



COVID-19 Vaccines Cybersecurity

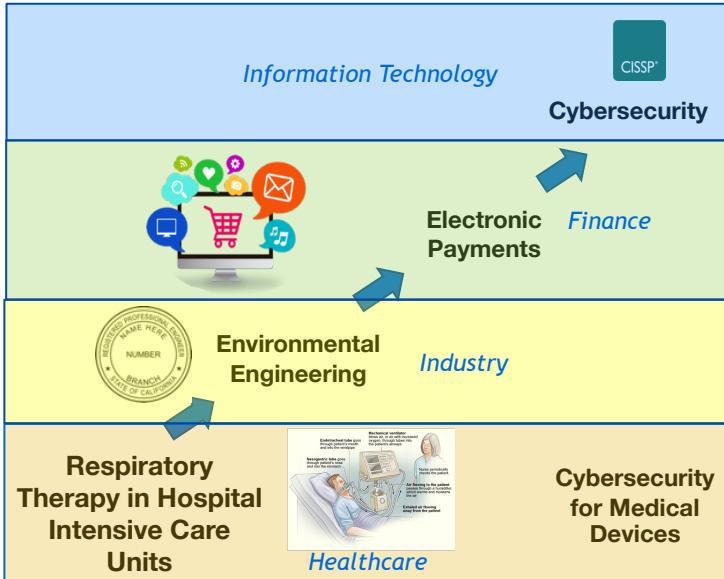
December 8, 2020

David Snyder, MBA, PE, CISSP, CSM

© 42TEK, Inc.

1

1



Snyder Background

2

1



Vaccine Production is Computer-Intensive, so Cybersecurity Matters

- ▶ Drug development and clinical trials are data-intensive.
- ▶ Quality management systems require substantial documentation.
- ▶ Large-volume manufacturing depends on industrial control systems.
- ▶ International supply chains and distribution channels operate with sophisticated logistics software.

- ▶ Once vaccines are distributed, another huge data management task will be tracking who has been inoculated and, for many, when will they be due for a second dose.

© 42TEK, Inc.

3



FORTUNE RANKINGS MAGAZINE NEWSLETTERS VIDEO PODCASTS CONFERENCES COVID-19 SEARCH SIGN IN Subscribe N

COMMENTARY • CORONAVIRUS

How bad actors could sabotage a COVID vaccine—and how that can be prevented

BY GUILDA REGEV November 17, 2020 5:00 PM EST

“It’s not unlikely that a bad actor could attempt to sabotage the availability of a vaccine by stalling or preventing its development, or even its distribution, through a targeted attack.”

“Another obvious way that a vaccine could be compromised through a cyberattack is at the manufacturing level.”

“...A cyberattack of this style, specifically intended to tamper with the vaccine formula, would home in on the Internet-connected operational technology (OT) and industrial networks that help run manufacturing facilities.”

<https://fortune.com/2020/11/17/covid-19-coronavirus-vaccine-cyberattack-sabotage/>

© 42TEK, Inc.

4



FORTUNE excerpts continued...

"Should a bad actor be interested in **damaging vaccine distribution**, they could stage an attack on the **temperature control systems** in place."

"The **logistics of shipping and finally distributing** a vaccine are prime for a cyberattack, given how often the product would have to change hands getting from the place of origin to the final destination."

"In terms of vaccines, a **ransomware attack could affect scheduling software**, leading to delays in delivery and affecting the vaccine distribution schedule. **Storage rooms could be locked down**. **Transportation could be rerouted**. The connected systems that grant operators visibility into their systems could very well be the downfall of the operations."

© 42TEK, Inc.

