T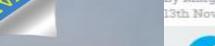he Arleigh Burke-class guided-missile destroyer USS Fitzgerald, damaged by colliding with a Philippine-flagged merchant vessel, at the US naval base in Yokosuka,, Japan, June 18, 2017. Toru

By Marin Ivezic - May 20, 2017

Test of insulin pumps
Finland smart building
Test defibrillators and pacemakers
Test traffic system vulnerabilities
Taum Sauk dam failure
2nd Ukrainian power grid attack
Stuxnet attack on Iranian nuclear power facility
SF Muni ransomware
Aurora Generator Test
Houston water distribution system hack
Worcester airport control tower lost communication
Texas power company hack
Unidentified water facility
Ransom attacks on hospitals
Maroochy shire wastewater plant compromised
Worm cripples industrial plants
German steel mill attack
Explosion of Siberian natural gas pipeline
U.S.S. Yorktown stranded

'82 '85 '96 '97 '99 '00 '03 '05 '06 '07 '08 '09 '10 '11 '12 '13 '14 '15 '16 '17

Ariane 5 rocket explosion
Los Angeles traffic system attack
Unidentified nuclear power plant
Therac-25 radiation poisoning
Alpine ski resort ransomware
Bellingham, Washington pipeline rupture
Lodz, Poland tram hack
Test of key card locks
Davis-Besse nuclear power plant worm
San Bruno gas pipeline explosion
Ukraine power grid attack
Browns Ferry nuclear plant
Dallas emergency sirens hack
Pacific Energy Resources hack
Researchers remotely control cars

Article   Cyber-Kinetic Security   IoT, Smart Cities and Smart Everything   References

Worm cripples CSX transport system
Marshall, Michigan crude oil spill
"WannaCry" Ransomware

Timeline of Key Cyber-Kinetic
Test of superyacht vulnerabilities

Collateral damage from untargeted attack
Harrisburg, Pennsylvania water filtration plant hack
Test of vulnerabilities in industrial robots

Attacks, Incidents and Research
Test of ICS vulnerability to ransomware

Hatch nuclear power plant
Demonstration of passenger jet vulnerabilities

IT

C O N F I D E N T I A L I T Y

I NTEGRITY

A V A I L A B I L I T Y

≠

SAFETY

R ELIABILITY

P RODUCTIVITY

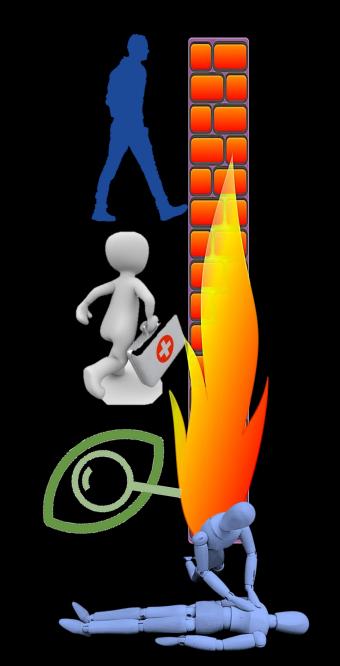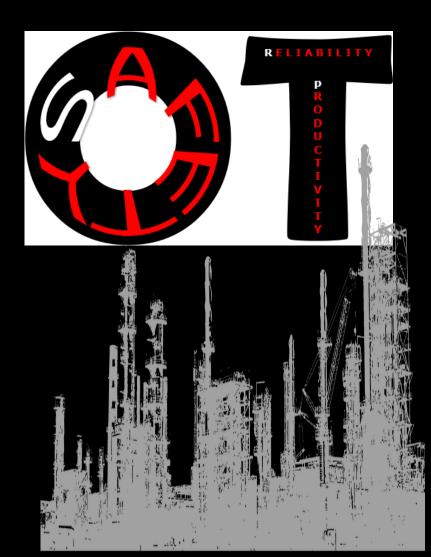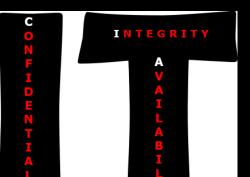# Boeing 757 Testing Shows Airplanes Vulnerable to Hacking, DHS Says

By Calvin Biesecker | November 8, 2017

Send Feedback

Cybersecurity, DHS

Sensor Node Network

Gateway

Mobile

Internet

Computer

SECURITY
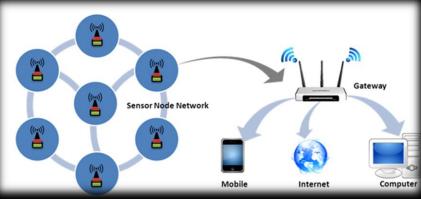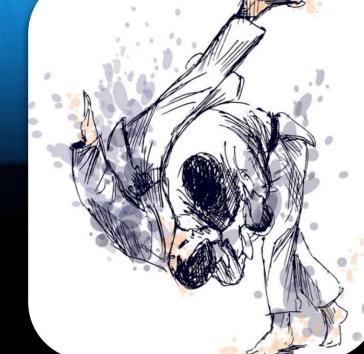
Existing users? Login   New User? Get ...

Mailbox name   Dom...

SPEAKER BIO

Mike Rebultan, aka "Art" has more than 15 years of experience as an IT professional with a background in PCI-DSS audit, Unix/Linux server lockdown and systems administration, R&D, VAPT, and currently a DFIR/SecOps in an ICS/OT company.

He is now pursuing a Doctorate in IT and holding a master degree in IT with concentration in E-Commerce security. He has also a professional graduate diploma in Digital Forensics and Cyber Security as continuing education.

He had been a local speaker of Division Zero (SG-2018), FOSS Asia (SG-2016), Null (SG-2016), PEHCON (PH-2017), Linux Meet-Up Group (SG-2016), PSITE/SSITE R3 Convention (PH-2006), and other minor conferences.

He is specializing in Computer Forensics, Network Intrusion, Data Breach, Cybercrime Investigation, Malware Analysis and Reverse Engineering.

DISCLAIMER

- The knowledge and ideas expressed in this talk does not reflect the view of any of Mike's employers – past, present, and future.

Q & A

- ## LinkedIn
  https://www.linkedin.com/in/ArtRebultan

- ## CyberSec-Blogs
  https://www.cybrary.it/members/Strainer/

- ## FB Page
  InfoSec-Tarlac

ACKNOWLEDGEMENT

- **Marin Ivezic**

  - Cyber-Kinetic Attack Compilation

- **Awesome Community & the World Wide Web {*Internet/Deep/Dark*}**

HITB CommSec SG 2018

Humongous Thanks !!!