

A photograph of an industrial facility, likely a refinery or chemical plant, featuring a complex network of pipes, metal structures, and large storage tanks. The scene is set against a clear blue sky with a city skyline visible in the background. The foreground is dominated by a dark, semi-transparent banner containing the title text.

How Threat Modeling Can Influence ICS Security Posture

Luca Bongiorno
21st September 2019

Bentley[®]
AppSec Team



 @lucabongiorni

- Principal Offensive Security Engineer at



- After this presentation, you will:

- Understand what is Threat Modeling and how can help you Securing your Industrial Control Systems
- Learn about its State of Art and which tools you can use nowadays

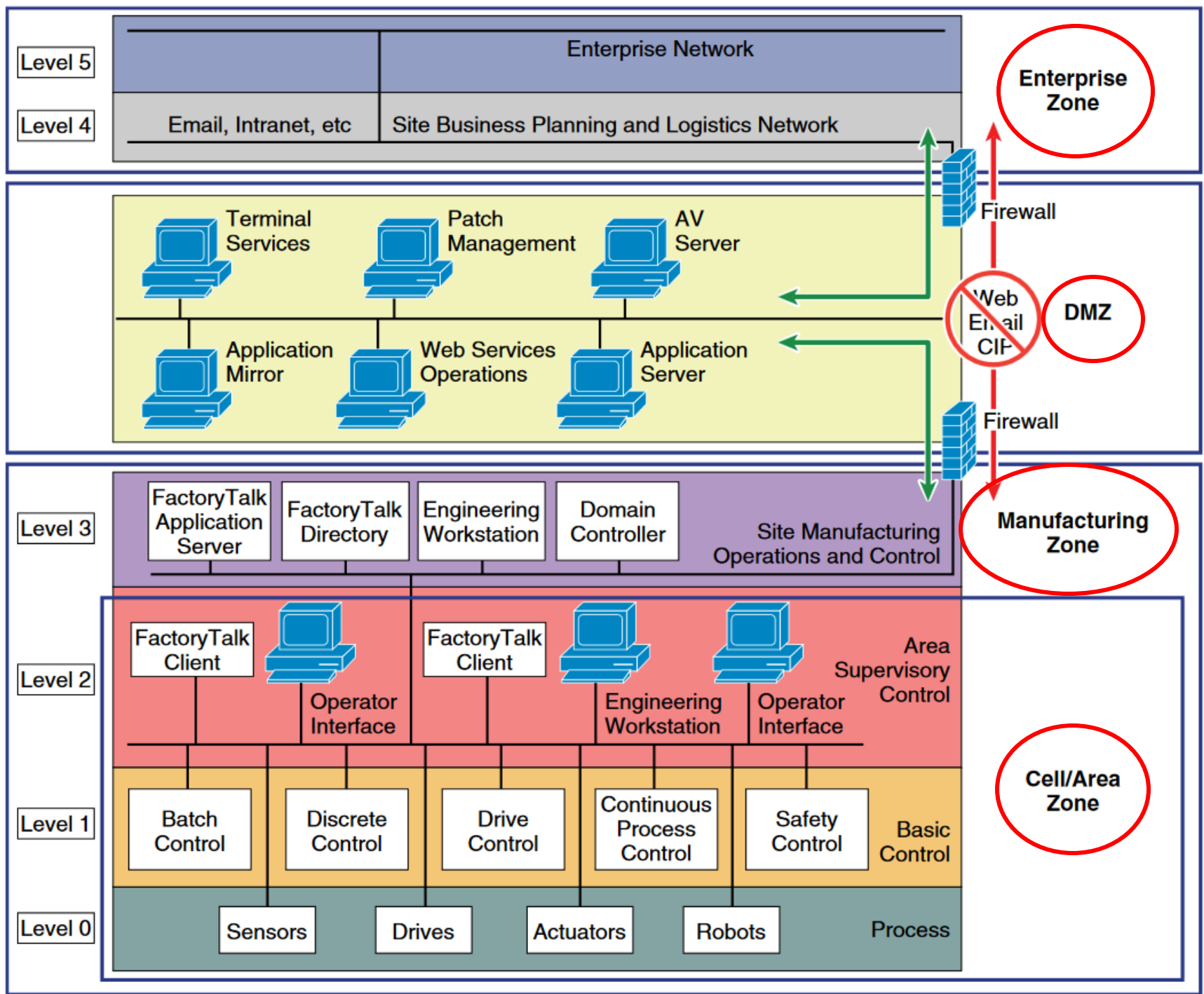
Vulnerability Vs Threat Vs Risk

Close the **Open Door**
(**Vulnerability**) to
keep out the **Bear**
(**Threat**).

Otherwise we are
Screwed (Risk).