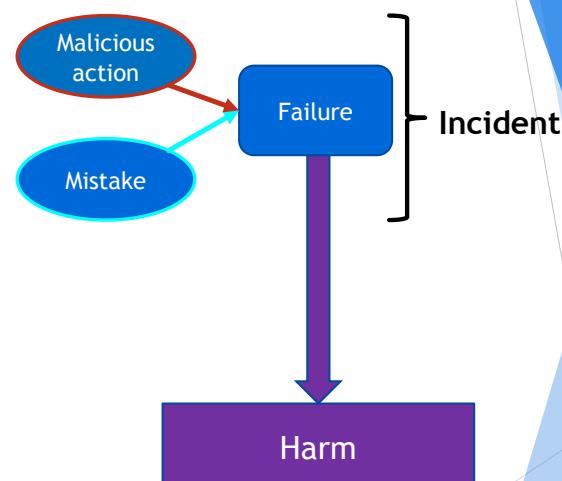
5

5

Cybersecurity is not only about malicious actions. Inadvertent failures can result from the unintended consequences of honest mistakes.

When industrial processes and healthcare are involved, there can be grave consequences from cybersecurity incidents, regardless of whether the incidents were intentional or not.

© 42TEK, Inc.



6

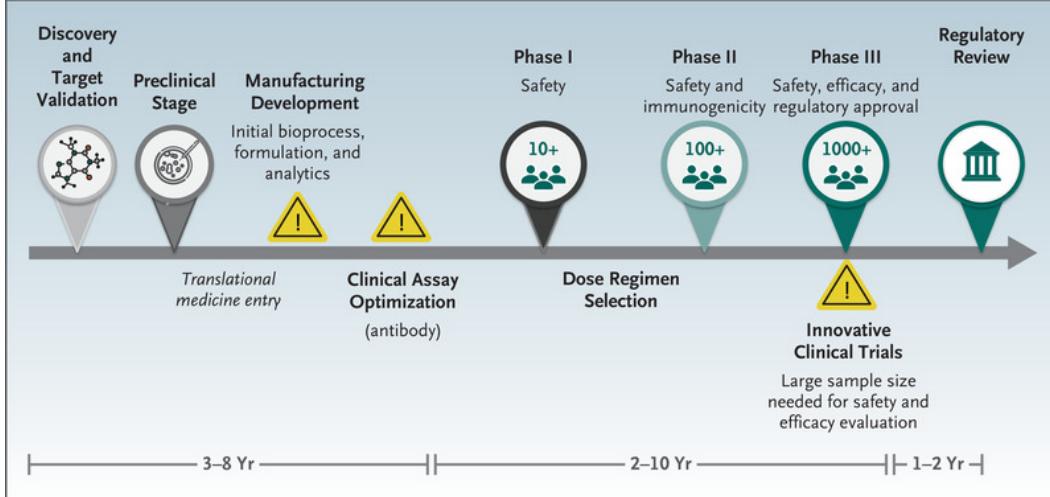
6



Vaccine Development and Production

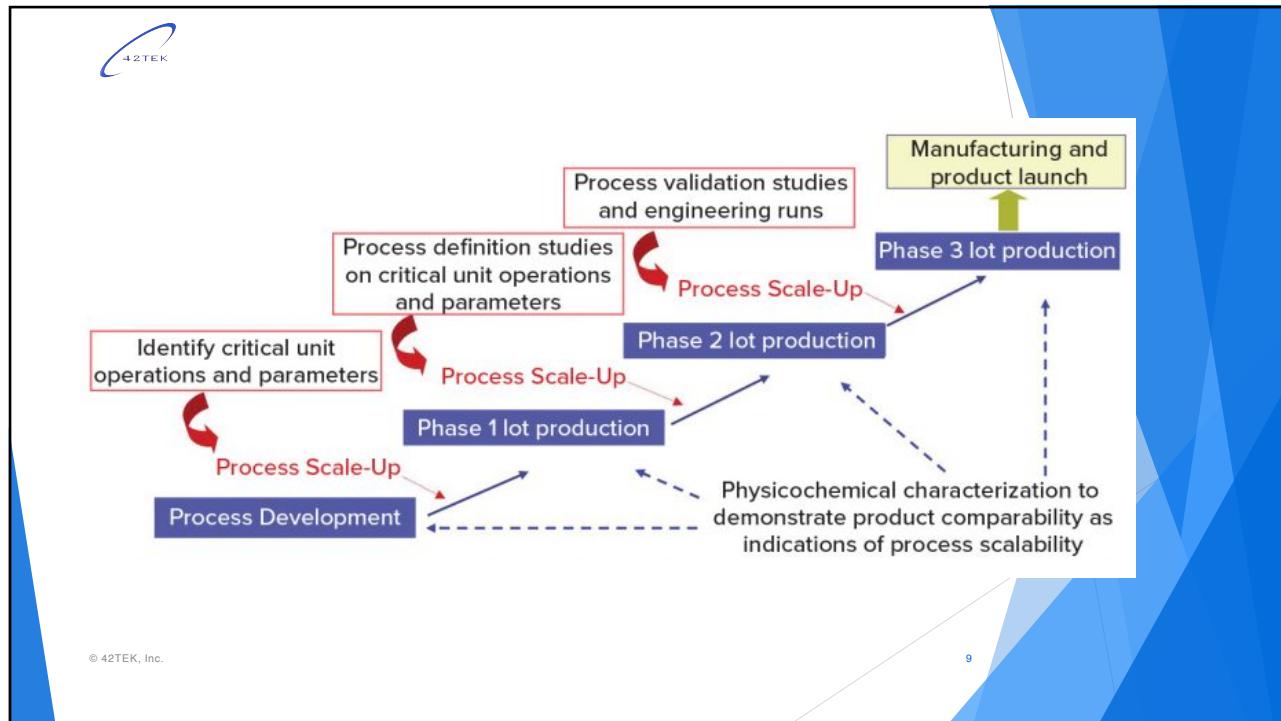
© 42TEK, Inc.

