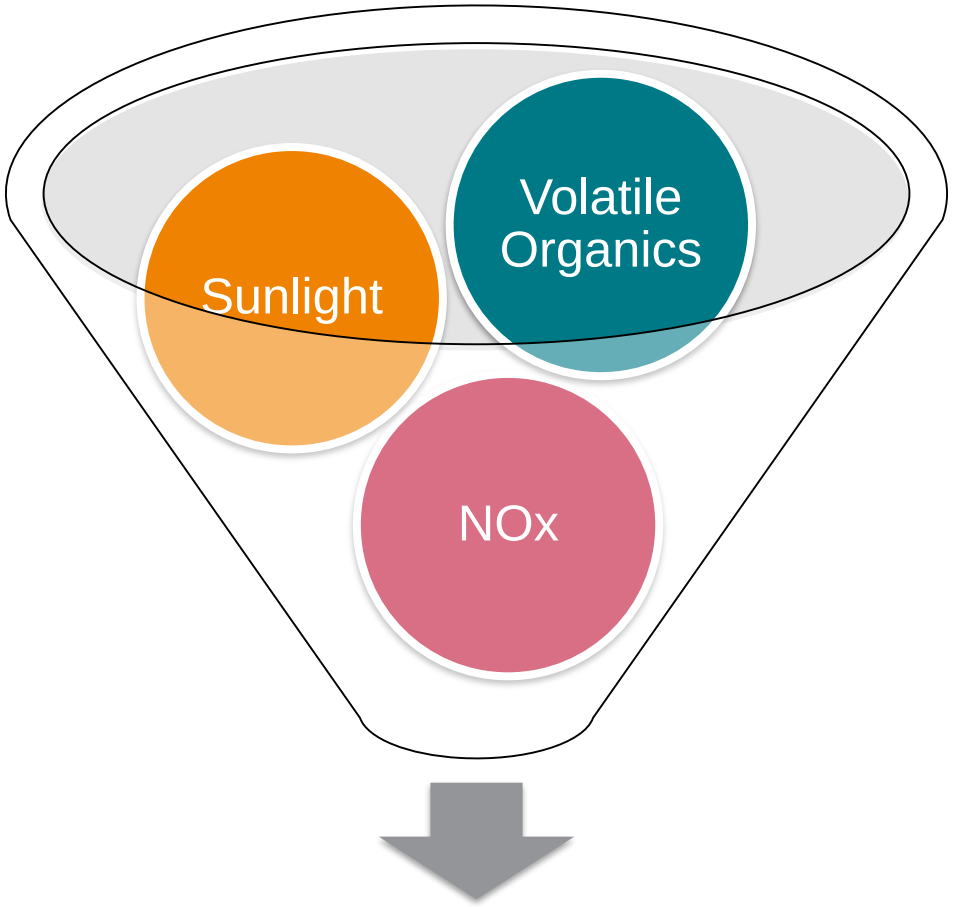
Vision for the Burner Industry
25 Years from Now

June 5, 2018

Travis F. Hardin
HVACR & Controls Principal Engineer Manager

Market Drivers

Why is NOx an Issue?



Ground Level Ozone (O_3)

US EPA Ozone Designation & Classifications (2008 Standard)

