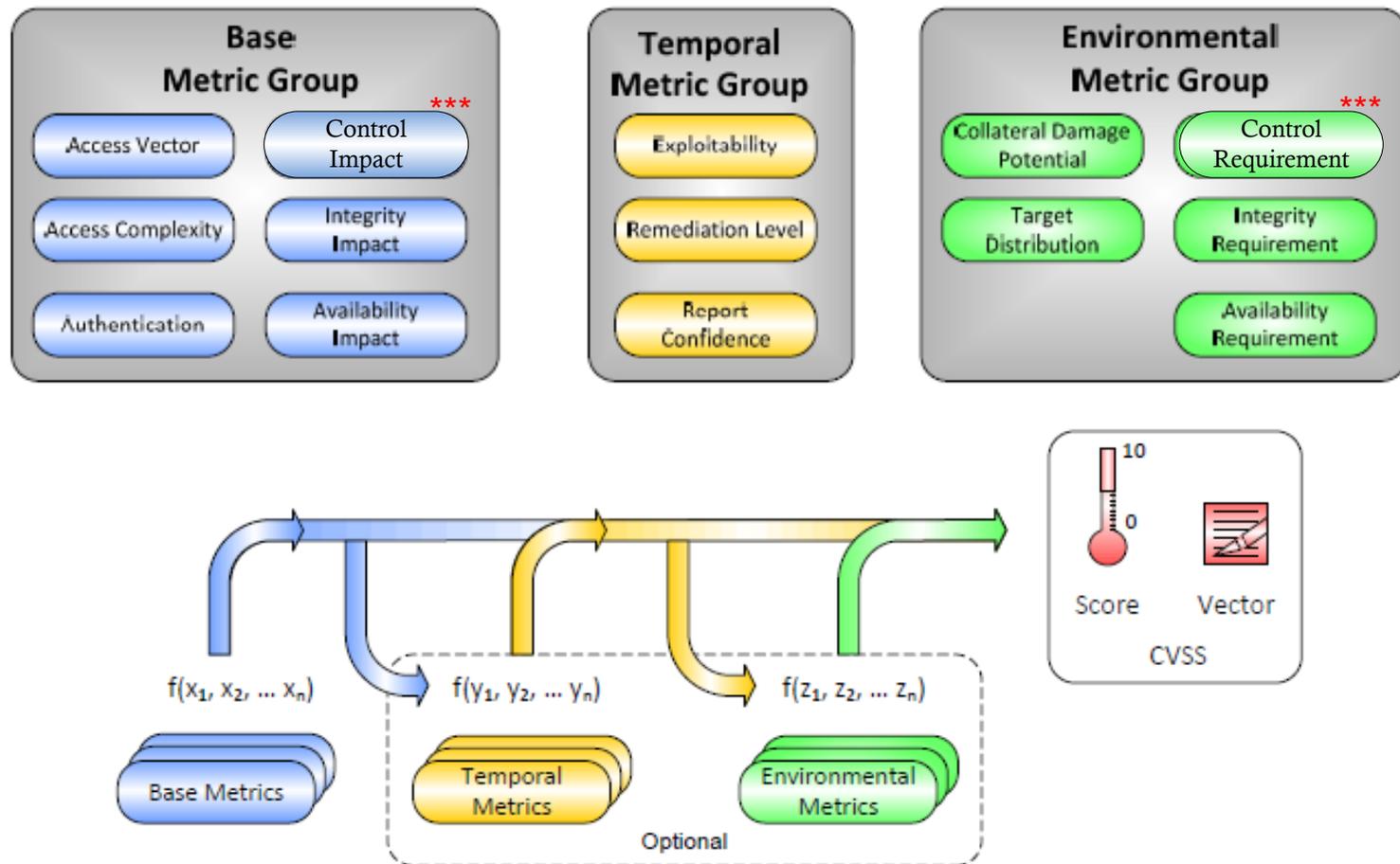
Device	Test Case	Monitors Impacted	Recovery Time	Rank
SIS PLC	Arp Cache Saturation Storm	Discrete, ICMP	Requires Restart	PLoV + PLoC

## Interesting, Intuitive, However Far From Complete

- How Complex Was The Attack? Can It Be Executed Remotely? How Important Is The Device's Operation To The Maintenance Of Your Business? Are There Environmental Or Public Safety Considerations?

# Vulnerability Ranking ++

## CVSS V2 Augmented For Embedded Devices



# Base Metric Group – Control & Availability Impact

## Control Impact

Metric Value	Description
None (N)	There is no impact to the control of the system.
Partial (P)	There is a temporary disruption of the device's ability to control other devices.
Complete (C)	There is a permanent disruption of the device's ability to control other devices. The device must be restarted or some other measure must be taken to resume normal device behavior.

- Maps Nicely To Loss-of-Control (LoC) and Permanent Loss-of-Control (PLOC)

## Availability Impact

Metric Value	Description
None (N)	There is no impact to the availability of the system.
Partial (P)	Monitoring devices are temporarily unable to view the status of the device.
Complete (C)	Monitoring devices are permanently unable to view the status of the device. The device must be restarted or some other measure must be taken to resume normal device behavior.

- Maps Nicely To Loss-of-View (LoV) and Permanent Loss-of-View (PLOC)

# Environmental Metric Group – Collateral Damage Potential

Metric Value	Description
None	There is no potential for loss of life, physical assets, productivity or revenue
Low	A successful exploit of this vulnerability may result in slight physical or property damage. Or, there may be a slight loss of revenue or productivity to the organization.
Low-Medium	A successful exploit of this vulnerability may result in moderate physical or property damage. Or, there may be a moderate loss of revenue or productivity to the organization.
Medium-High	A successful exploit of this vulnerability may result in significant physical or property damage. Or, there may be a significant loss of revenue or productivity to the organization.
High	A successful exploit of this vulnerability may result in catastrophic physical or property damage. Or, there may be a catastrophic loss of revenue or productivity to the organization.