7

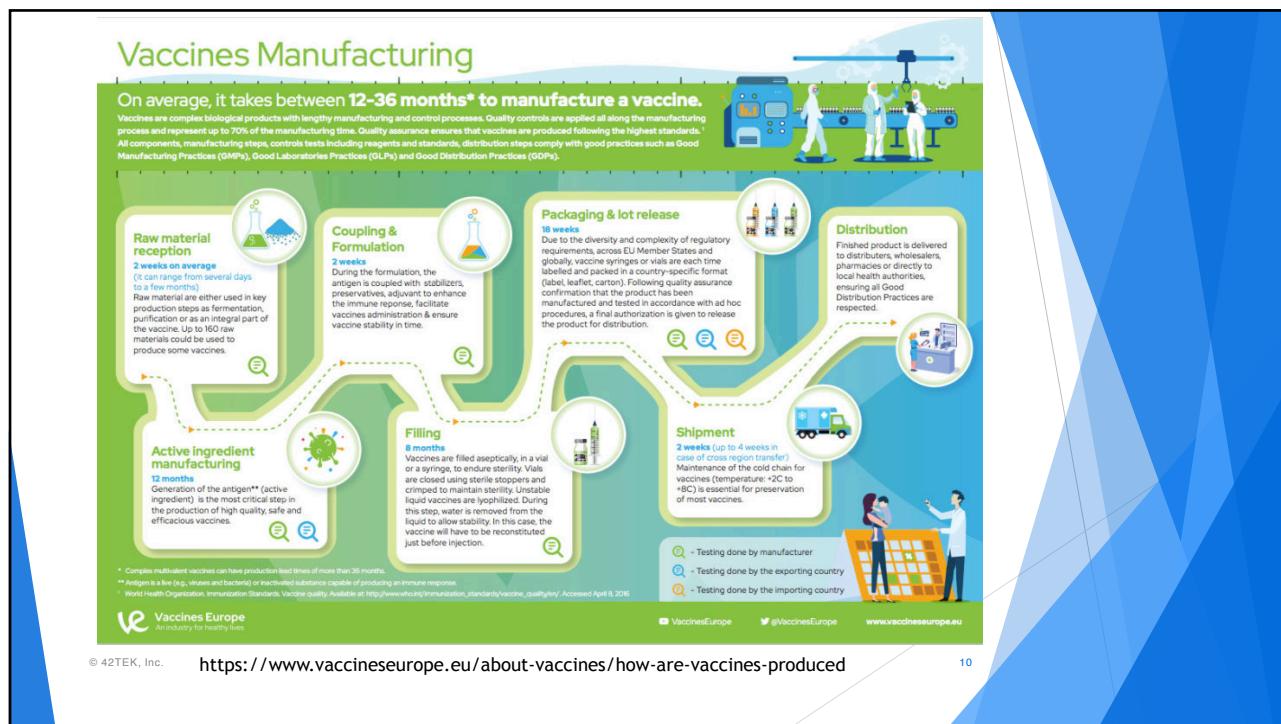


© 42TEK, Inc.