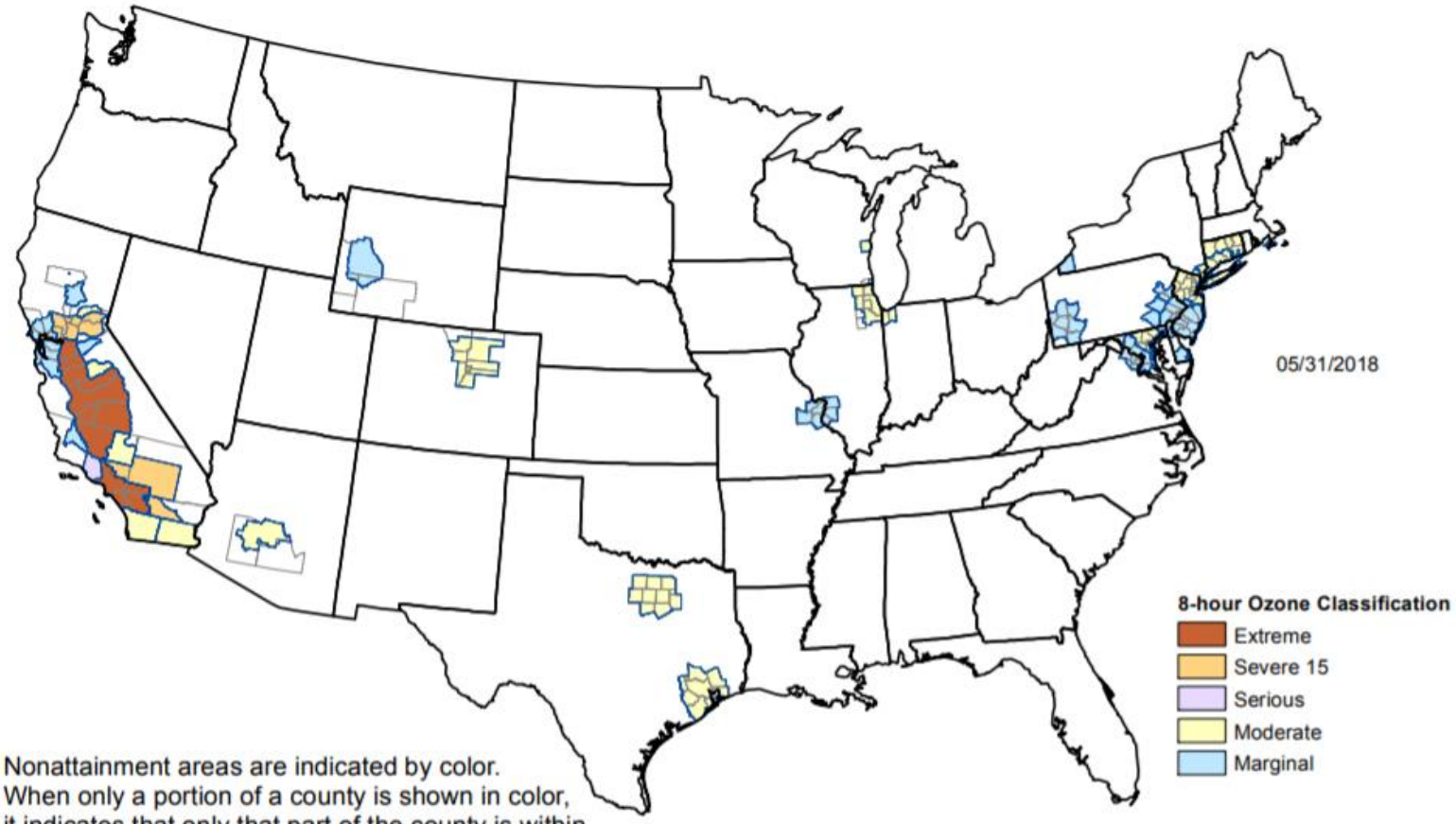
Designations – National Ambient Air Quality Standards

- Nonattainment
- Attainment

8 hour Ozone Classifications

- Extreme (0.175 ppm and above)
- Severe 17
- Severe 15
- Serious
- Moderate
- Marginal (begins at 0.076 ppm)

USA Regulations and Current Conditions



For the Ozone-8Hr (2008) St. Louis-St. Charles-Farmington, MO-IL nonattainment area,
the Illinois portion was redesignated on March 1, 2018.
The Missouri portion has not been redesignated.
The entire area is not considered in maintenance until all states in a multi-state area are redesignated.

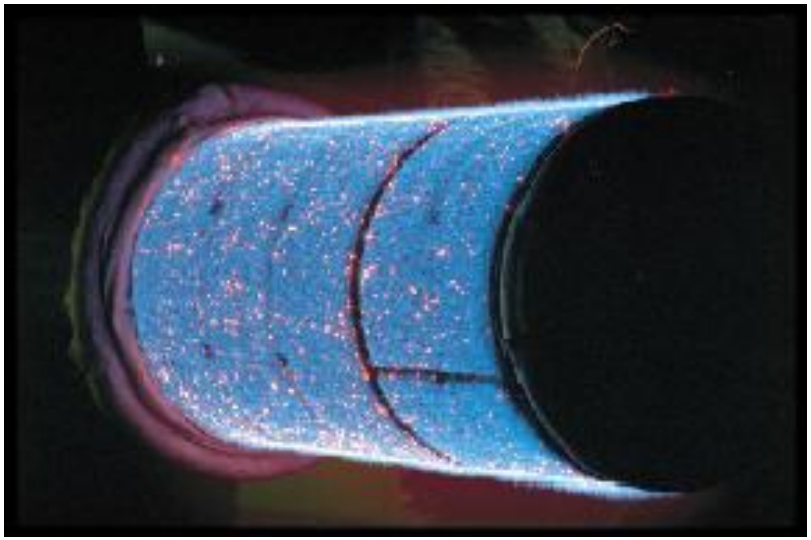
Efficiency

- USA DOE
  - Commercial Boilers

- NRCan
  - Amendment 15

Current Burner Technology

- Surface Combustion
  - Pre-mix
  - Ceramic Fiber
  - Increased maintenance
  - 6ppm
  - 1500 hp firetube



