AcuTech
PROCESS RISK MANAGEMENT

P2SAC
Purdue Process Safety & Assurance Center

The Convergence of Process Safety and Security Strategies for Critical Infrastructure Protection of Emerging Threats

DAVID MOORE, PRESIDENT & CEO, ACUTECH GROUP, INC.; DMOORE@ACUTECH-CONSULTING.COM

P2SAC FALL 2019 CONFERENCE PURDUE UNIVERSITY, WEST LAFAYETTE, IN, 4 DECEMBER 2019

www.acutech-consulting.com

Who We Are

Since 1994, AcuTech has been the global leader providing management and technical consulting services, a world-class training institute and a new enterprise risk management software for improving risk, safety, environmental, and security performance specific to the oil and gas, petrochemical and chemical industries.

AcuTech seeks innovation with technical excellence, and fosters a collaborative, team approach to problem solving. We are committed to excellence and customer satisfaction and continuously strive to provide responsive, flexible, and cost-effective solutions that exceed expectations.

AcuTech consultants possess strong project management skills and emphasize high-quality, on-time, cost-effective performance. AcuTech has robust project experience in safety, security, and preparedness for industries handling hazardous materials.

www.acutech-consulting.com

Emerging Threats to Critical Infrastructure

- The threat landscape to the process industries is rapidly changing and all companies have to face the difficult decision on what to do about it.
- Asymmetrical technological threats are increasing at an unprecedented pace.
- Of those, air-borne drones pose the most significant new threat to all forms of activities, businesses, and critical infrastructure bringing physical (and possibly even cyber) threats not dealt with before in the United States.
- Process safety management has a critical role in preparation for, damage limitation and improving the resilience form attacks.

Drone Capabilities

- A "drone," or "unmanned aircraft," is an aerial vehicle designed to be used without a human pilot onboard.
- Drones can be remote controlled or purely automated.
- Due to the heights at which drones can fly, they are often beyond the range of sight for most people and are difficult to detect by conventional radar.
- There are a wide range of models and capabilities from extremely small surveillance devices to very large high altitude long range drones.
- In addition, drones can also be designed to be very small and maneuverable. This means drone surveillance often occurs without the knowledge of the individual being monitored.

Drone Capabilities

Category	Size	Maximum Gross Takeoff Weight (MGTW) (lbs)	Normal Operating Altitude (ft)	Airspeed (knots)
Group 1	Small	0-20	<1,200 AGL*	<100
Group 2	Medium	21-55	<3,500	<250
Group 3	Large	<1320	<18,000 MSL**	<250
Group 4	Larger	>1320	<18,000 MSL	Any airspeed
Group 5	Largest	>1320	>18,000	Any airspeed

*AGL = Above Ground Level
**MSL = Mean Sea Level
Note: If the UAS has even one characteristic of the next level, it is classified in that level.
Source: "Eyes of the Army" U.S. Army Roadmap for UAS 2010-2035

Drone Use Expansion
FAA Forecast 2019

- The forecast highlights the phenomenal growth in the use of Unmanned Aircraft Systems (UAS).
  - The FAA projects the small model hobbyist UAS fleet to more than double from an estimated 1.1 million vehicles in 2017 to 2.4 million units by 2022.
  - The commercial, small non-model UAS fleet is set to grow from 110,604 in 2017 to 451,800 in 2022.
  - The number of remote pilots is set to increase from 73,673 in 2017 to 301,000 in 2022.
- One determined adversary is all that is required to cause damage

FBI Drone Threat Assessment

- “Terrorists likely to attack U.S. with drones”, says FBI director.1
- Christopher Wray said the risk of a drone attack is "steadily increasing" due to their widespread availability and ease of use.

1 NBC News 10-10-18 https://www.nbcnews.com/politics/national-security/terrorists-likely-attack-u-s-drones-says-fbi-director-n918586

Drone Threats

- Drones (airborne and maritime) had been used to attack Saudi Aramco prior to the Abqaiq–Khurais attack
- Similar drone strikes on Saudi Arabian oil production infrastructure had caused no significant damage.
- The targets included a Saudi airport.