ENTRY POINTS

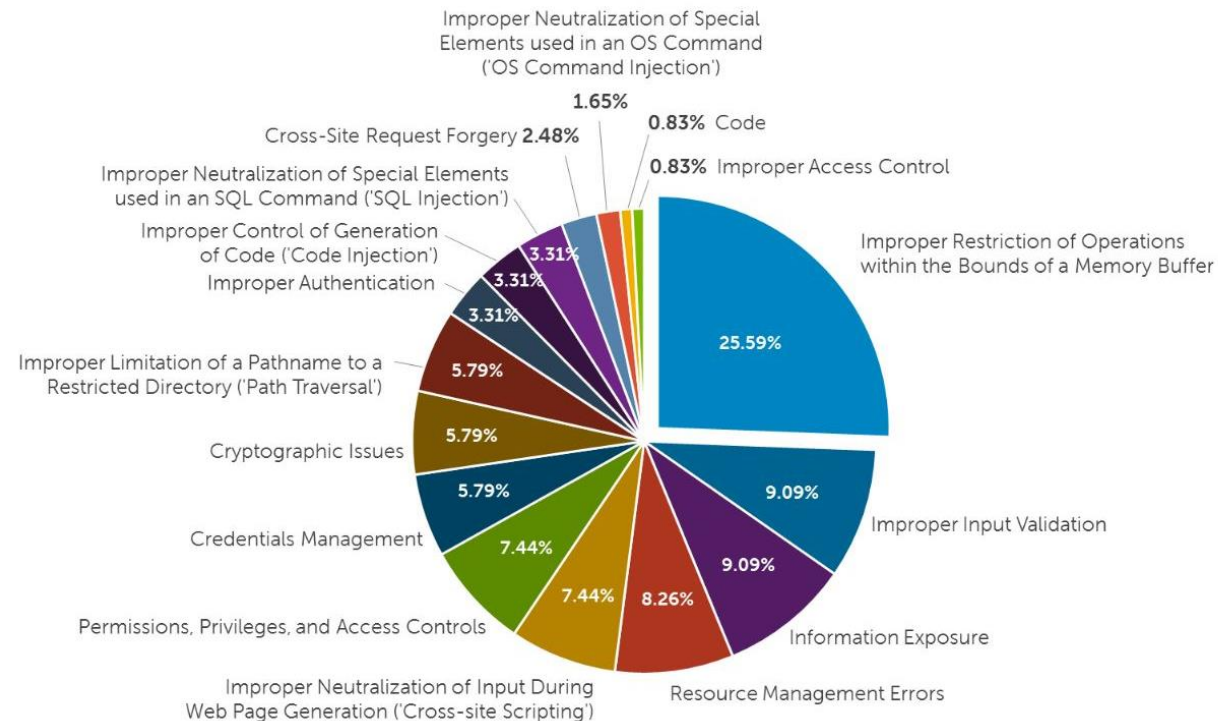


Most of the Attacks Methods are related to Application Security*

(i.e. OWASP Top 10 and SANS Top 25)

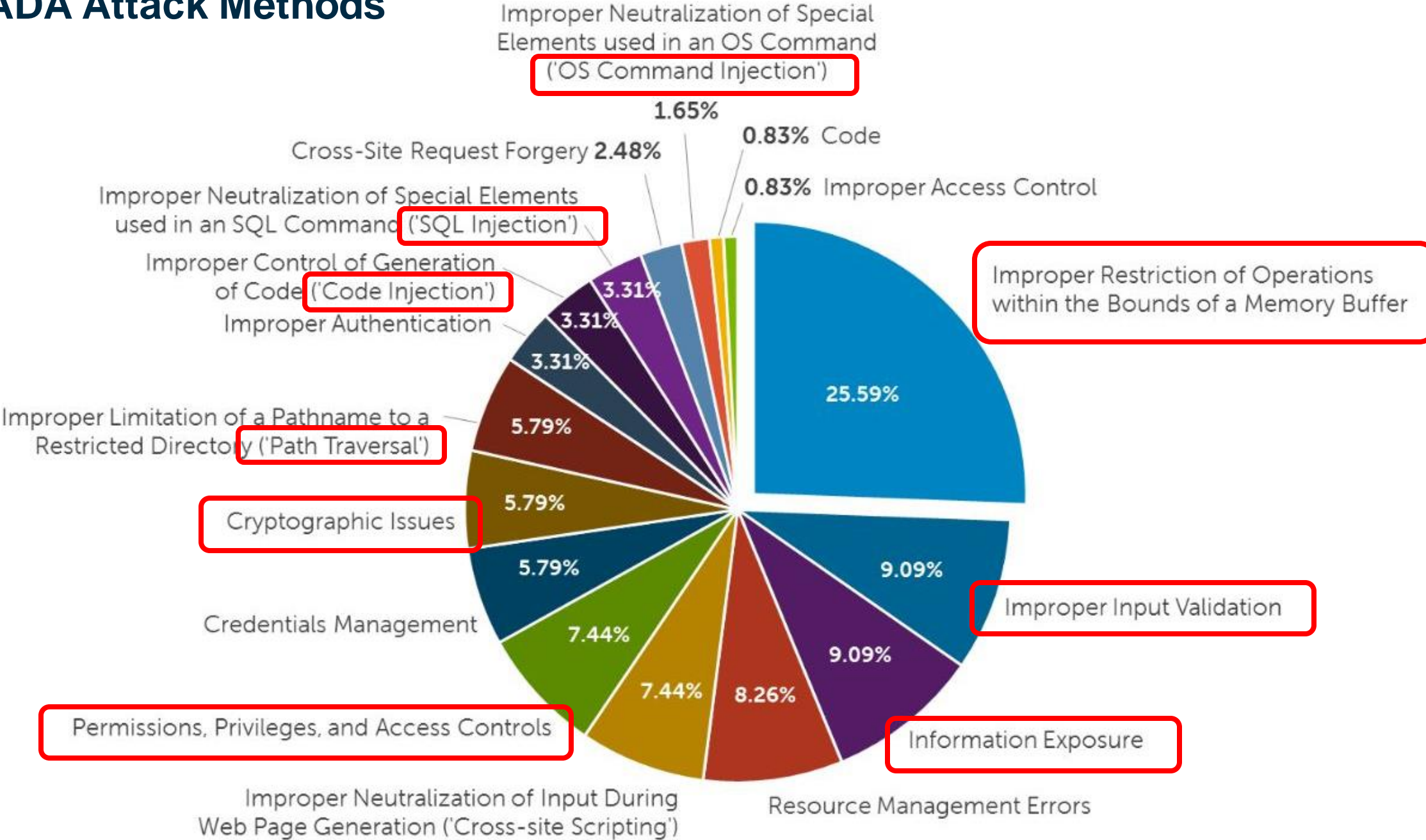
Which are:

- **Well documented**
- **Already have recommended mitigations available**



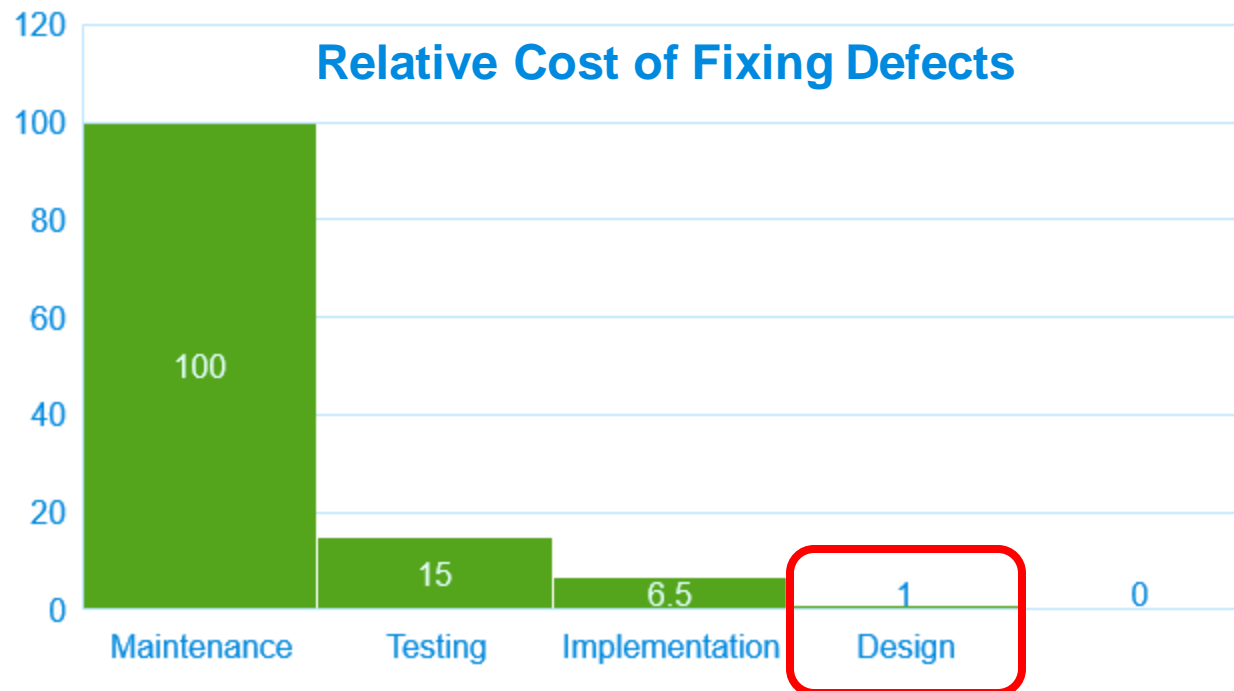
* [Dell Security Annual Report 2015](#)

Key SCADA Attack Methods



Three Reasons for Threat Modeling

- **Produces Measurable Data** >> # of Threats & Associated Risk
- **It Smooth the path to Compliance** >> Happy Auditors
- **It Saves Money** >> Happy CFO/CEO/Shareholders
 - You Spot Security Flaws When It's Much Cheaper to Fix Them

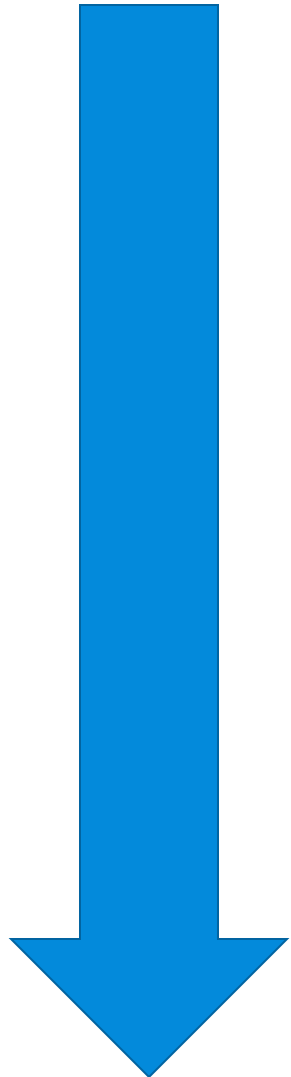


Software Development Life Cycle



Secure Software Development Life Cycle

Threat Modeling Process



Create Assets' Inventory

Architecture Review Model

Decompose Model in Single Assets

Identify Threats within those Assets

Document Threats

Rate Threats

STRIDE

- Invented in 1999 & Adopted by Microsoft in 2002
- The most mature
- It evaluates the system architecture by using Data Flow Diagrams (DFD)
- It is used to identify system's entities and boundaries
- It applies a general set of known threats based on its acronym for its entity or boundary

	Threat	Property Violated	Threat Definition
S	Spoofing	Authentication	Pretending being something/someone else
T	Tampering	Integrity	Modifying something on net/disk/memory/etc
R	Repudiation	Non Repudiation	Claiming that you didn't do something or viceversa
I	Information Disclosure	Confidentiality	Access information to someone not authorized
D	Denial of Service	Availability	Exhausting resources needed to provide service
E	Elevation of Privilege	Authorization	Allowing someone to do something not authorized

STRIDEPP (ICS-STRIDE)

	Threat	Property Violated	Threat Definition
S	Spoofing	Authentication	Pretending being something/someone else
T	Tampering	Integrity	Modifying something on net/disk/memory/etc
R	Repudiation	Non Repudiation	Claiming that you didn't do something or viceversa
I	Information Disclosure	Confidentiality	Access information to someone not authorized
D	Denial of Service	Availability	Exhausting resources needed to provide service
E	Elevation of Privilege	Authorization	Allowing someone to do something not authorized
P	Physical DoS	Resilience	Exhausting ICS operational controls in order to mine its reliability
P	Physical Harm	Safety	Undermining/Bypassing ICS safety controls in order to cause physical harm to assets and humans