Lower Flame Temperature

Larger Heating/Burning Surface

Current Burner Technology

- Staged Combustion
  - Staged injection of air
  - Low O_2 in primary combustion zone
  - Lower flame temps in secondary combustion zone
  - Flame impingement
  - Larger footprint
  - Can be difficult to retrofit

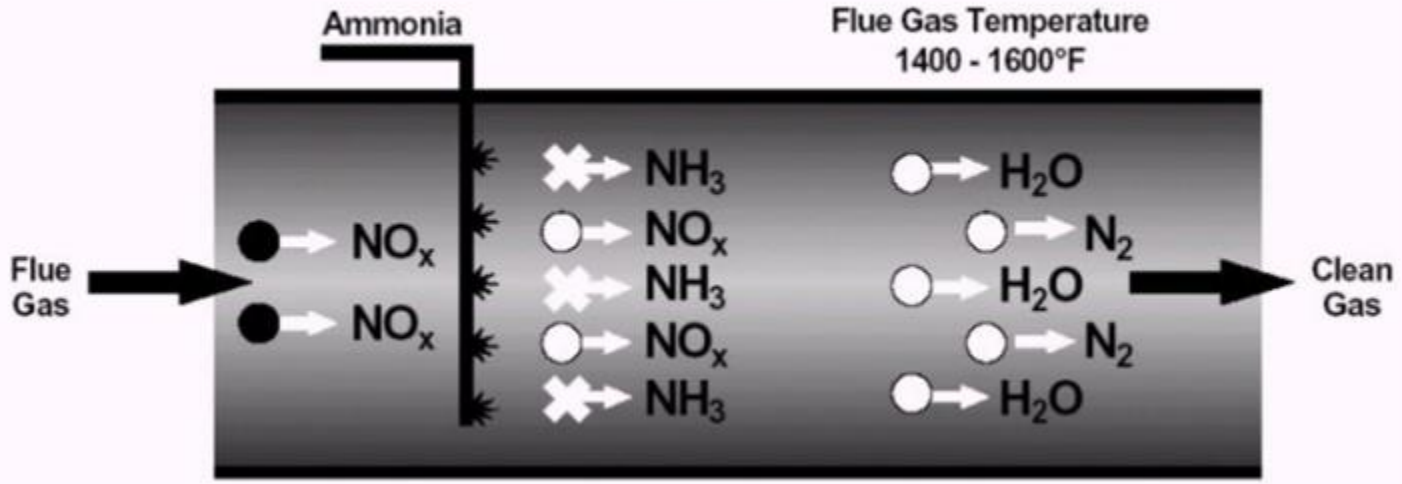
Design and Development

- Hot Water
  - Surface Combustion (premix) burners within condensing boilers
    - Continue to improve technologies/costs/etc.
- Steam
  - Surface Combustion (premix) burners
    - Improving mixing technology while maintaining safety/performance
  - Utilize gun-style burner designs
    - Low excess air & higher flame temperatures for better efficiency
    - Treating NOx after the combustion process

