COMBATREADYIT.COM

FRISKSI - FOOD RISK AND SECURITY INTEGRITY

Presented by:
Paul B Dove MVP

- **PURPOSE**
  - COMBATREADYIT.COM - PROTECTION AND SECURITY SOLUTIONS
    - Our Focus is on Dominions
    - SMBs within Dominions
    - Team Members Organisation within SMBs
    - Broadsourcing and Application Development
    - Security Audits and Security Support
  - OUR MISSION IS TO HELP SUBSCRIBERS AND SMBs SECURE THEIR INFORMATION
  - WE ARE A TRANSFORMATION ADVISORY HELPING SMBs REALISE QUANTIFIABLE COST SAVINGS BEYOND CLOUD
  - OUR PASSION IS PERPETUAL IMPROVEMENT EVERYWHERE

- **PRODUCTS**
  - SHAZOPS
  - VIA FERRATA RISK ASSESSMENTS
  - FRISKSI
  - PROJECT MANAGEMENT
    - ITIL
    - IT STRATEGY
    - SECURITY STRATEGY
    - ORGANISATION STRATEGY
  - DISCIPLINED AGILE DEVELOPMENT
  - RUGGED SECURE APPLICATIONS
  - DEVOPS and SecOPS

- **PEOPLE**
  - BOUTIQUE CONSULTING PRACTICE
  - CONSULTANT HAVE A MINIMUM OF 20 YEARS EXPERIENCE
  - 1400 YEARS OF EXPERTISE ACROSS 62 TEAM MEMBERS
  - SECURE RUGGED DEVELOPMENT AND PROJECT MANAGEMENT
  - 3 DECADES IN IT & OPS SECURITY
  - PROJECTS DELIVERED IN 44 COUNTRIES
  - DEVELOPED PERPETUALLY IMPROVE EVERYTHING

COMBATREADYIT™

COMPANY PROFILE

- **Established 2009 as part of HazardologyLtd based in Vancouver**
- **Focus on CyberSecurity**
- **Our market sector is IT Security, Secure Products and Advisory, Cloud Transitions, Project Managment, Team Member Broadsourcing, Organisation Alignment, Mobile App and DataCentre design**
- **Target Markets are Internet connected Pioneers and SMBs**
- **We are represented in Switzerland, Canada, UK, and USA**