A Houthi Qasef-1 model drone, as used against Aramco target in Jazan (screengrab) Middle East Eye 4-11-18

Attack on Aramco Operations
September 14, 2019

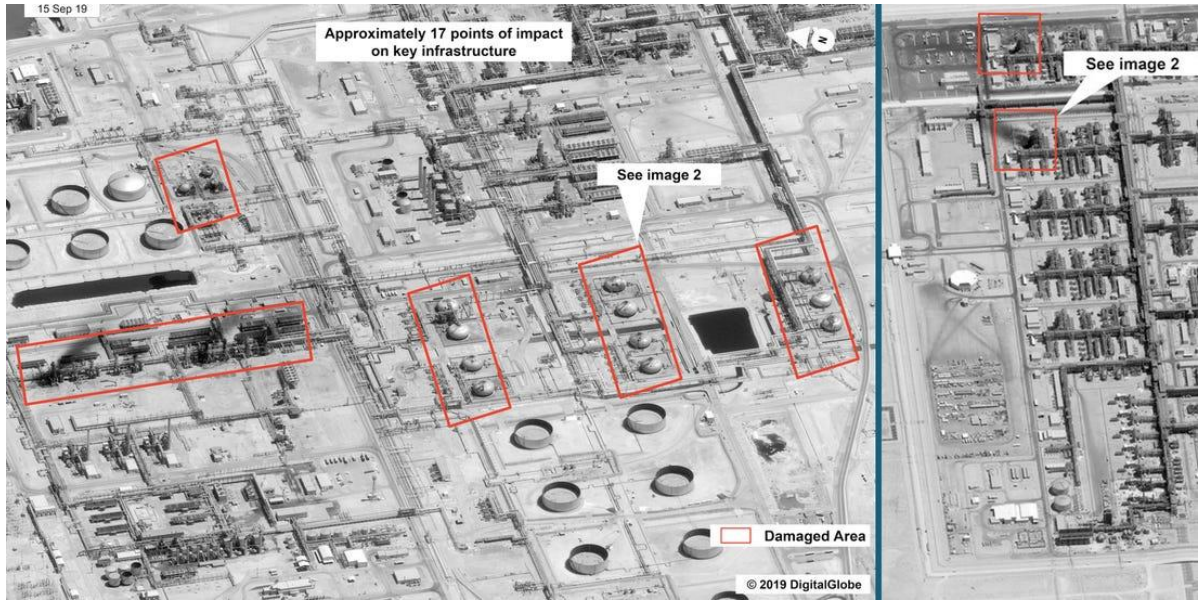
- Attacks on Saudi Arabia's Abqaiq and Khurais oil facilities from up to 21 drones.
- caused disruption to half of Saudi Arabia's oil production capacity, or 5.7 million barrels per day of crude — 5% of the world's global daily oil production.
- Saudi Aramco brought roughly half of that lost capacity back on line within two days, officials told media on Tuesday, and full production by the end of September.

1 **Remains of the missiles which were used to attack an Aramco oil facility, are displayed during a news conference in Riyadh, Saudi Arabia September 18, 2019.** *Hamad Mohammed | Reuters*

Attack on Aramco Operations
September 14, 2019

Attack on Aramco Operations
September 14, 2019

- Stealth – undetected
- Indefensible – ground counter attacks were unable to defend the facility
- Precision – most of the drones achieved their targets
- Planning – perpetrators had intelligence on critical components of the operations and strategically targeted key facilities
- Effectiveness – the damage caused was substantial to the equipment targeted but did not take out the entire operation and repair and recovery was possible.



What Process Safety Management Can Contribute to Controlling Drone Risk

- Process safety has many advantages in:
  - Prevention or minimization through design and operating practices
  - Damage limitation
  - Consequence limitation
  - Incident response
  - Incident mitigation
  - Reliability analysis
  - Resilience planning
  - Emergency planning and response
  - Crisis Management

DHS CISA Threat Statement

- UAS-related threats may include:
- Weaponized or Smuggling Payloads – Depending on power and payload size, UAS may be capable of transporting contraband, chemical, or other explosive/weaponized payloads.
- Prohibited Surveillance and Reconnaissance – UAS are capable of silently monitoring a large area from the sky for nefarious purposes.
- Intellectual Property Theft – UAS can be used to perform cyber crimes involving theft of trade secrets, technologies, or sensitive information.
- Intentional Disruption or Harassment – UAS may be used to disrupt or invade the privacy of other individuals.

https://www.dhs.gov/cisa/uas-critical-infrastructure

DHS CISA Threat Statement

- Recognizing and implementing security practices that meet federal, state, and local regulatory requirements are key to successfully managing potential security incidents associated with UAS. Although no single solution will fully mitigate this risk, there are several measures that can be taken to address UAS-related security challenges:
- Research and implement legally approved counter-UAS technology.
- Know the air domain around the facility and who has authority to take action to enhance security.
- Contact the FAA to consider UAS restrictions in close proximity to fixed site facilities. More information can be found on the Federal Aviation Administration (FAA) website.
- Update Emergency/Incident Action Plans to include UAS security and response strategies.
- Build federal, state, and local partnerships for adaptation of best practices and information sharing. More information can be found at Hometown Security.
- Report potential UAS threats to your local law enforcement agency.

https://www.dhs.gov/cisa/uas-critical-infrastructure https://www.youtube.com/watch?v=o6x-cj1wXZk