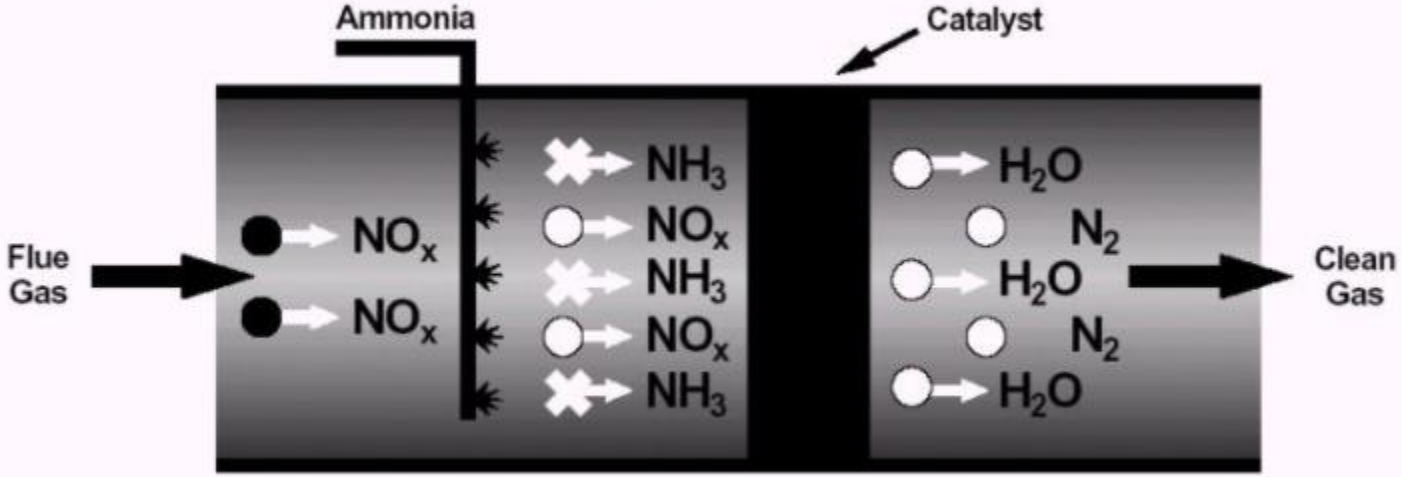
Design and Development

- After combustion processing
  - SNCR “Selective Non-Catalytic Reduction”
    - Operates in range of 1400˚ to 1600˚F flue
  - SCR “Selective Catalytic Reduction”
    - Operates in range of 600˚ to 800˚ F flue
  - Ammonia injection (reagent)
  - Urea injection (reagent)
    - Positives: Non-hazardous, non-volatile, non-explosive, non-flammable
    - Negatives: Less efficient than ammonia; Cold climate issues

Selective Non-Catalytic Reduction (SNCR)



Selective Catalytic Reduction (SCR)



Design and Development

- New Technologies & Designs in NOx control
  - Ceramic filters & SCR combination
  - Ease of retrofit
  - Lower costs
  - Etc.

Connectivity/IOT

IOT / Connected Technology

System Performance

Is it easy to set-up and use?

Do I perform as well as I say I do?

Interoperability (includes Connectivity)

Do I work with other devices?

Cyber Security & Privacy

Can I be hacked and is my data secure?

Functional Safety

Are my safety systems reliable?

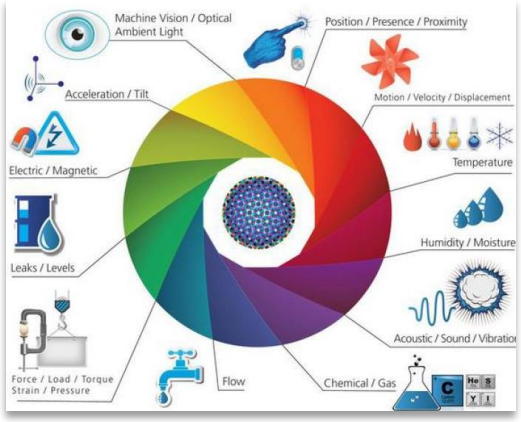
System Reliability

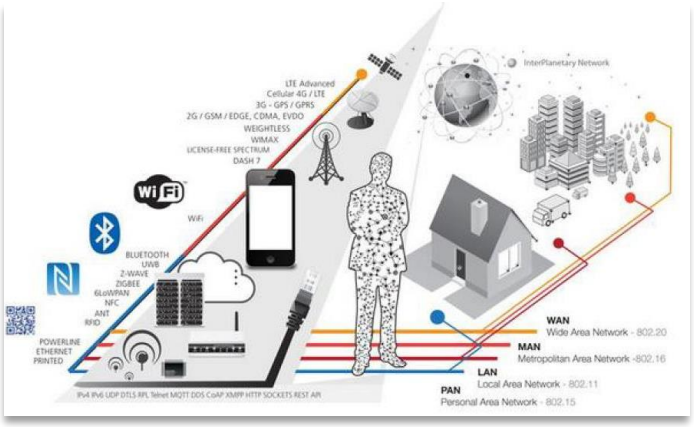
Can I rely on the system functioning?

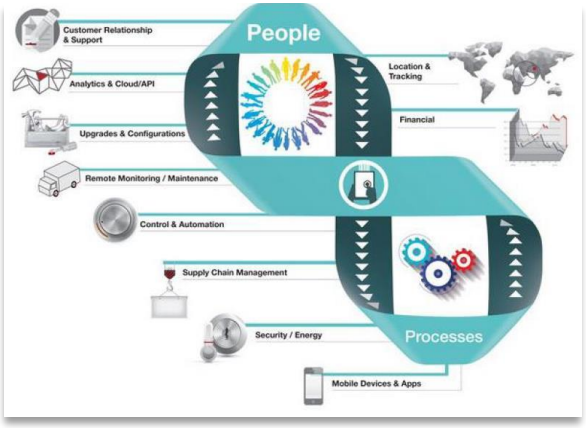
Software Upgrade Support

Connected technologies explained

Smart system and IoT are driven by:







Components
(sensors, controller, attuators..)