Control Impact	Availability Impact	Collateral Damage	
		DCS	SIS
None	Partial	Low	Low-Medium
Partial	None	Low-Medium	Medium-High
Partial	Partial	Low-Medium	Medium-High
None	Complete	Low-Medium	Medium-High
Partial	Complete	Medium-High	High
Complete	None	High	High
Complete	Partial	High	High
Complete	Complete	High	High

# Environmental Metric Group – Control & Availability Requirement

## Control Requirement

Metric Value	Description
Low (L)	Loss of control is likely to have only a limited adverse effect on the organization or individuals associated with the organization (for example, employees, customers).
Medium (M)	Loss of control is likely to have a serious adverse effect on the organization or individuals associated with the organization (for example, employees, customers).
High (H)	Loss of control is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (for example, employees, customers).
Not Defined (ND)	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

- Depends On Device Type. For DCS Control Requirement Is Medium, For SIS it Is High

## Availability Requirement

Metric Value	Description
Low (L)	Loss of availability is likely to have only a limited adverse effect on the organization or individuals associated with the organization (for example, employees, customers).
Medium (M)	Loss of availability is likely to have a serious adverse effect on the organization or individuals associated with the organization (for example, employees, customers).
High (H)	Loss of availability is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (for example, employees, customers).
Not Defined (ND)	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

- Depends On Device Type. For DCS Control Requirement Is Low, For SIS it Is Medium

# DCS Example Excerpt

Device	Test Case	Monitors Affected	Recovery Time
DCS Controller A	ICMP Storm	ARP, ICMP, Discrete	<60 sec after test ends

Metric	Value
Access Vector	Network
Control Impact	Partial
Availability Impact	Partial
Collateral Damage Potential	Low-Medium
Control Requirement	Medium
Availability Requirement	Low

Calculations for Base Score:

```

BaseScore = (.6*AdjustedImpact +.4*Exploitability-1.5)*f(AdjustedImpact) =
(.6 * 3.9005 + .4 * 9.9968 - 1.5)*1.176 = 5.69
AdjustedImpact =
Min(10,10.41*(1 - (1-ContImpact*ContReq)*(1-IntegImpact*IntegReq)*(1-AvailImpact*AvailReq))
) = Min(10,10.41 * (1-(1-0.275*1)*(1-0*1)*(1-0.275*0.5))) =
Min(10,10.41 * (1-.725*1*.8625)) = 3.9005
Exploitability = 20*AccessComplexity*Authentication*AccessVector = 20 * 0.71 * 0.704 * 1 =
9.9968
f(AdjustedImpact) = 0 if Impact=0; 1.176 otherwise
  
```

The Base Score value is then used to calculate the Temporal Score:

```

TemporalScore = BaseScore*Exploitability*RemediationLevel*ReportConfidence =
5.69 * 1 * 1 * 1 = 5.69
  
```

# Delphi Statistics – Entry Overview

## What Is Considered A “Unique” Vulnerability?

{device; attack type; rate; impact}

## What Do Typical Entries Look Like?

Test	Severity	Monitors Impacted	Rate (fps)	Packet Size (bytes)	Recovery Time	Device Type	Industries
Ethernet Unicast Storm	3.1	ARP	14880	60	<10 sec after test ends	DCS	Oil & Gas, Chemicals, Marine
IP Unicast Storm	6.5	Discrete	10000	60	<10 sec after test ends	DCS	Mining and Metal, Pulp and Paper
TCP/IP LAND Attack	8.5	ARP, Discrete	50	60	Reset required	DCS	Power T & G, Oil & Gas, Chemicals
UDP Multicast Storm	5.3	ICMP, ARP	2000	60	<10 sec after test ends	SIS	Oil & Gas, Chemicals, Food and Beverage
IP Fuzzer	8.7	ICMP, ARP	1000	60	Reset required	SIS	Food and Beverage, Water/Waste Water

# Delphi Statistics – Industry Overview

## 46 Embedded Devices/Versions

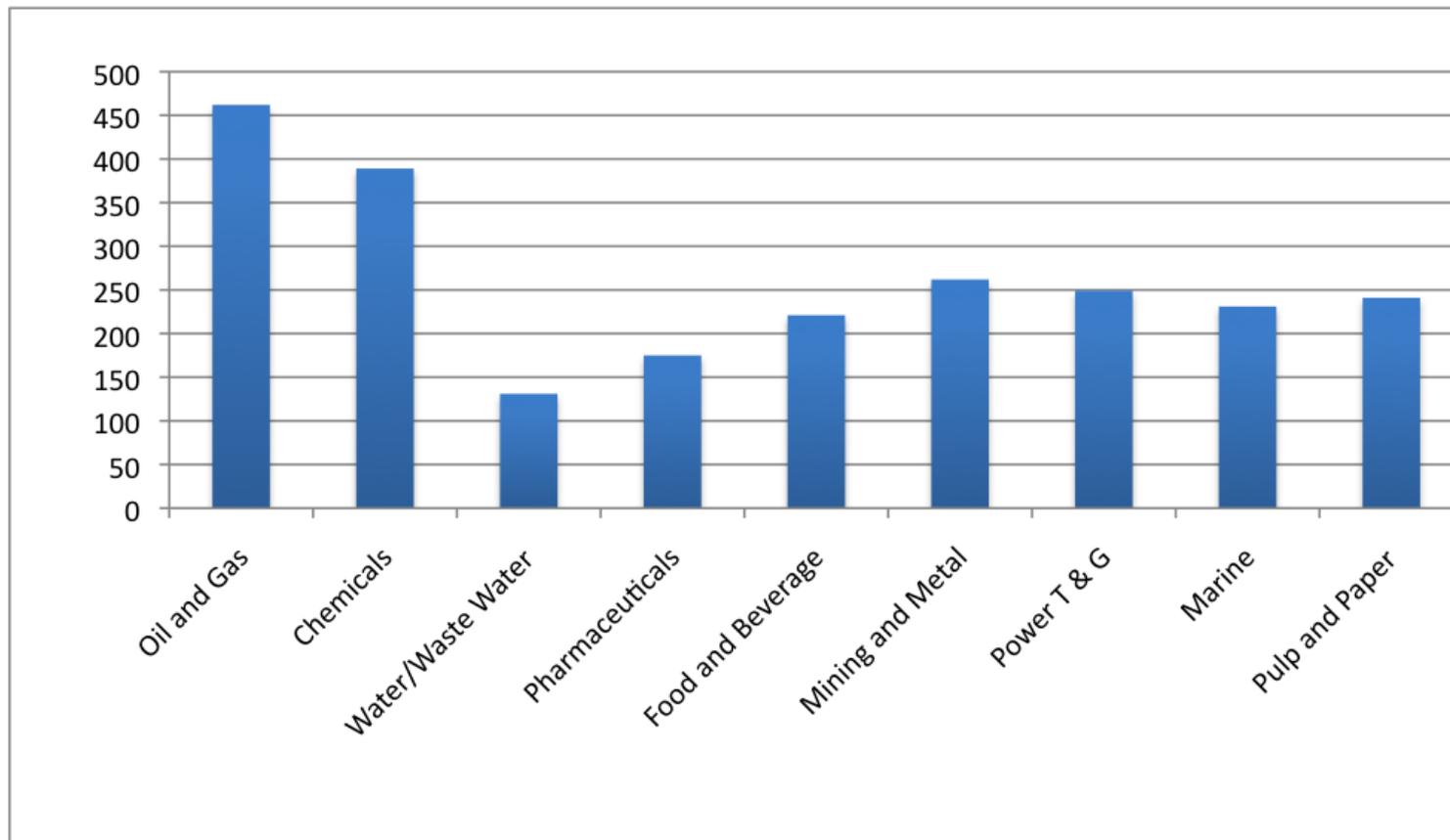


Figure 1: # vulnerabilities over all embedded devices; all industries; all protocols