8



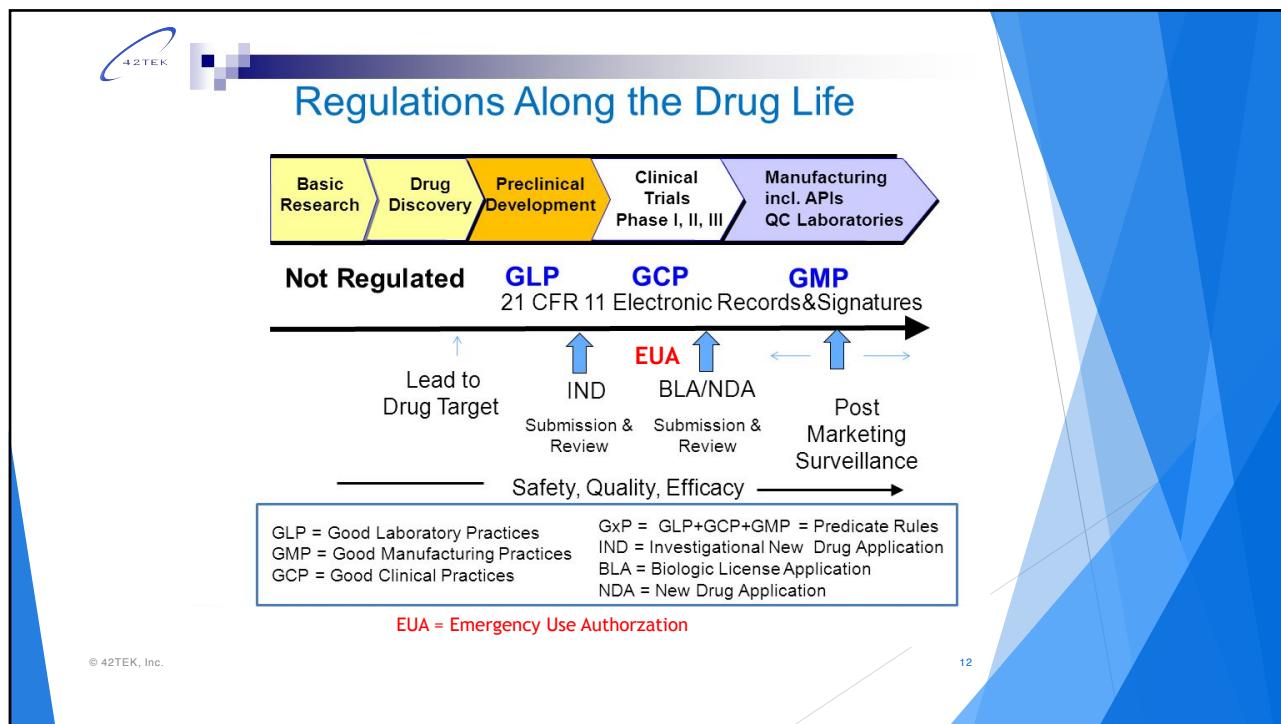
9

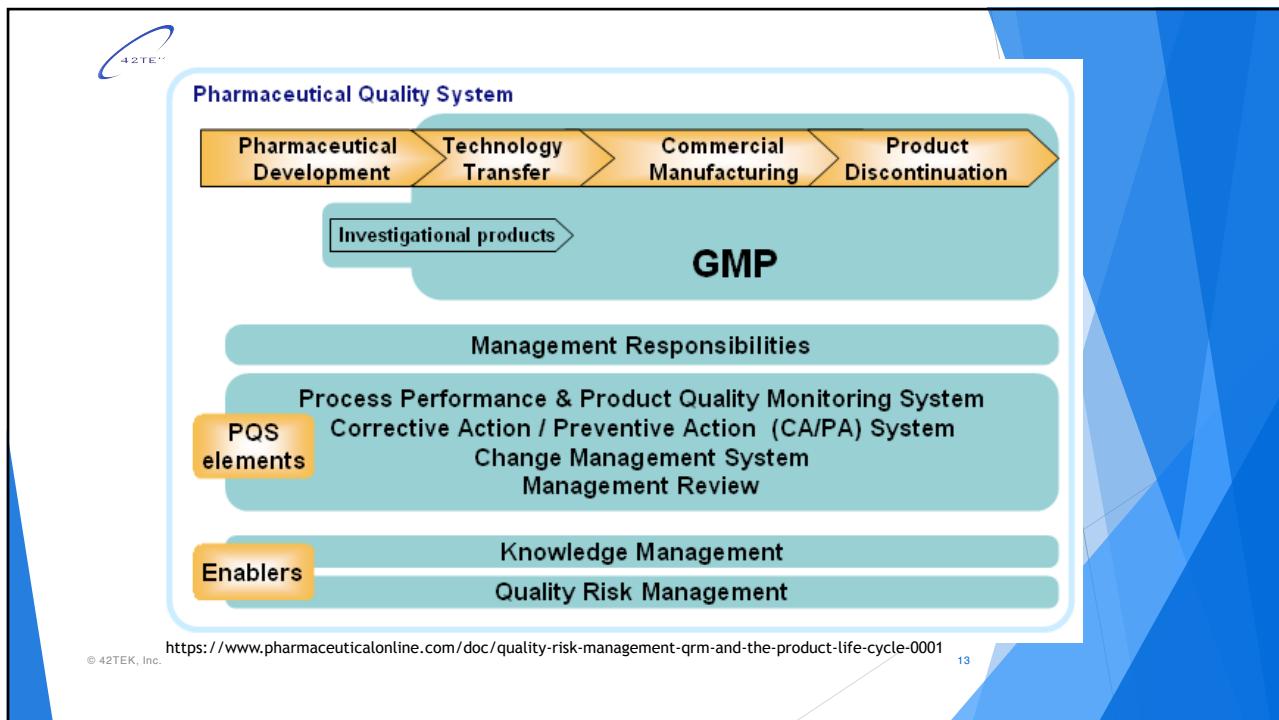


10



11





13

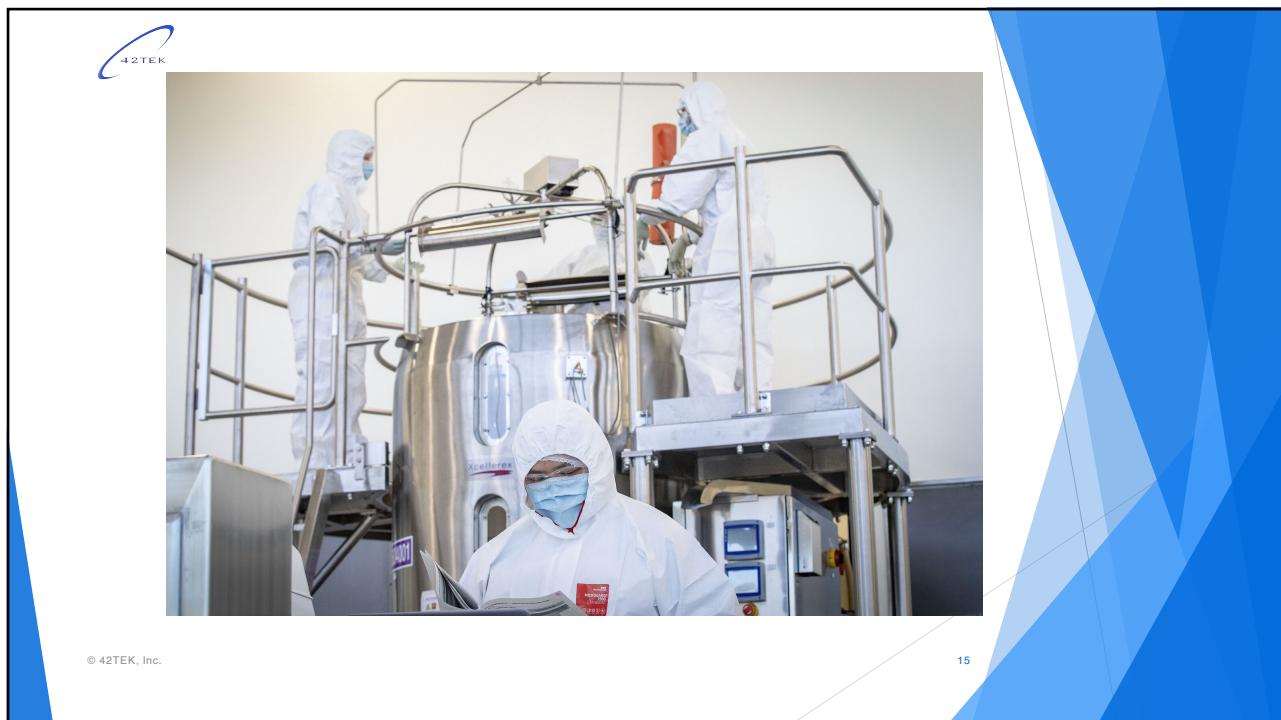
The Vaccines Will Probably Work. Making Them Fast Will Be the Hard Part.

Front-runners in the coronavirus vaccine race won't make nearly as many doses this year as were predicted, but they may kick into high gear next year.

"Industry analysts and company executives are optimistic that hundreds of millions of doses will be made by next spring. But the companies – backed with billions of dollars in federal money – will have to overcome hurdles they've encountered in the early days of making vaccines. Moderna's and Pfizer's vaccines use **new technology that has never been approved** for widespread use. They are ramping up into the millions for the first time. Other challenges include promptly **securing raw vaccine ingredients** and mastering the art of **creating consistent, high-quality batches.**"