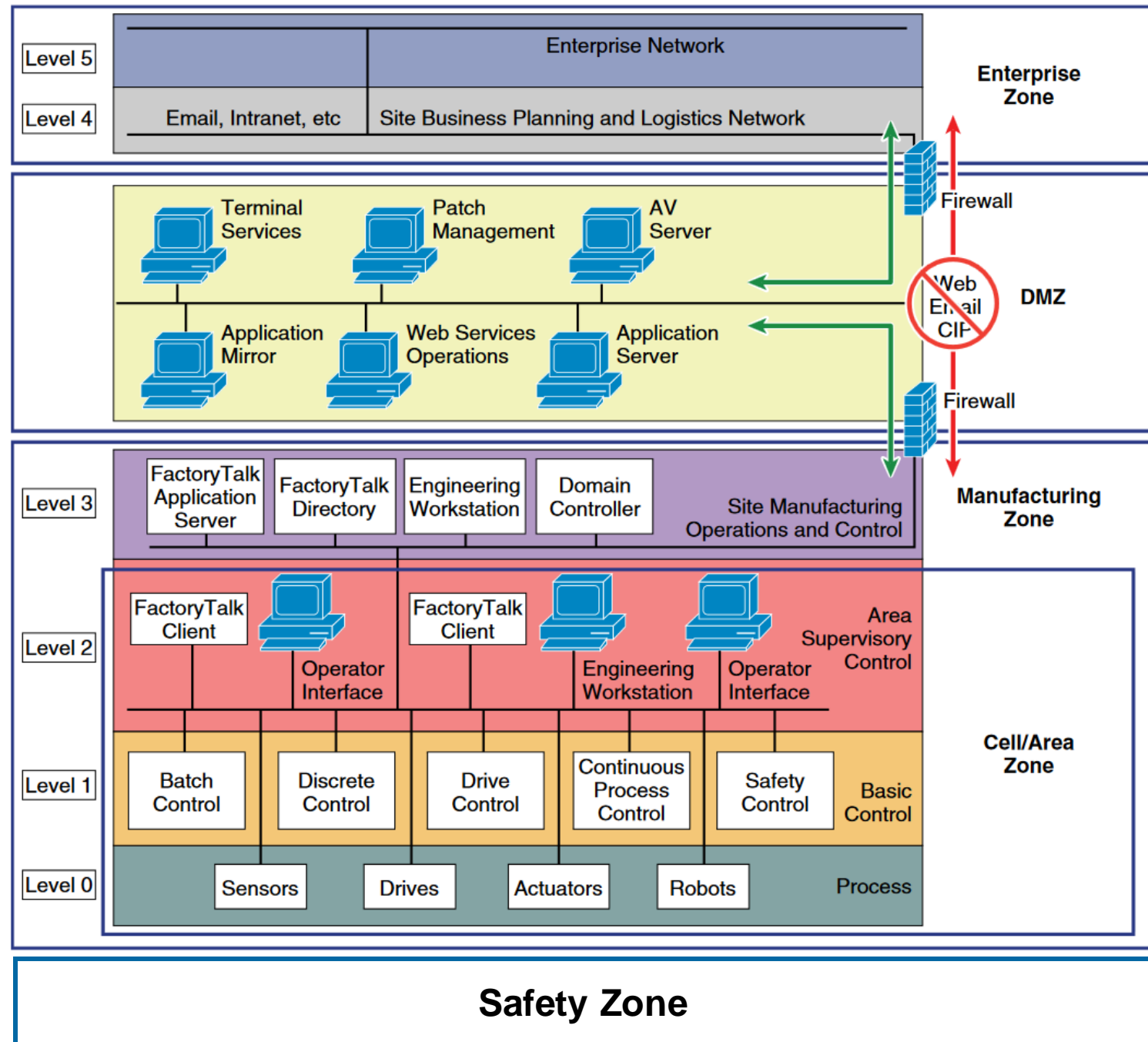
DREADE (ICS-DREAD)

- DREAD methodology is used to rate, compare and prioritize the severity of risk presented by each threat that is classified using STRIDE.

	Threat	Definition
D	Damage	How much damage will be caused?
R	Reproducibility	How easy is it to reproduce the threat exploit?
E	Exploitability	What is needed to exploit this threat?
A	Affected users	How many users will be affected?
D	Discoverability	How easy is it to discover this threat?
E	Environmental Impact	How many living casualties there will be?

Purdue Enterprise Reference Architecture

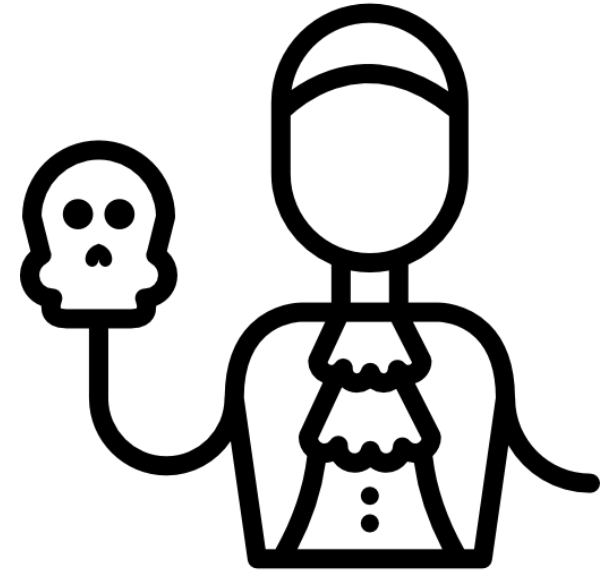
A 1990s reference model for enterprise architecture



The Hamletic Question: Threat Modeling Yes or No?