# Delphi Statistics – Oil & Gas Impact Overview

## 23 DCS And SIS Devices/Versions Tested In Oil and Gas

460 Unique Vulnerabilities

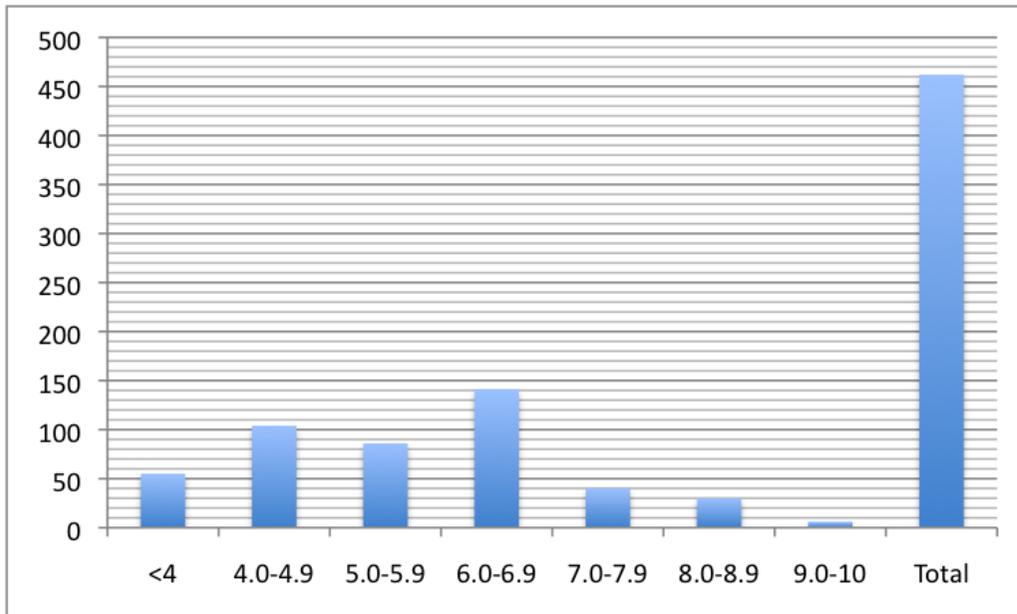


Figure 2: # of vuls in oil and gas by cvss score

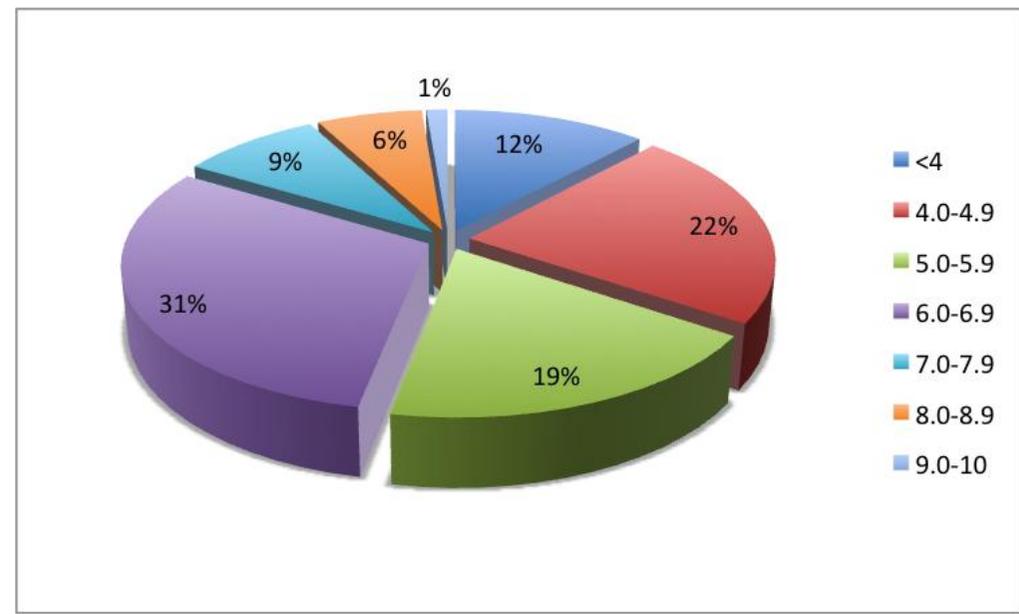


Figure 3: distribution of cvss scores over all oil & gas vuls

# Delphi Statistics – DCS / SIS Impact Overview

**32 DCS And SIS Devices/Versions**

**505 Unique L2-L4 Vulnerabilities**

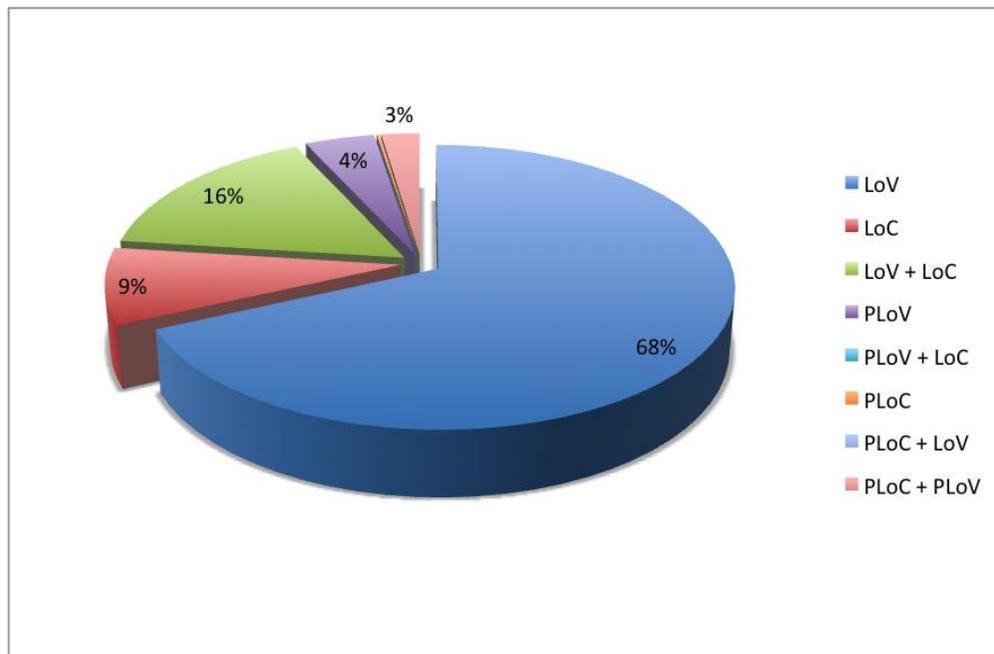


Figure 4: distribution of monitor impact over L2-L4 dcs/sis vuls

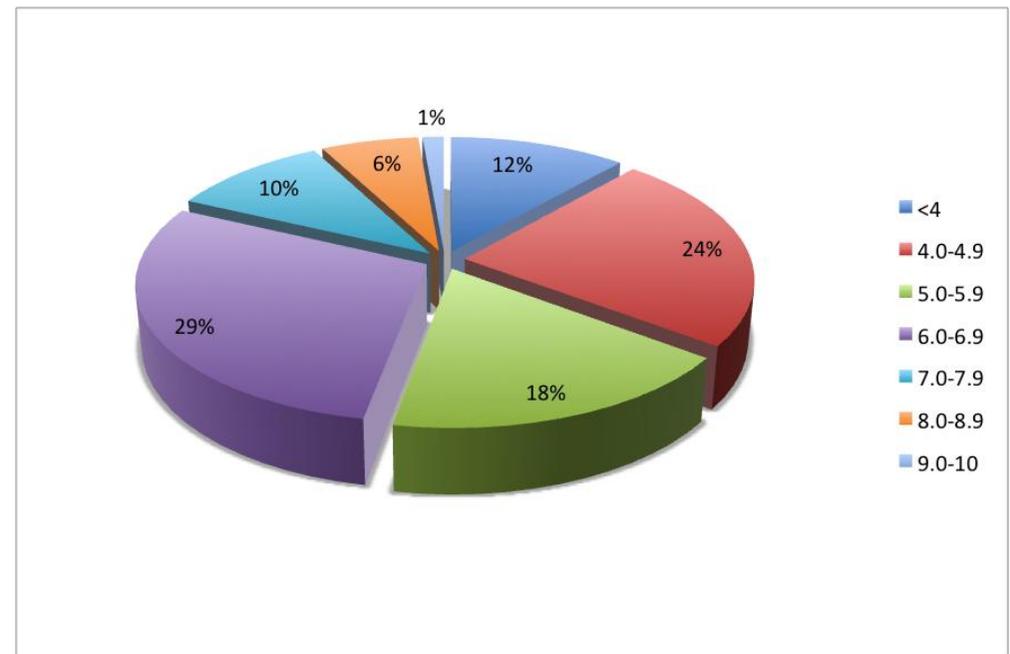


Figure 5: distribution of cvss scores over L2-L4 dsc/sis vuls

# Delphi Statistics – DCS Impact Overview

## 21 DCS Controllers/Versions

289 Unique L2-L4 Vulnerabilities