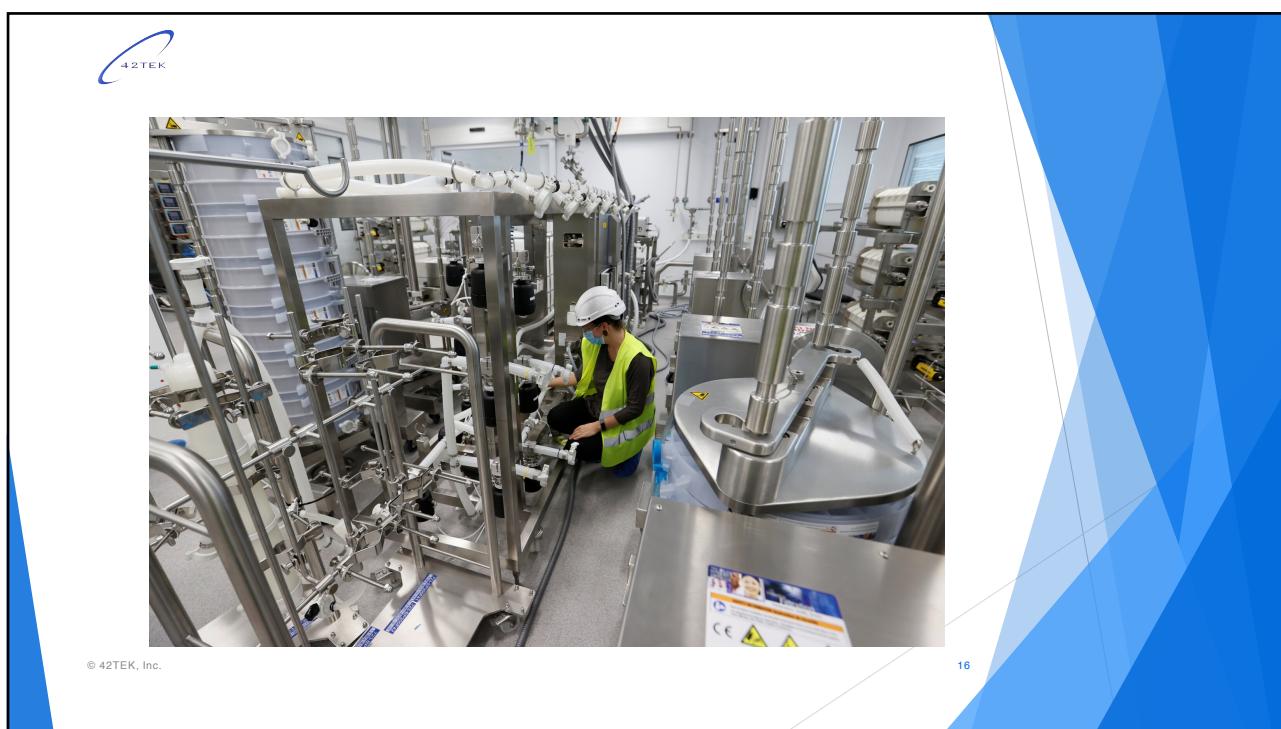
<https://www.nytimes.com/2020/11/17/health/coronavirus-vaccine-operation-warp-speed.html>

14



© 42TEK, Inc.