Inherently Safer Design – It Is For Everybody

- Premise: ISD can be widely and routinely used in any facility during any stage of the process lifecycle
- ISD can and should be the first strategy for security or safety threats

ISD is the First Level in the Hierarchy of Controls

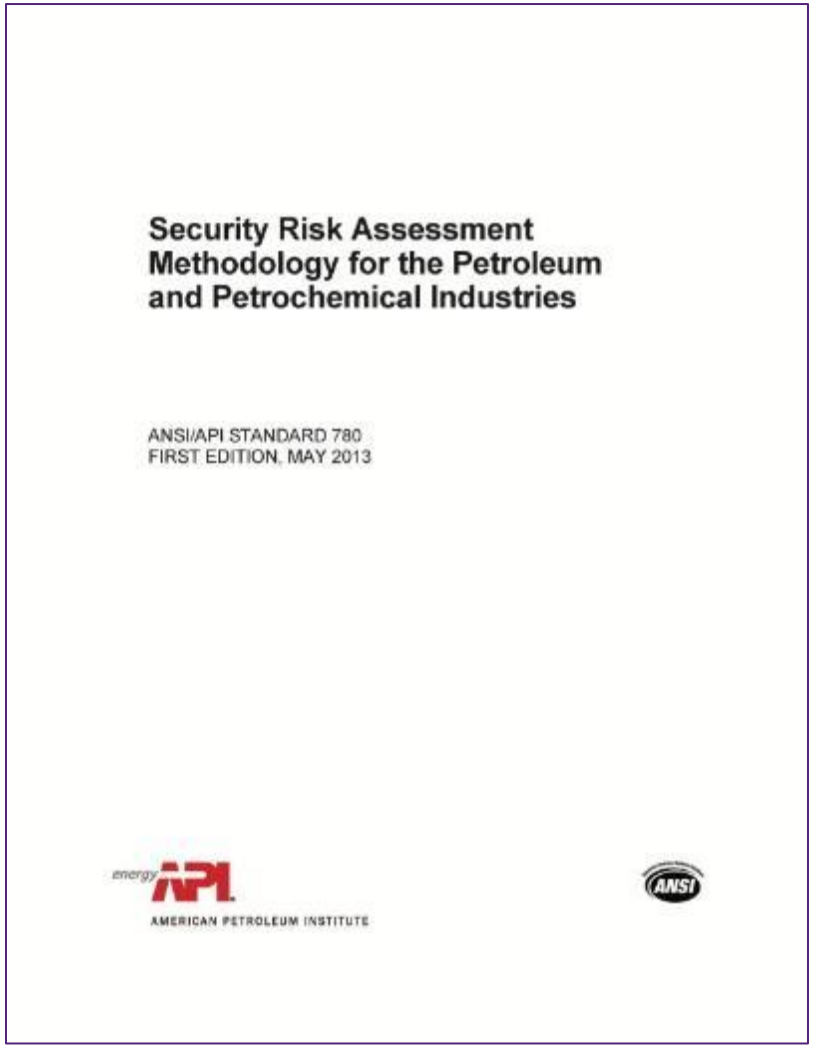
Control	Objective
Inherent	Eliminating or reducing the hazard
Segregate	Using of distance and barriers to reduce the effects of hazards
Passive	Minimizing the hazard through process and equipment design features
Active	Using controls, alarms, and other means to minimize the likelihood of the hazard escalating or to limit the consequences
Procedural	Using policies, procedures, training, administrative checks, emergency response, and other management approaches to prevent incidents, or to minimize the effects of an incident;

Inherently Safer Design Strategies

Strategy	Examples
Minimize	Use smaller quantities; eliminate unnecessary equipment; reduce size of equipment or volumes processed.
Substitute	Replace hazardous material with a less hazardous substance.
Moderate	Use less hazardous conditions, a less hazardous form of material or facilities which minimize the impact of a release.
Simplify	Design facilities which eliminate unnecessary complexity and make operating errors less likely.

US National Standard for Security Risk Assessment in the Petroleum and Petrochemical Industry

- ANSI/API Standard 780.
- A Five Step SRA methodology that is widely applicable to any threat including drones.
- Assists in identifying critical equipment, understanding potential threats, understanding potential consequences, and determining adequacy of existing and the need for additional risk mitigation.



Conclusions

- Drone threats should be addressed.
- There are possible strategies company can and should take including:
  - Evaluation of the threat, vulnerability, and consequences from drones
  - Determining options for countermeasures
  - Applying process safety management principles and practices to the issue
  - Preparing for higher level emergencies especially if high threat environment or critical infrastructure or very high consequence potential.

AcuTech Consulting Group
1919 Gallows Road
Suite 900
Vienna, VA 22182 USA
www.acutech-consulting.com