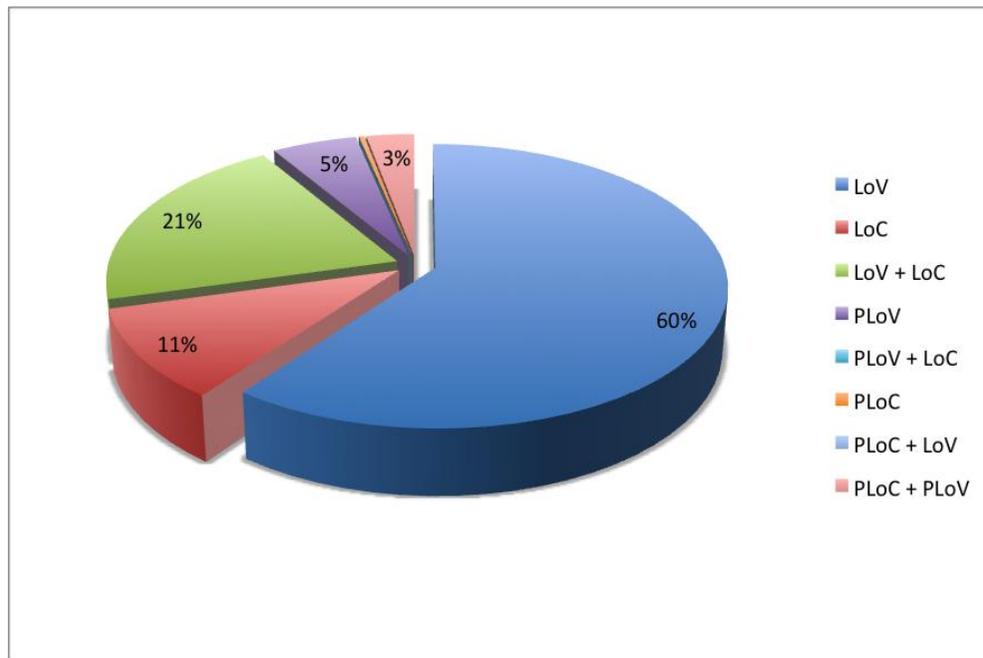


Figure 6: distribution of monitor impact over L2-L4 dcs vuls

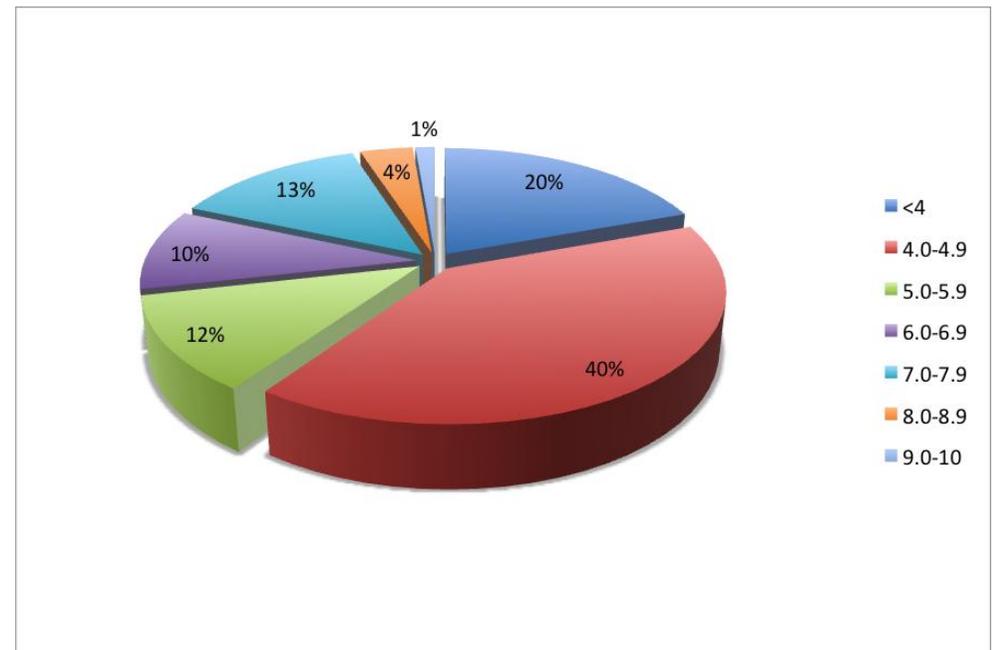


Figure 7: distribution of cvss scores over L2-L4 dcs vuls

# Delphi Statistics – SIS Impact Overview

## 11 SIS PLCs/Versions

207 Unique L2-L4 Vulnerabilities

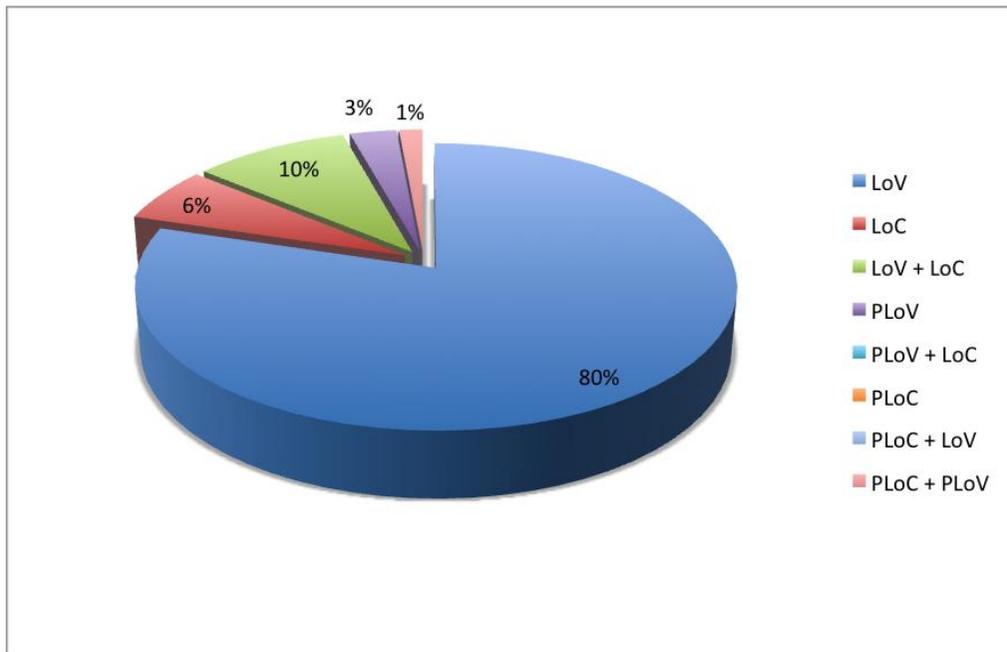


Figure 8: distribution of monitor impact over L2-L4 sis vuls

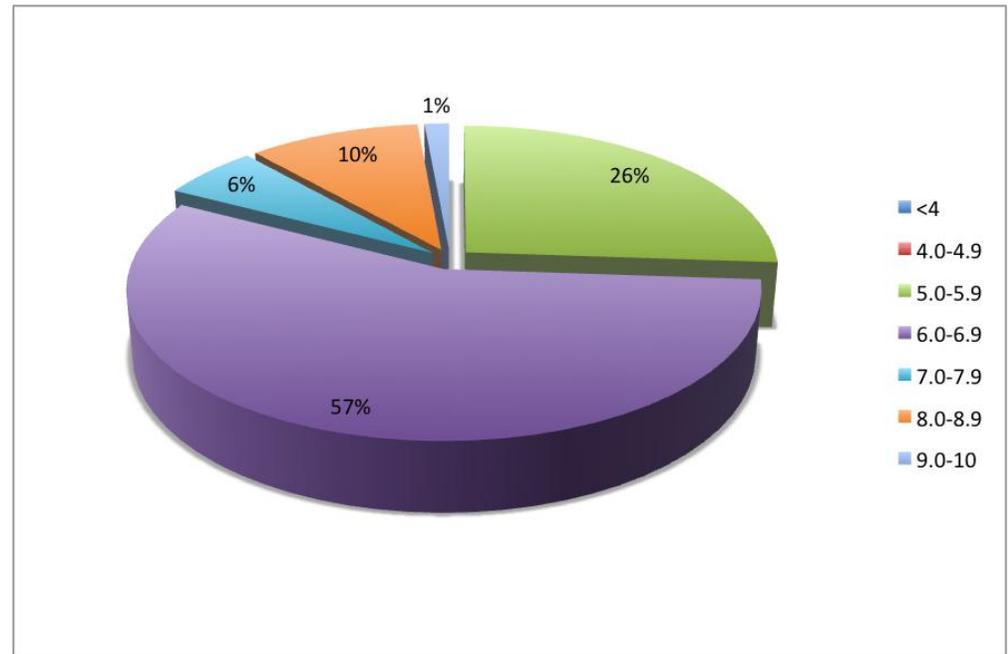


Figure 9: distribution of cvss scores over L2-L4 sis vuls

# Delphi Statistics – Lower Layers & Rate

## 32 DCS And SIS Devices/Versions

505 Unique L2-L4 Vulnerabilities

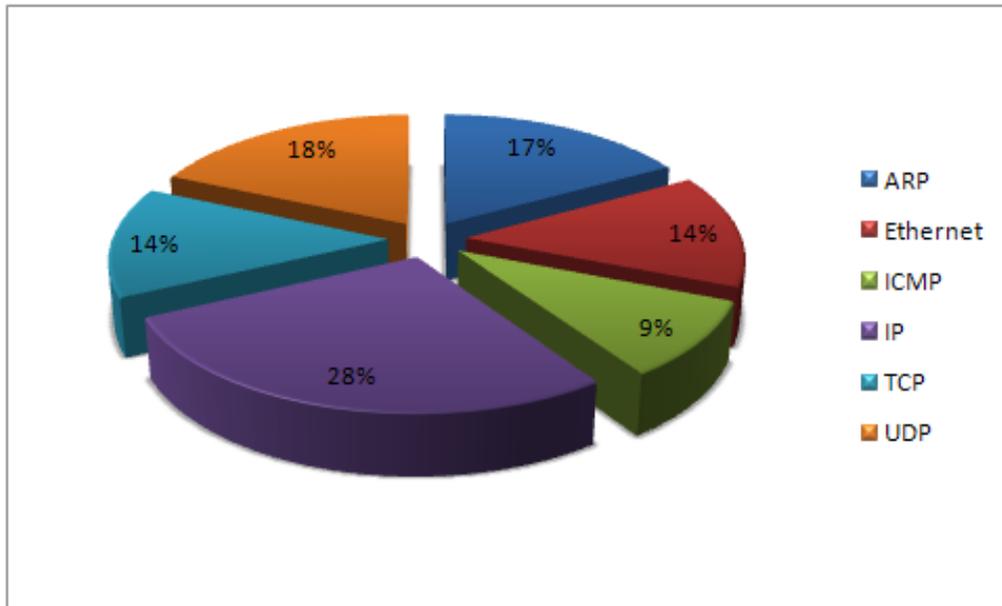