Nowadays the ICS world is split in two:

- **Companies that do Threat Modeling already**
 - Recurring Problems:
 - Lack of Adequate Tools
 - Resources Vs # of Threats detected and mitigated
- **Companies that don't do Threat Modeling**
 - Recurring Problems:
 - Lack of Resources (i.e. Time and Budget)
 - Lack of Expertise (i.e. Security Architect)



Work Instruction or Operating Procedure for Threat Modeling

██████████ · Product Security Leader

· 3 wk ago

Has anyone developed a work instruction or standard operating procedure for threat modeling of ICS/IIOT devices (or network)?

(I'm trying to do an analysis of what we can get the process architects, control engineers, or entry-level security professionals to document so that we can more efficiently use our principle ICS/IIOT security experts. This will also help us maintain a pipeline to get starting professionals trained and exposed to knowledge, skills, abilities, etc.. I will start by mapping out the workflow, so I was just curious if anyone has already done this for their org.)



Threat modelling



· Lead Automation Engineer
· 5 mths ago

Hello Everyone,

I am curious to find out if people are creating threat models for their ICS? If so what tools are you using and are you happy with the tool?

We are currently using the Microsoft tool and it really does not lend itself to modeling an ICS environment. It is fine if you are developing C++ type software but not for the type of "integration" that normally makes up an ICS.

Thanks



Question for Engineers - Visio vs. CAD

Cybersecurity Engineer & Consultant

· 9 mths ago

To engineers out there.

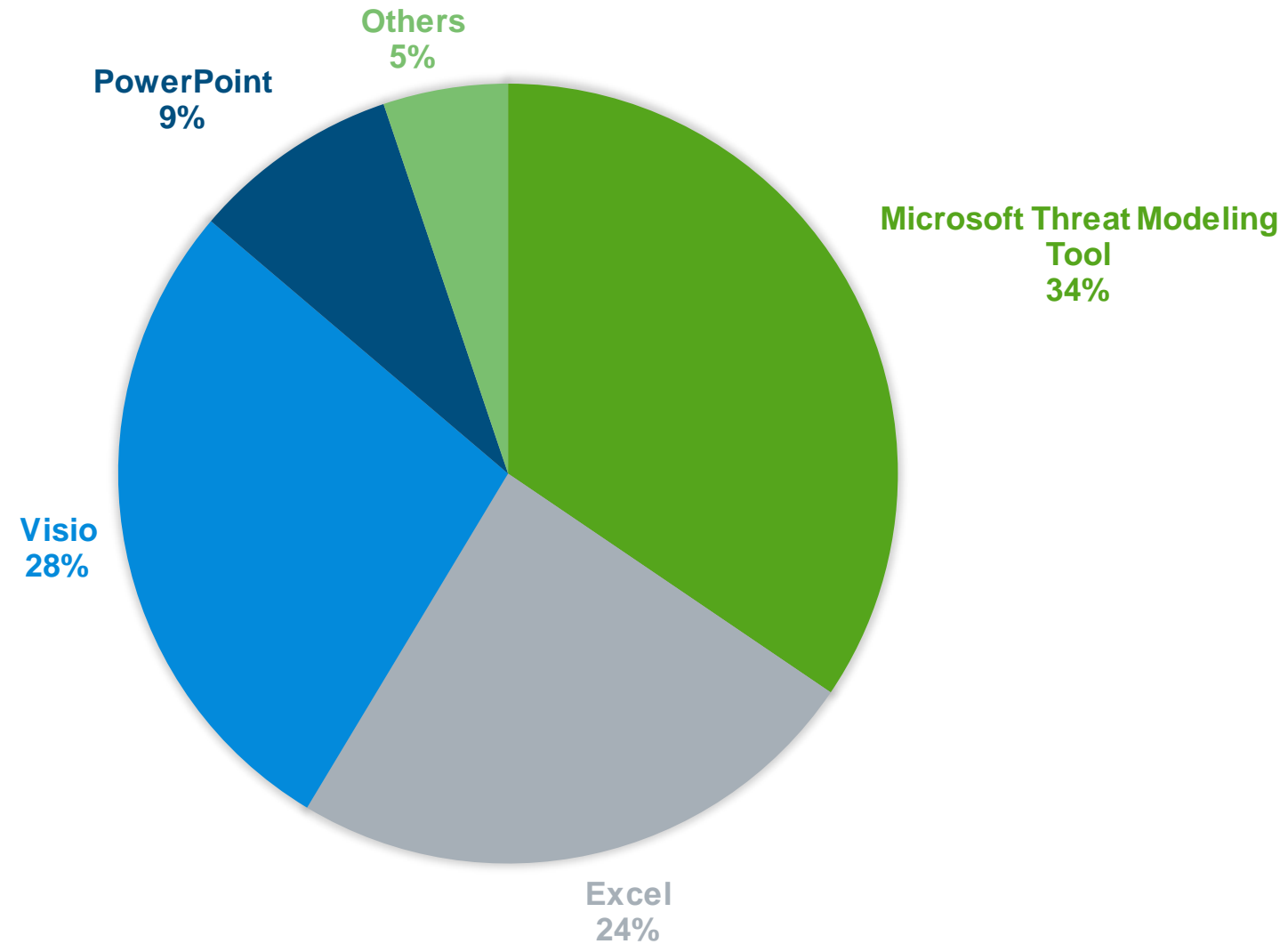
How would you want to see a Visio diagram? I have been working on a cyber security project using Visio to diagram an environment. Visio is generally fairly high level and conceptual. Some engineers on the project are wanting more detail, but I think what they want is a more physical representation of the environment. The physical layout will most likely be a handful of devices with minimal connections - everything is architected and separated by config e.g. VLANs, zones, etc.