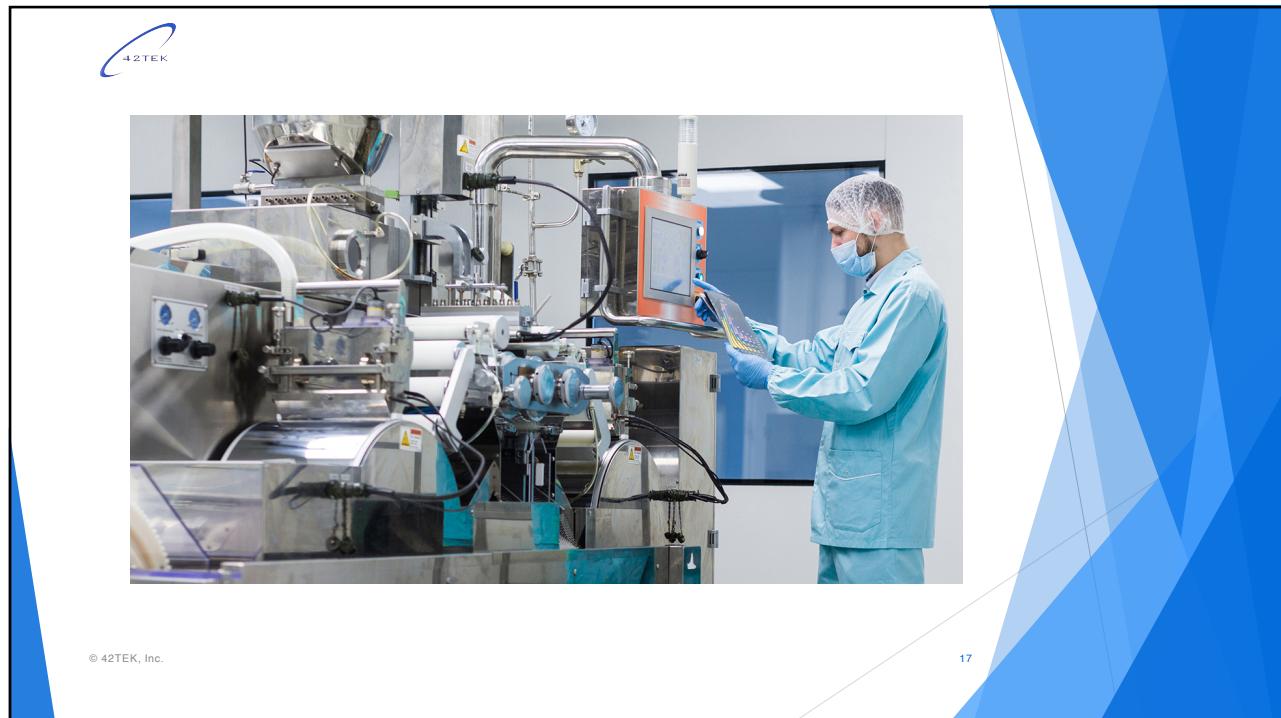
15



© 42TEK, Inc.

16

16