Figure 10: L2-L4 distribution over dcs/sis vuls

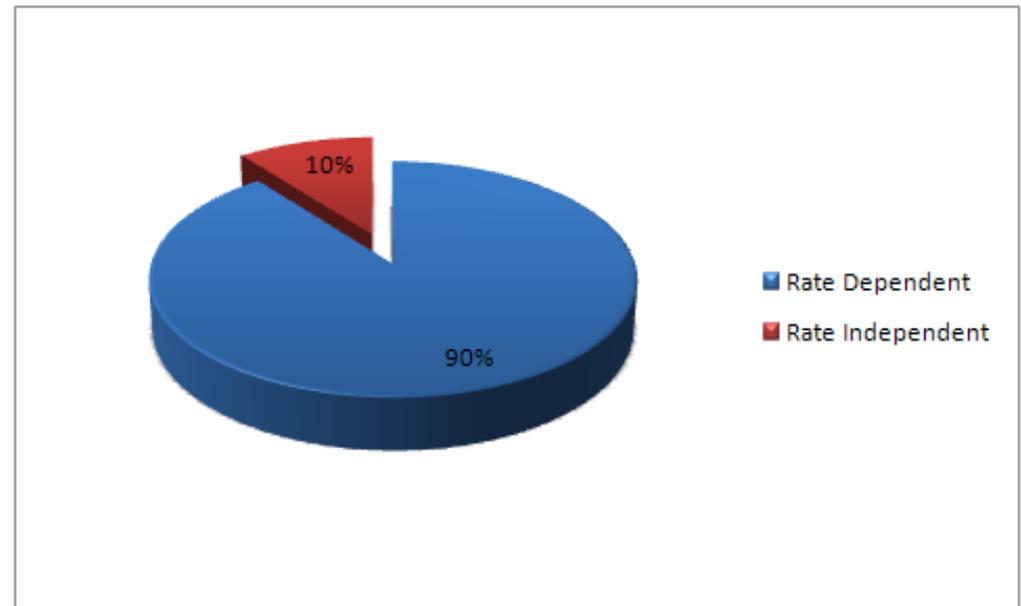


Figure 11: rate requirement distribution over L2-L4 dcs/sis vuls

# Delphi Statistics - Achilles Level 1 Test Cases

## 46 Embedded Devices/Versions

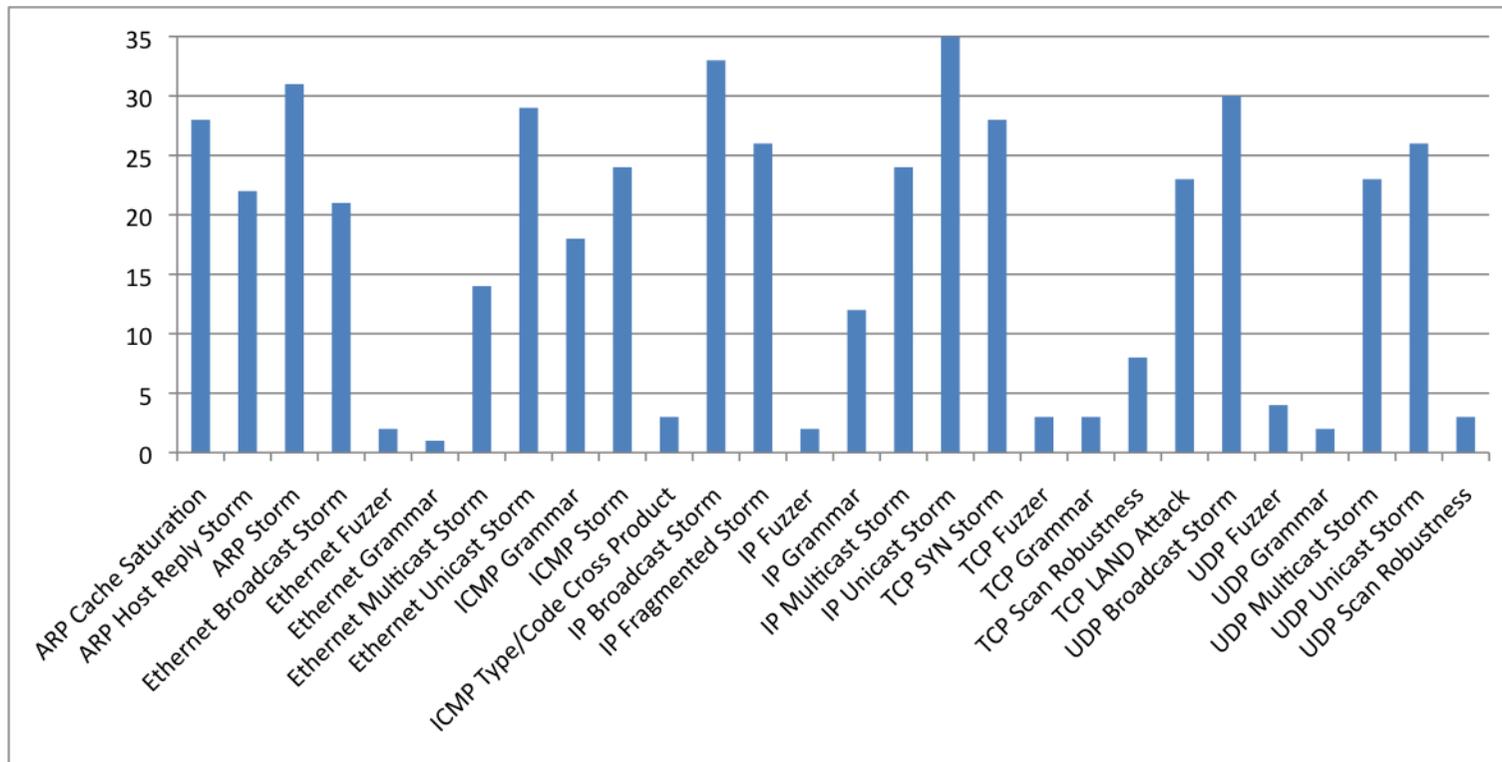


Figure 12: # of L2-L4 vuls found per Level 1 test case

# Delphi Statistics – Achilles Level 1 Overview

## 32 DCS And SIS Devices/Versions

505 Unique L2-L4 Vulnerabilities

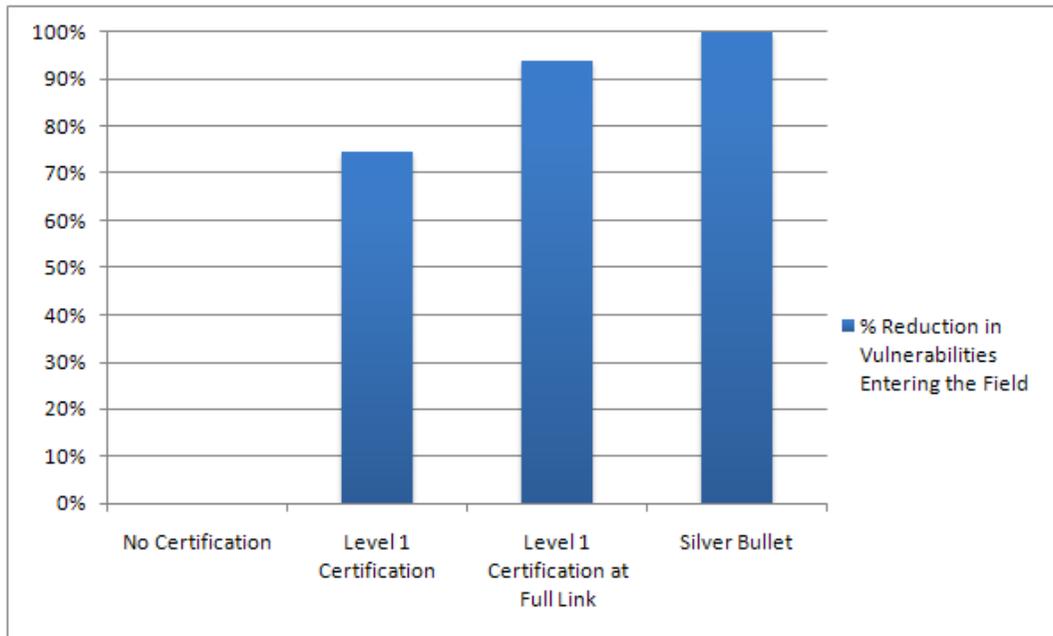


Figure 13: % reduction in L2-L4 dcs/sis vuls

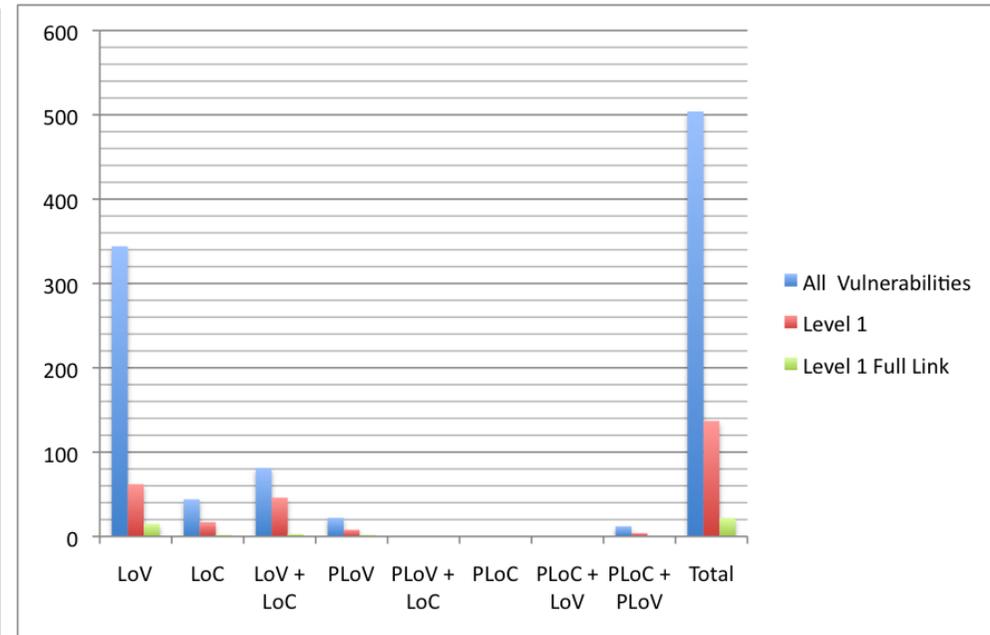


Figure 14: # L2-L4 dcs/sis vuls present post Achilles Level 1

# Delphi Statistics – Achilles Level 1 DCS/SIS

## 21 DCS And 11 SIS Devices/Versions

298 Unique DCS And 207 Unique SIS Vulnerabilities