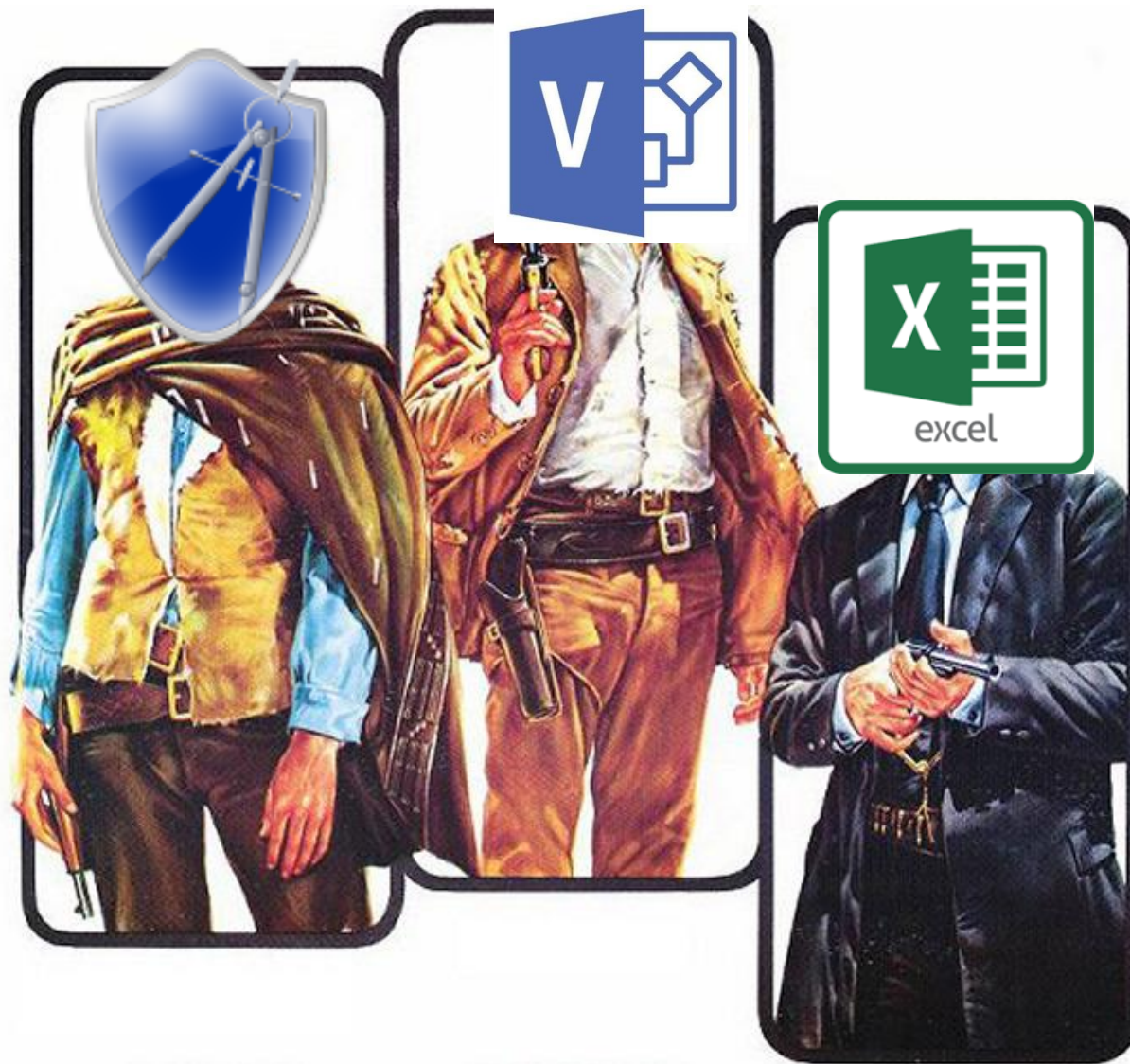
Ultimately this will probably end up as a CAD drawing (that I won't create).

How would an engineer want to see what doesn't physically exist (logical, config) in a way that makes sense?

I'm thinking of replacing Visio style icons (brick wall for a firewall) with plain boxes to make it look more like a CAD drawing.

Which tools are you using for Threat Modeling?