BLACK MINUTE

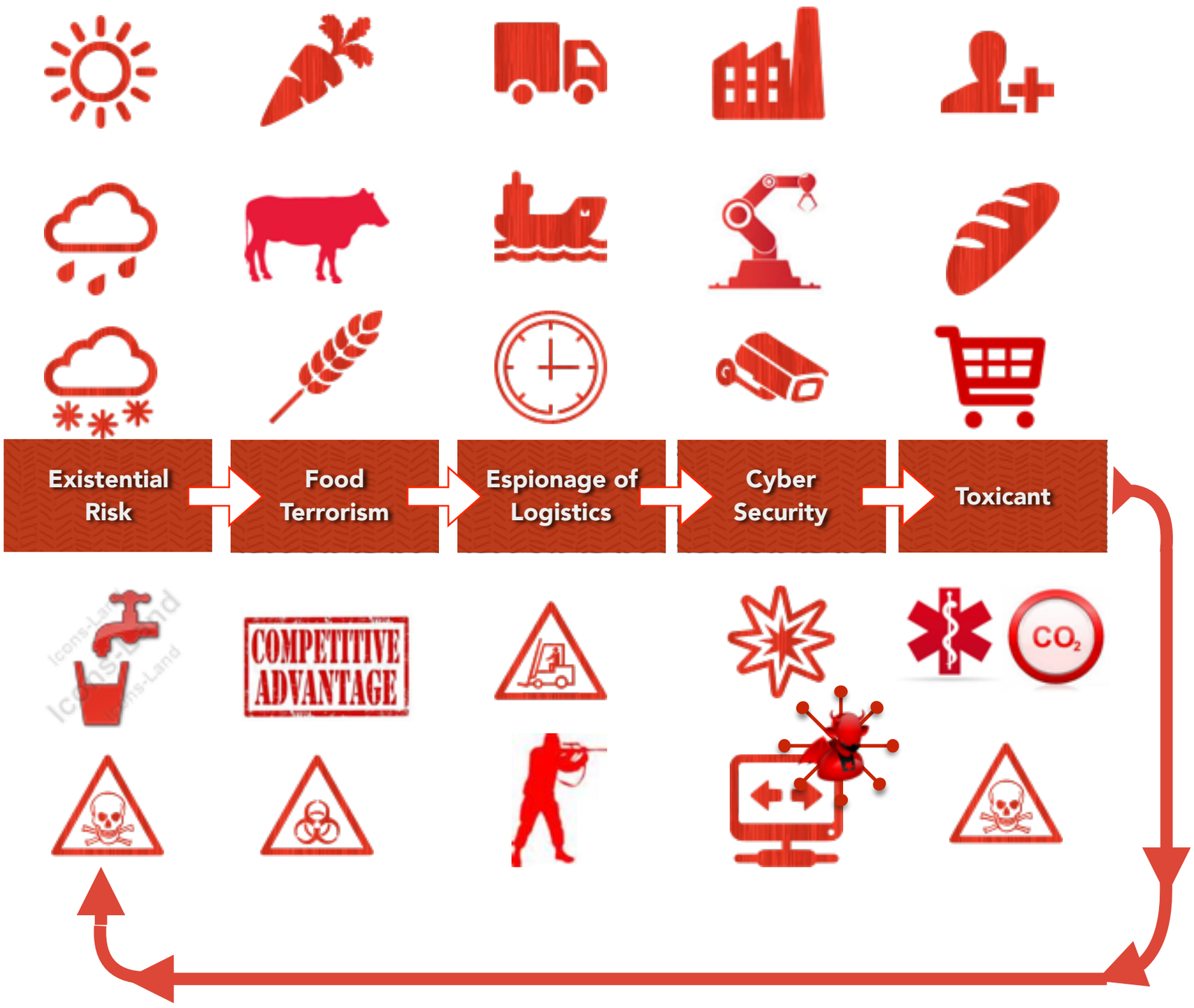
The average cost to a company for a One minute Data Breach is $3 MILLION

- The Black Minute is all an adversary needs to inflict espionage or wipe PLC data or manipulate an entire Process facility to cause damage (or death)
- An estimated 1,250,000 hackers now hack 50,000 websites and installations a day

THE BLACK MINUTE

- Food processing and production data breaches can have major impacts on reputation
- Adversaries and Competitors can manpulate data even at Analytical Data Laboratories which can lead to major recalls of food brands in a country or even globally
- The Food sector is now a leading target for Cyber attacks

E.F.E.C.T.



FOOD RISK & SECURITY INTEGRITY

- FRISKSI - End to End Integrity of the Food Supply Chain
- E.F.E.C.T. LOOP -
  - EXISTENTIAL RISK - manipulation of natural resources
  - FOOD AND BIO TERRORISM - Conflict and Competition
  - ESPIONAGE - Storage of food as target -Conflict impacts
  - CYBER SECURITY - Malware attacks on SCADA and ICS - Explosions/Leaks of hazardous material
  - TOXICANT - Consumption Safety at POS and waste

FRISKSI

COMBAT READY IT™

The Food industry is under attack as part of a hacking campaign by Cyber and Food Terrorists

- Food Processing facilities now account for 24% of known cyber attacks in the first half of 2015
- Dell reported 647,000 attacks globally on the Food sector in 2014
- 1000 directed SCADA attacks on Process facilities in Europe in first quarter 2015
- 67% of Process facilities do not know that they may already be infected
- Over 50% of attacks are initiated internally by Insiders
- Cyber Security tools and practices are brittle
- In the UK alone this costs the food industry £8 BILLION in ANNUAL lost revenue and added IT expenditure
- Global Food Sector losses are estimated at $189 BILLION