Connectivity

People & process

THE INTERACTION BETWEEN THESE ENTITIES
ARE CREATING NEW TYPES OF SMART APPLICATIONS AND SERVICES

SMART THERMOSTATS

nest

Save resources and money on your heating bills by adapting to your usage patterns and turning the temperature down when you're away from home.

CONNECTED CARS

CAR 2GO

Tracked and rented using a smartphone. Car2Go also handles billing, parking and insurance automatically.

ACTIVITY TRACKERS

BASIS

Continuously capture heart rate patterns, activity levels, calorie expenditure and skin temperature on your wrist 24/7.

SMART OUTLETS

belkin

Remotely turn any device or appliance on or off. Track a device's energy usage and receive personalized notifications from your smartphone.

PARKING SENSORS

STREETLINE

Using embedded street sensors, users can identify real-time availability of parking spaces on their phone. City officials can manage and price their resources based on actual use.

Network Connectable Products and Systems

Industrial

PLC and Factory Automation

Smart Meters

Automotive

IoT

Commercial

HVAC

Building Automation & Security

Fire Systems

Appliances

Consumer

Lighting

Smart Home

IoT

Medical Devices

How an Attack Works

The Attacker:

Nation States

Professional Activity

Hobbyists

Insiders/Employees

The Asset to be Appropriated:

Access Control

Lighting Gateway

Building Lighting

A Flaw:

Poorly Written Code

Improper Installation

Hard Coded Passwords

Inadequate Security Attributes

Common Attack Mechanisms

01 MALWARE
- Viruses, Trojans, and Worms
- Botnets
- Ransomware

02 ADVANCED PERSISTENT THREATS
- Requires Resources
- Specific Target

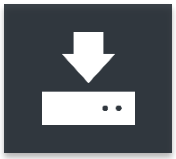
03 DENIAL OF SERVICE (DoS)
- Overwhelm System
- Degrade Performance

04 COMMON
- Phishing
- Brute Force
- Back Door

Data Breaches

Data Breaches 66%

International Data Corporation (IDC) Research shows that 66% of networks will be breached by 2018