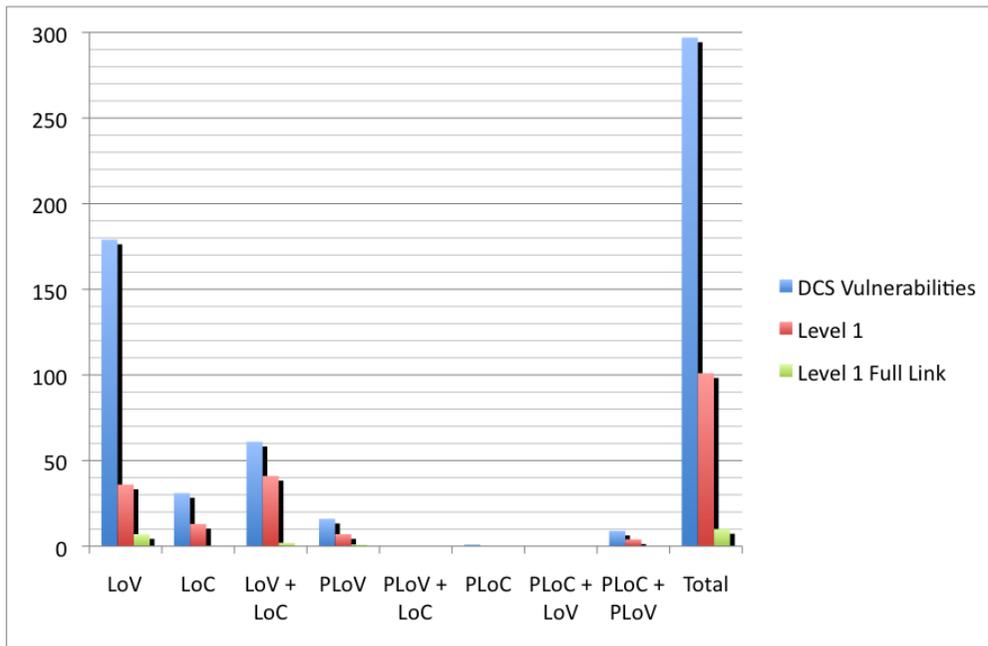


Figure 15: # L2-L4 dcs vuls present post Achilles Level 1

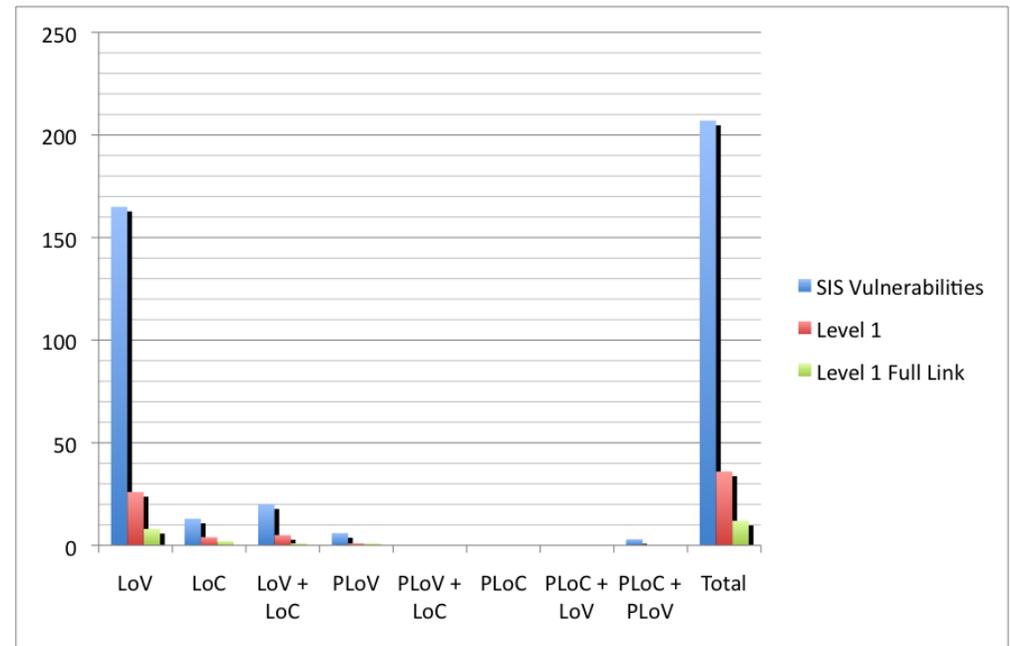


Figure 16: # L2-L4 sis vuls present post Achilles Level 1

# Conclusions

## Let's Recap

- **What Is Delphi?**
  - *Information Architecture Designed To Centralize & Distribute Meaningful, Relevant & Up To Date IA Cyber Risk Information*
- **Why Did We Create Delphi?**
  - *We Had The Data, Experience, Access & Distribution*
  - *Because Our Customers Asked!*
- **What Are The Benefits Of Delphi Information?**
  - *Business Case / ROI & Effective Decision Making*
  - *Targeted, Proactive, and Rapid Mitigation*
- **Some Examples**