FOOD RISK & SECURITY INTEGRITY

- One gram of botoxin (the organism that causes botulism) can kill hundreds of thousands
- 2 Million people die from food related illness
- 1.3 BILLION tons of food wasted

MOTIVATION

8 Billion earth citizens need feeding - The planet cannot sustain the increasing nutritional demand

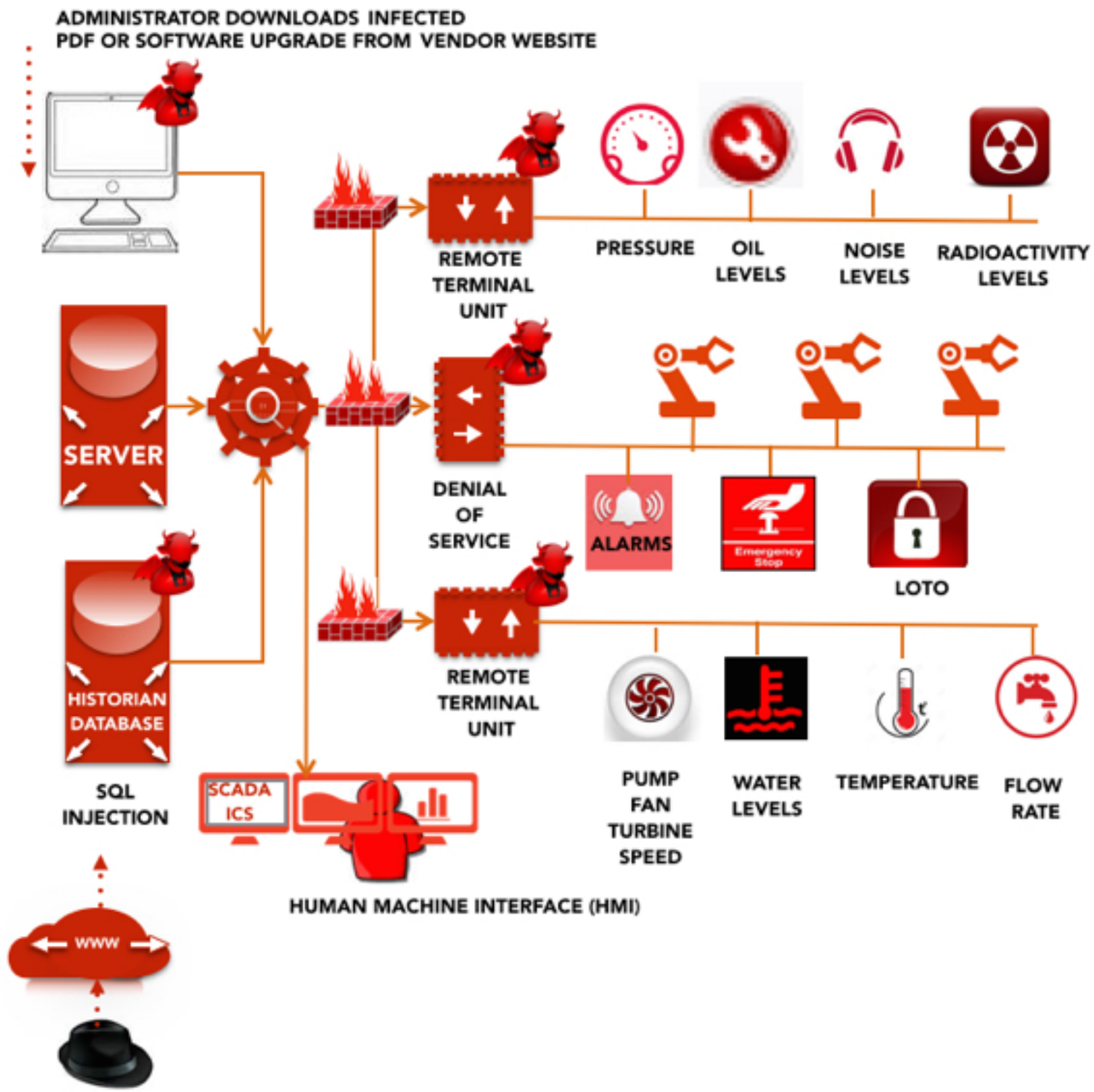
- Food Terrorists seek to disrupt dominons by destroying crops and water supplies and processing in localised conflicts
- 250,000 hackers globally will attempt to infiltrate manufacturers Enterprise and Plant networks JBIT*
- Water supplies are affected by drought or flood
- Essential minerals required to maintain health are being depleted and this increases disease
- The weather is now a deep concern for governments as the costs to maintain sustenance in disaster areas is high
- Food supply needs to increase 70% by 2050
- Patents for gastronomic recipes, synthetic foods (sugar replacements), syrups, molecular level food manipulation and genomics (biotechnology) are goldust to adversaries