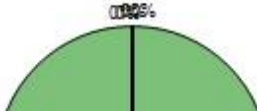




THE GOOD THE BAD AND THE UGLY

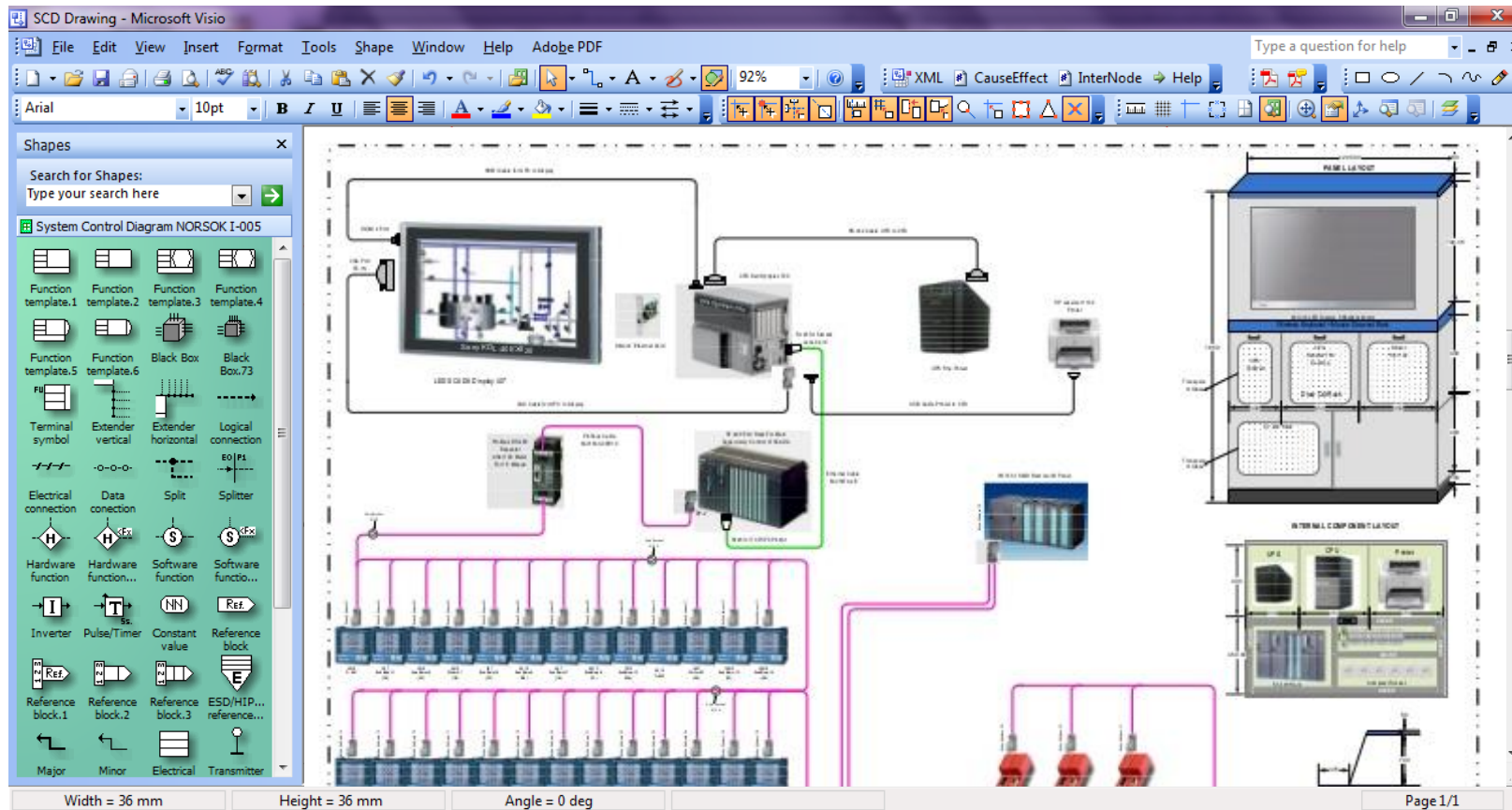


Microsoft Excel

	A	B	C	D	E	F	G	H	
1	Risk Assessment Template Excel								
2									
3	Consequences								
4			Insignificant	Minor		Moderate	Major	Catastrophic	
5	Likelihood:		1		2		3	4	5
6	A (almost certain)		H		H		E	E	E
7	B (likely)		M		H		H	E	E
8	C (possible)		L		M		H	E	E
9	D (unlikely)		L		L		M	H	E
10	E (rare)		L		L		M	H	H
11									
12									
13		Key	Description						
14		E	Extreme Risk: Immediate action required to mitigate the risk.						
15		H	High Risk: Action should be taken to compensate for the risk.						
16		M	Moderate Risk: Action should be taken to monitor the risk.						
17		L	Low Risk: Routine acceptance of the risk.						
18									
19	Risk Status								
20	<input type="checkbox"/> Open <input type="checkbox"/> Closed <input type="checkbox"/> In Progress <input type="checkbox"/> Monitoring <input type="checkbox"/> Resolved								
21	 0.00%								
22									
23									
24									



Microsoft Visio



SIEMENS

Bilddatenbank Sprache Kontakt Hilfe Site E

Home > Suche Motive

Suchtext

Artikelnummer

37-48 von 1448 Motiven Motive pro Seite 12 | 20 | 40 | 100

Allgemein - IED	Allgemein - Batterie	SIMATIC ET 200SP PS 24 V	LOGO!Power 36 mm
SIMATIC RF188C	LOGO!Power 72 mm	LOGO!Power 54 mm	LOGO!Power 18 mm
Reaktor	SIMATIC RTLS4083T	SIMATIC RTLS4030T	SIMATIC RTLS4030A



Microsoft Threat Modeling Tool

The screenshot displays the Microsoft Threat Modeling Tool 2014 interface. The main workspace shows a diagram with a 'Browser Client' connected to a 'Web Server' via an 'HTTP' connection. The 'Web Server' and 'Web Application' are connected via an 'RPC/DCOM' connection. Trust boundaries are indicated: a 'Machine Trust Boundary' separates the Browser Client from the Web Server, and a 'Generic Trust Boundary' separates the Web Server from the Web Application.