  - *Case Study #1: Major Oil & Gas Operator*
  - *Case Study #2: Major DCS Vendor*

# So What Can You Do? Be Proactive & Get Involved



## Equipment Manufacturers Of Industrial Control / Safety Systems

- Integrate Robustness & Certification Testing Into Development Lifecycle
- Partner With Wurldtech Labs (Utilize Delphi Data For Directing Security Resources)
- Send Systems To Wurldtech Labs For Testing and Analysis



## Asset Owners / Operators & System Integrators

- Insist On Achilles Certified Systems & Introduce Certification Criteria Into FAT's
- Partner With Wurldtech Labs (Utilize Delphi Data Feed For Current Risk Posture)
- Engage Wurldtech Testers For Rapid Risk Analysis Of Critical Assets

# Conclusions

## Let's Recap

- **What Is Delphi?**
  - *Information Architecture Designed To Centralize & Distribute Meaningful, Relevant & Up To Date IA Cyber Risk Information*
- **Why Did We Create Delphi?**
  - *We Had The Data, Experience, Access & Distribution*
  - *Because Our Customers Asked!*
- **What Are The Benefits Of Delphi Information?**
  - *Business Case / ROI & Effective Decision Making*
  - *Targeted, Proactive, and Rapid Mitigation*
- **Some Examples**
  - *Case Study #1: Major Oil & Gas Operator*
  - *Case Study #2: Major DCS Vendor*

## THANK YOU

Any Questions?

**For Further Information:**

Contact: Nate Kube  
[nkube@wurldtech.com](mailto:nkube@wurldtech.com)

Or

Visit Our Website:

[www.wurldtech.com](http://www.wurldtech.com)