FOOD RISK & SECURITY INTEGRITY

- Agroterrorism
- Subversion of Level 2 and Level 3 Supply Chain
- Audit controls on contract suppliers
- Quality and Security assessments on primary growers and providers
- Traceability
- *Just Because Its There

SCADA/ICS

Traditional Process IT Architecture



FOOD RISK & SECURITY INTEGRITY

- Overlap of ISA84 (process safety) and ISA/IEC-62443 (cyber security)
- The safety integrity level (SIL) concept is well established and described in the ISA84 and IEC 61511 standards
- Do they work?
  - Direct Attacks
  - Denial of Control
  - Denial of Service
  - Divergent
  - Dissonant (Insider)

ROASTS

Really Old Antiquated Software Thats Slow

- Most ICS Software has more holes than a Swiss Cheese (Stands to (James) Reason))
- Designed for low latency speeds they let Hackers through Firewalls or Switches and can easily intercepted and reverse engineered….
    - MODBUS
    - PROFITNET (No Authentication, Not encrypted)
    - SIEMENS S7
    - IEC 61850-8-1
    - IEC 404
- Most installations can be compromised in under an hour

FOOD RISK & SECURITY INTEGRITY

- Attackers have access to malware that circumvents old programming language and topologies
- These attacks are well docmented and available freely on the web

ATTACK TYPES

Current thinking and existing IT architectures, Cyber Controls and Protocols cannot handle sophisticated attacks

- Hackers can easily access Process Facilities PLCs
  - STUXNET, FLAME, HAVEX , DUQU, SHAMOON
- PLC Vendors websites and software upgrades are already hacked
- Once a PLC is corrupted a hacker can control energy plants, additive controls, water treatment
- Most PLCs are custom programmed leaving the Operating System open to Insider
- A PLC attracts significant reprogramming costs (7 figures)
- Most Process facilities are connected to the Enterprise networks…everyone uses IP to connect
- Vendors, support and maintenance engineers and operators connect remotely using IP

FOOD RISK & SECURITY INTEGRITY

- Attackers can crack a password in 15 seconds
- An adversary can take over a WiFi network in 30 seconds
- A firewall can be circumvented in under a minute
- A SCADA Command and Control system can be hacked and have malware that hides from normal scanning software
- Traditional Operating Systems have vulnerabilities that have been around for 20 years
- MALWARE SCRABBLE
  - STUXNET - IRAN Centrifuges
  - FLAME- 20 times more powerful than STUXNET
  - SHAMOON- Aramco 30,000 PCs
  - HAVEX-Energy Sector -Remote Access Trojan (RAT)-SInce 2011
  - DUQU-ICS Data collection