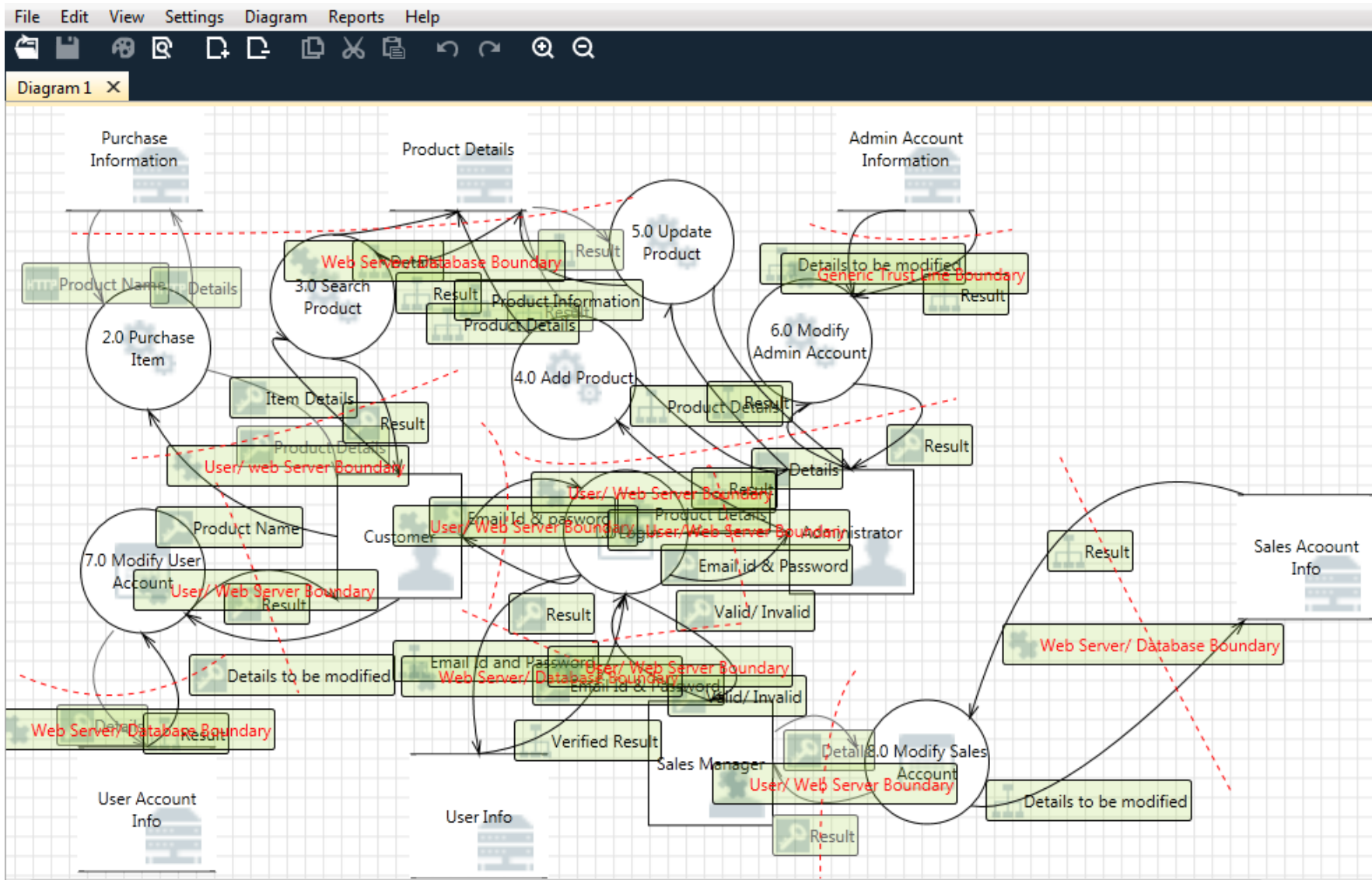
The Threat List Filter panel on the right shows the following settings:

- By Threat State: Threat States (22)
- Not Started (21)
- Mitigated (0)
- Not Applicable (1)
- Needs Investigation (0)

The Threat Information panel at the bottom shows a list of 22 threats. The following table represents the visible threats:

Threat	Category	State	Severity
Potential Lack of Input Validation for Web Server	Tampering	Not Started	High
Spoofing the Web Application External Entity	Spoofing	Not Started	High
Spoofing the Web Server Process	Spoofing	Not Started	High
Spoofing the Browser Client Process	Spoofing	Not Started	High
Potential Lack of Input Validation for Browser Client	Tampering	Not Started	High
Web Server Process Memory Tampered	Tampering	Not Started	High
Potential Data Repudiation by Browser Client	Repudiation	N/A Not Applicable	High
This threat requires justification explaining why it does not apply.			
Data Flow Sniffing	Information Disclosure	Not Started	High

It may become messy in ICS



- **What Can Do:**

- **Good for Risk Assessment**

- Allows evaluating a control system network as part of a comprehensive cybersecurity assessment
- Specify cybersecurity recommendations
- Report using standards-based information analysis
- Provide a baseline cybersecurity posture

- **What CANNOT Do:**

- **Bad for Threat Modeling**

- Validate accuracy of user inputs or Identify Threats from a STRIDE POV
- Ensure implementation of cybersecurity enhancements or mitigation techniques
- Identify all known cybersecurity vulnerabilities
- Re-Use Existing 3D models of the ICS Plant in scope

ICS Threat Modeling Nowadays

- **Not yet Fully Implemented**
- **A lot of uncertainties on:**
 - **How to do it Systematically**
 - **How to Scale it**
 - **Which Tool to use**
 - Excel spreadsheets and Risk Matrixes
 - Microsoft Threat Modeling tool
- **Extremely Time Consuming** (due the reasons above)
- **Need for a Better Approach**
 - **Ad-Hoc Tools**
 - **Continuous Threat Modeling & Dedicated Methodology for ICS**
 - **CATHAMA**

STRIDEPP + DREADE + PERA/CPwE = CATHAMA



Continuous Advanced Threat Hunting And Modeling Activity

CATHAMA



- Based on Assets Levels (0 to 5) Division from Purdue Model (PERA)
- Continuous Effort in Hunting, Analyzing, Evaluating and Prioritizing Threats
- Risk Rating It is supported by Intel Feeds, Existing Vulnerabilities of each Asset (e.g. CVEs) and Automated Scanners reports
- Able to Simulate Existing Threats and What happens to the plant in case of a patch/hotfix is going to be applied.
 - E.g. Device A.1.2.3 has new 1-day RCE. It is used in different parts of the plant. One more critical than other places. We need to simulate what happens when patch is applied. SLA uptime is impacted? Is it safe to patch now?



Your Success Stories or Opinions Are Valuable!

<https://www.surveymonkey.com/r/55FDWT6>

Wanna Hear More About
Threat Modeling in
ICS?



@lucabongiorni

Resources

- Usual standards related to Risk Assessment mostly: NIST 800-82, NERC-CIP, IEC 6244.
- The problem I see in ICS, related to Threat modeling, is the lack of proper tools and a specific resources exclusively related to Threat Modeling (and not Risk Assessment).
- Said that I really love the two following books:
 - **Threat Modeling: Designing for Security, Adam Shostack, 2014**
 - **Hacking Industrial Control Systems, Clint Bodungen , 2017**