Unplanned Downtime

Loss of Production

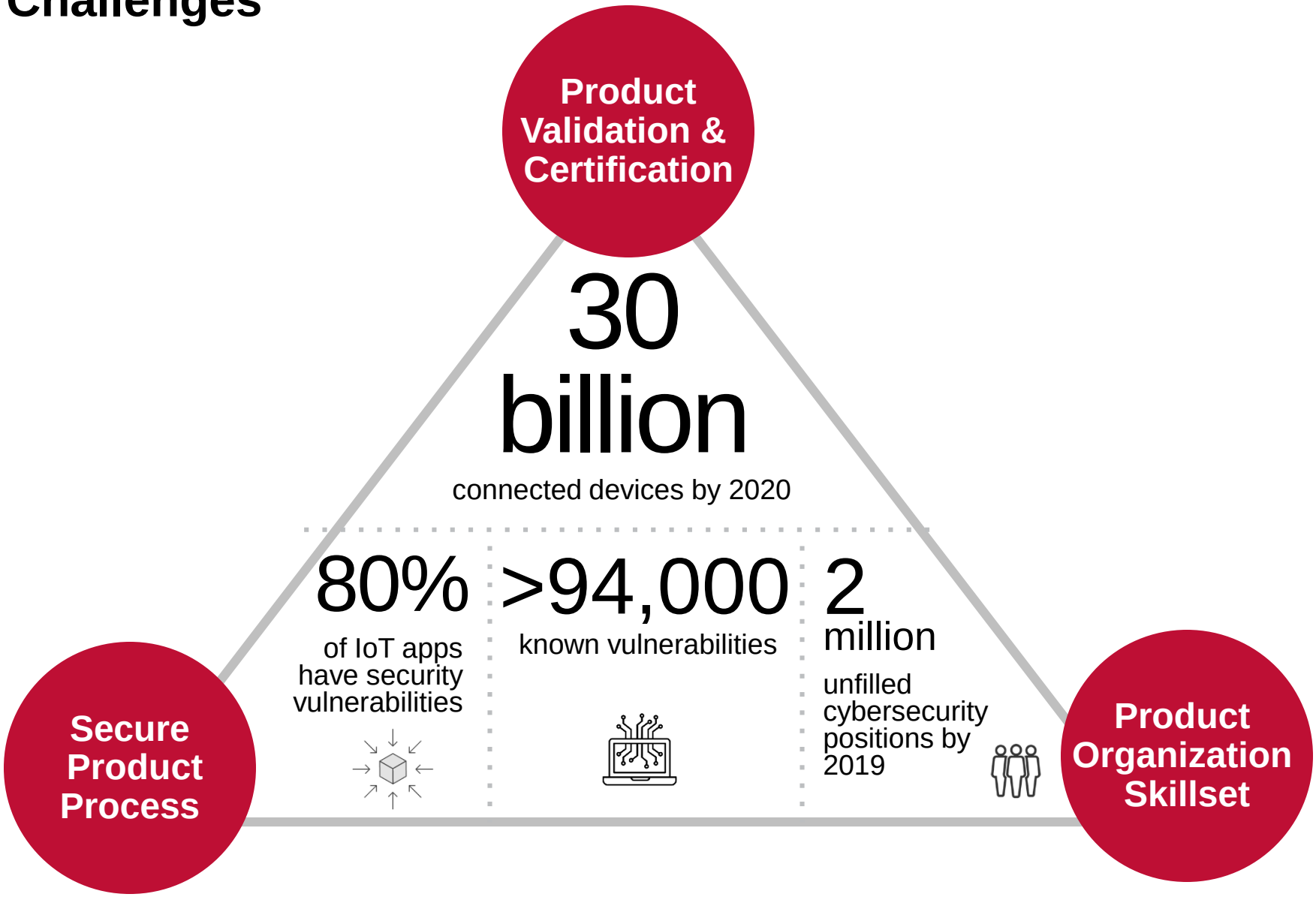
Harm to Assets

Damage to Reputation

Guidance Documents

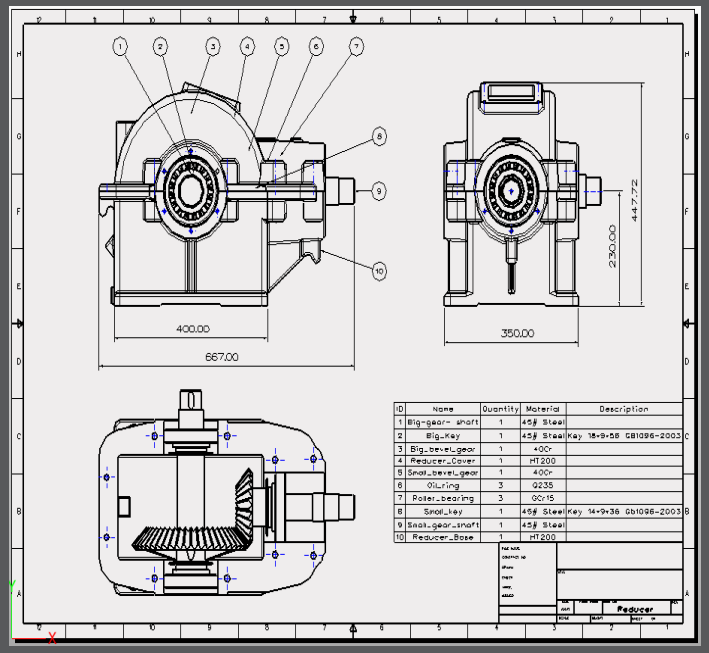
- ISO/IEC TR 15443
- ITU-T CYBEX 1500 series
  - CVE / NVD
  - CWE (CWRAF/CWSS, SANS CWE Top 25 / OWASP Top 10) and CAPEC
- ISO/IEC 27000 series
- ISO/IEC 15408
- ISO/IEC DIS 20243 /O-TTPS
- FISMA
- HIPAA
- IEC 62443
- IEC 80001
- PCI
- SANS 20 CSC
- Cyber Essentials (UK)
- Top 35 mitigation strategies (AU)
- NIST Cybersecurity Framework & SP 800-53r4 security controls
- DHS C^3 VP & CRR
- SAE AS5553 & 6174