ATTACK TIMELINE

Actions that can make a Boiler or Ammonia Plant explode

- Administrator downloads compromised software upgrade from vendors website
- Insider who becomes influenced under the FREXAGON pressures
- Insider can manipulate ICS to misbehave
- Insider has high level of Access and privilege
- Insider creates and sells Admin Accounts (after being bribed or being let go) these accounts are sold on the Hackers sites
- Infiltrate
- Adversary buys Admin credentials
  - Accesses network via VPN
  - Accesses Citrix and Microsoft Terminal Server
- Adversary attempts IP Network attacks, bypass firewalls
- Adversary collects Human Machine Interface
- Accesses PCs and Servers and drops cloaked malware on multiple devices
- Adversary creates additional accounts on TRUs and Wifi and drop off point for data with FTP access. Access Histroy deleted
- Exfiltrate
- Attack Phase
- Mimics Command and Control operator (HMI) using Man in The Middle
- Can use SQL INjection to steal data
- Launch

FOOD RISK & SECURITY INTEGRITY

- Attacks are simple and can be carried out by trainee adversaries

ROOT CAUSES

Use of the Internet Protocol throughout a facility is an open book to an adversary

- The Internet is a 30 year old car designed by motorbike fanatics in the 80's
- Internet Designers scoff at the mere suggestion that IP ubiquity has led to the massive rise in Cyber Security attacks
- Blame and responsibility is aimed at Enterprise IT teams (Its not their Fault)
- Regulatory bodies recommendations are to implement Firewalls and Micro Segment the network…this induces severe latency and impacts on Machine Safety and Capabilities
- Anti-Virus software is only 60% effective by the vendors own admission (can your company handle 1,000,000 new viruses per week?
- Company engineers download unauthorised software from the Internet
- Programmers copy previously corrupted code into new environments
- Penetration and Vulnerability tests and practices are outdated

FOOD RISK & SECURITY INTEGRITY

- Malware can spread through an organisation through the IP Protocol
- The Internet of Things uses IP
- IOT is the biggest growth market in the Food Industry
- This all makes perfect sense right?

REMEDIALS

By the book - the usual approach. Most common controls recommended by most all regulators

- Identifying and categorizing assets,
- Establishing a plan to eliminate significant vulnerabilities,
- Developing systems to identify and prevent potential attacks,
- Identifying, containing, and fighting back against known attacks,
- Applying and maintaining the latest operating system and application patches,
- Using current antivirus definitions,
- Updating authorized application software,
- Enabling network antivirus software,
- Not using a USB stick unless it's been scanned and malware free
- Hardening servers and workstations,
- Changing default admin passwords,
- Controlling user rights,
- Implementing backup and restoration,
- Taking inventory of network assets,
- Using physical network isolation when possible,
- Using logical network segmentation (secure zones) with strict firewall rules,
- Enabling firewall logging,
- Using Network Management Systems, SIAM, Omniocular Automism
- Creating an incident response plan before an incident occurs.

FOOD RISK & SECURITY INTEGRITY

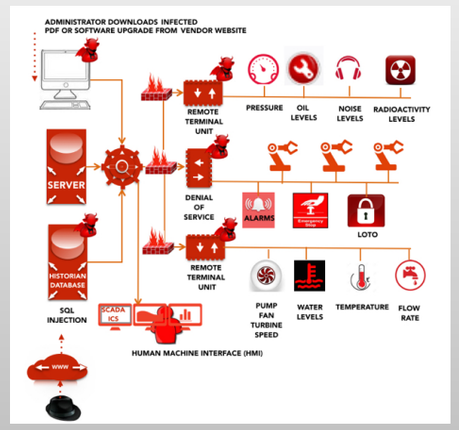
- If you are not doing this now at each facility you are in trouble
- BUT …Paper regulations do not stop hackers
- Look at mircosegmentation and localising the Data Centre
- Use DEVOPS and SecOPs to ensure stability of configurations
- SHAZOPS the code
- Combat Ready Rugged Coding
- Disciplined Agile Development