Key Product Development Cybersecurity Challenges

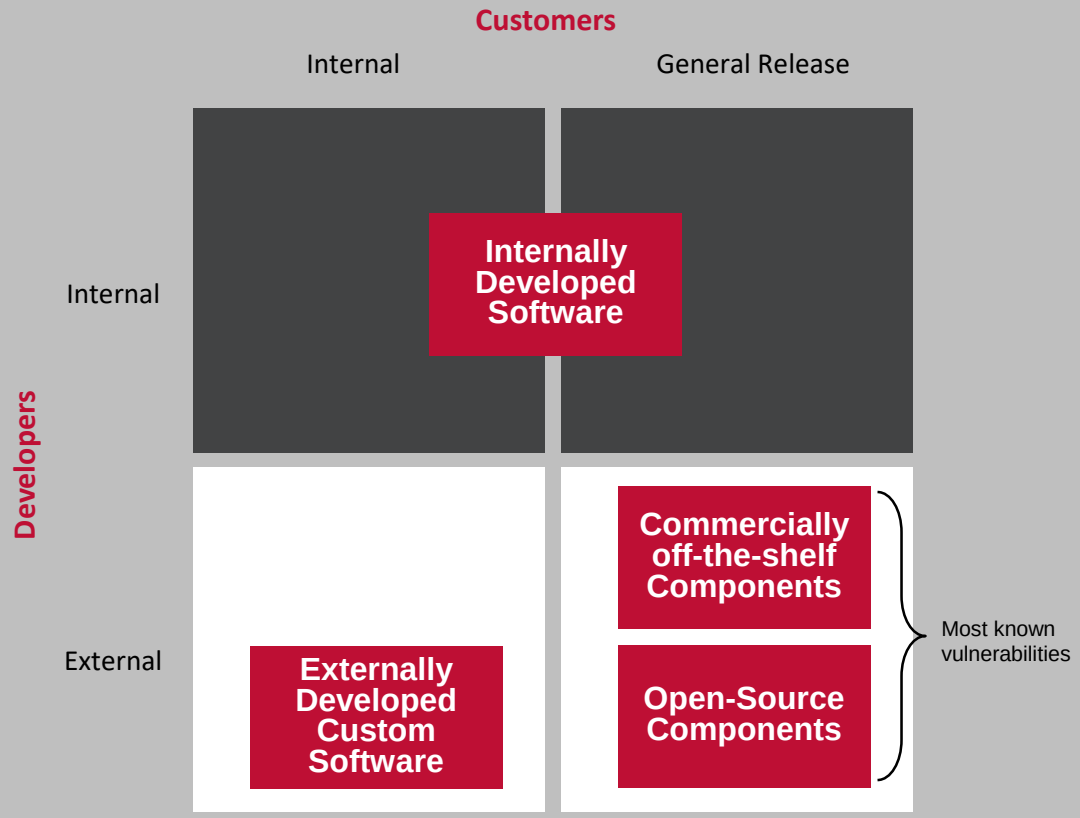


Smart Products Have Two Bills of Materials

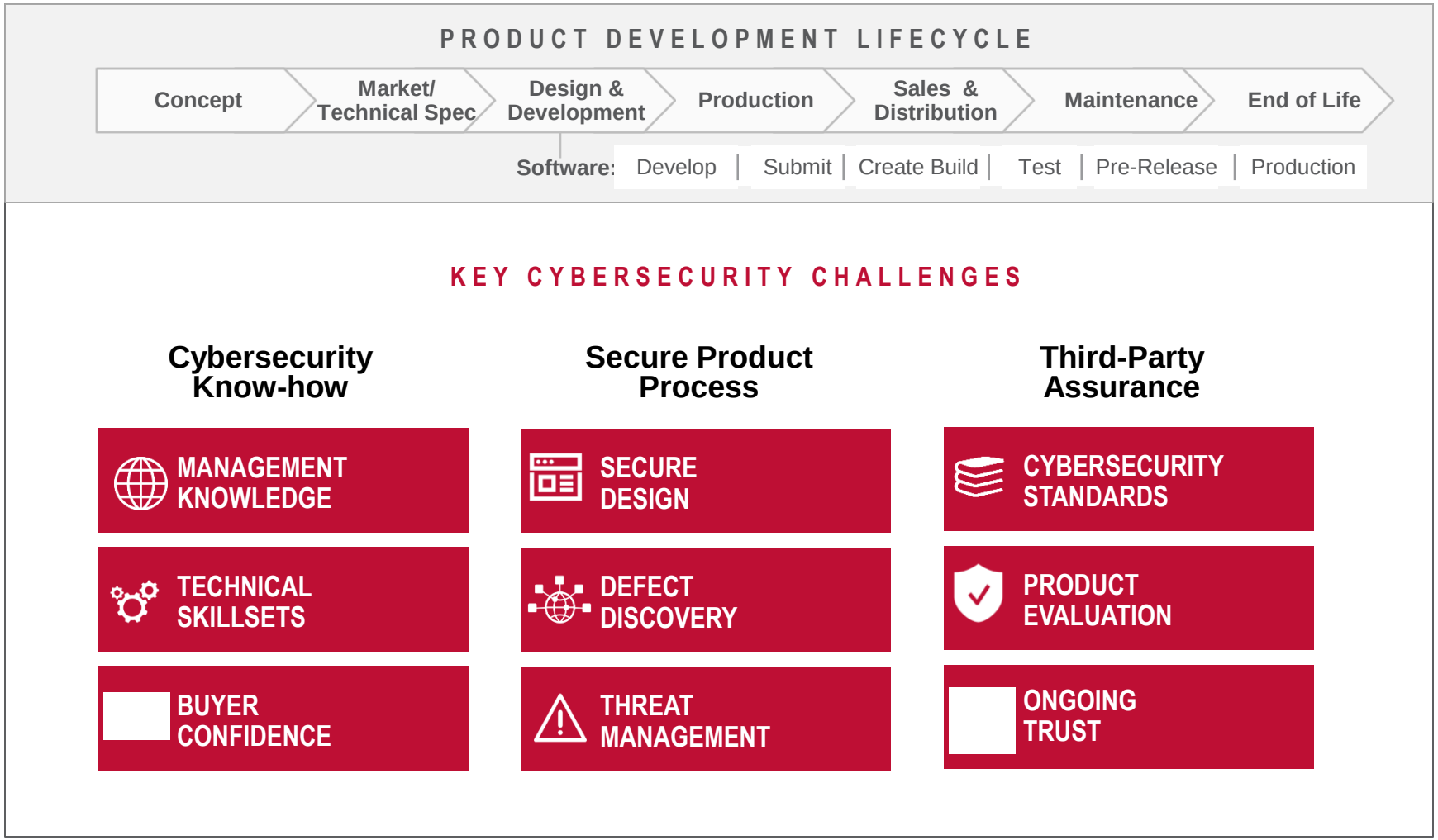
Hardware
BILL OF MATERIALS (BOM)