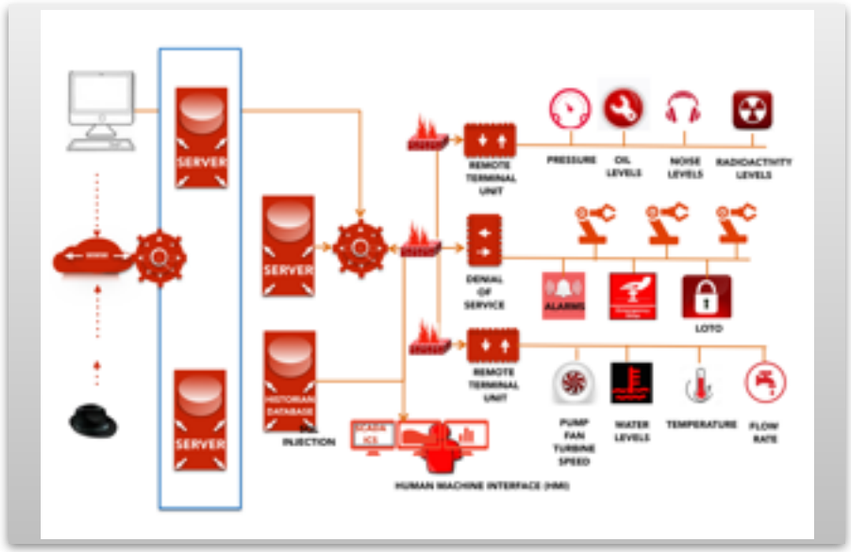
THINK DIFFERENT

IP OPENESS AND UBIQUITY = BAD
LEGACY AND PROPRIETARY = JOB SAVER

FOOD RISK & SECURITY INTEGRITY

- Quick Win: IP (numeric access is an open door to hackers) - Isolate the Process facility from the Internet
- Introduce different device access options for:
  - Localised Authentication
    - Install a Security Bubble (an IP Blanket)
    - IOT Devices Authenticated locally
    - Remove RAT and Network Management SNMP
    - Deploy ENUM
    - Move to Named (an Alpha named schema) - Data Link Switching
  - Remote Access via Browns Boxes (yes… secure modems)





ALL SORTS OF THINGS

IOT Futures

FOOD RISK & SECURITY INTEGRITY

- Traceability and Transparency
- Consumers want to know where their food comes from
  - In the new world…
    - Shoppers pick up milk from local supermarket
    - Milk carton has Smart Packaging and QR code
    - Using a smartphone the shoppers can scan the QR
      - The QR Code reveals:
      - Where the milk came from
      - When the cow was last inspected
      - When it was milked
      - How long it took to package
      - How long it took to reach the store

DISCLAIMER STUFF

This communication may contain confidential and/or privileged copyright information belonging to CombatReadyIT™, CRITTERS, or PIE.Institute. This information is intended only for the use of the individual or entity named. If you are not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you should return to sender immediately. You are notified that any disclosure. copying, distribution or the taking of any action in reliance on the contents of this communication is strictly prohibited. This document was created by CombatReadyIT™, limiting to zero liability. The analysis is the result of our exercise of our best professional judgement based in part upon materials and information supplied to us by techanets'™ partners and others. Use of this document by any third party for whatever purpose should not, and does not, absolve a third party from using due diligence in verifying the document's contents. This document is also subject to the Mutual NDA and copyrights associated. Any use which a third party makes of this document, or any reliance on it, or decisions to be made based on it, are the responsibility of such a third party. CombatReadyIT™ accepts no duty of care or liability of any kind whatsoever to any such third party, and no responsibility for damages, if any, suffered by any third party as a result of decisions made, or not made, or actions taken, or not taken, based on this document. *CombatReadyIT.com is a new company, project experience illustrated in this document may refer to work carried out by our consultants and associates and is illustrative of skills and knowledge depth