Software
BILL OF MATERIALS (SBOM)



Manufacturers Face Cybersecurity Challenges Throughout the Product Lifecycle



Cybersecurity Services

Vulnerabilities & Exploits

- **Known Vulnerabilities Analysis** - All software binaries, including executables and libraries, in a product are assessed for known vulnerabilities at the time of evaluation. The vulnerabilities are identified from the NIST National Vulnerability Database (NVD).
- **Structured Penetration Testing** - A mechanism of evaluation of a product to exploit vulnerabilities and weaknesses discovered in the vulnerability assessment phase.
- **Malformed Input Testing (Fuzzing)** - A black box testing technique used to reveal software weaknesses and vulnerabilities in a product by triggering them with invalid or unexpected inputs on the external interfaces of the product. The product is evaluated for unexpected behavior based on the customer's specifications.

Software Weaknesses

- **Static Code Analysis** - Static analysis of all compiled executables and libraries of the product, in order to look for known weaknesses
- **Static Binary and Byte Code Analysis** – Analysis of all compiled or intermediate binary executables and libraries of the product.
- **Common Weakness Enumerations(CWE)** - The product shall not contain any software weakness identified from CWE/SANS Top 25 Most Dangerous Software Errors, CWE/SANS on the cusp list or OWASP Top 10 2013 web application software weaknesses.

Security Controls

- **Access Control** - Review of authorization testing, a process of determining if a requester is allowed to receive a service of perform an operation
- **Cryptography** - Validates data is stored and transmitted in a form that can only be processed by its intended audience.
- **Communications** - Verifies the appropriate responses to random sets of logical information
- **Software Update Support**

Real World Example

Target

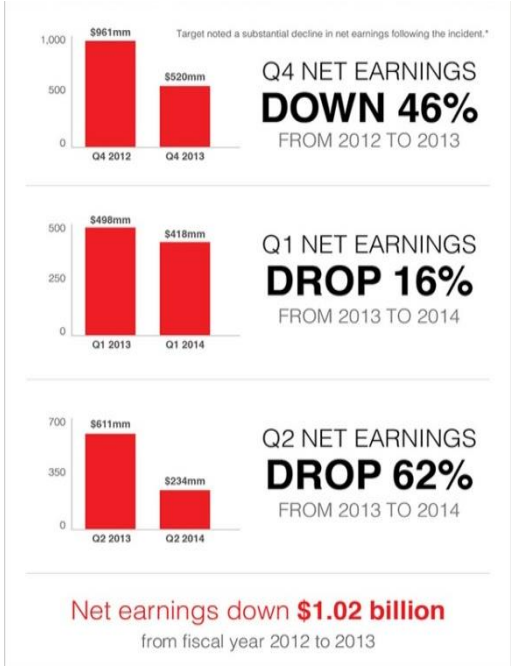
When November & December 2013

What Data from 40 million credit and debit card accounts and 70 million customer email addresses

Where Data was stolen from point-of-sale terminals in Target stores nationwide

Why Batches of data that appeared to originate from the attack appeared on underground forums around the time of the breach

How Attackers were able to access the Target network through the company's HVAC vendor; they then exploited an unpatched vulnerability in the Windows system running the POS terminals and installed malware that allowed them to capture valuable data



Key Questions for Consideration

1. Do you embed IoT devices within the products that you develop?

2. What are the cybersecurity risks associated with the IoT devices embedded in your products?

3. What are the current and future challenges that you face in mitigating those risks?

4. What might you look to gain from an engagement with a cybersecurity expert?

Thank you