© 42TEK, Inc.

17

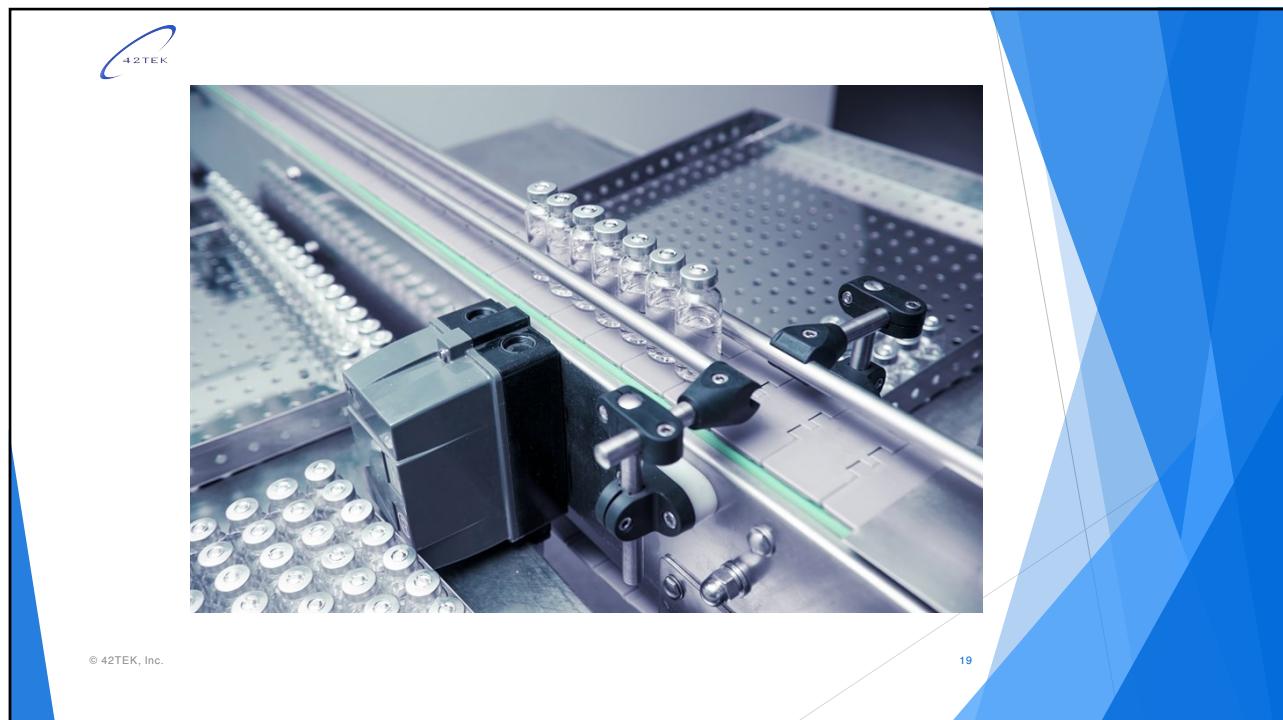
17



© 42TEK, Inc.

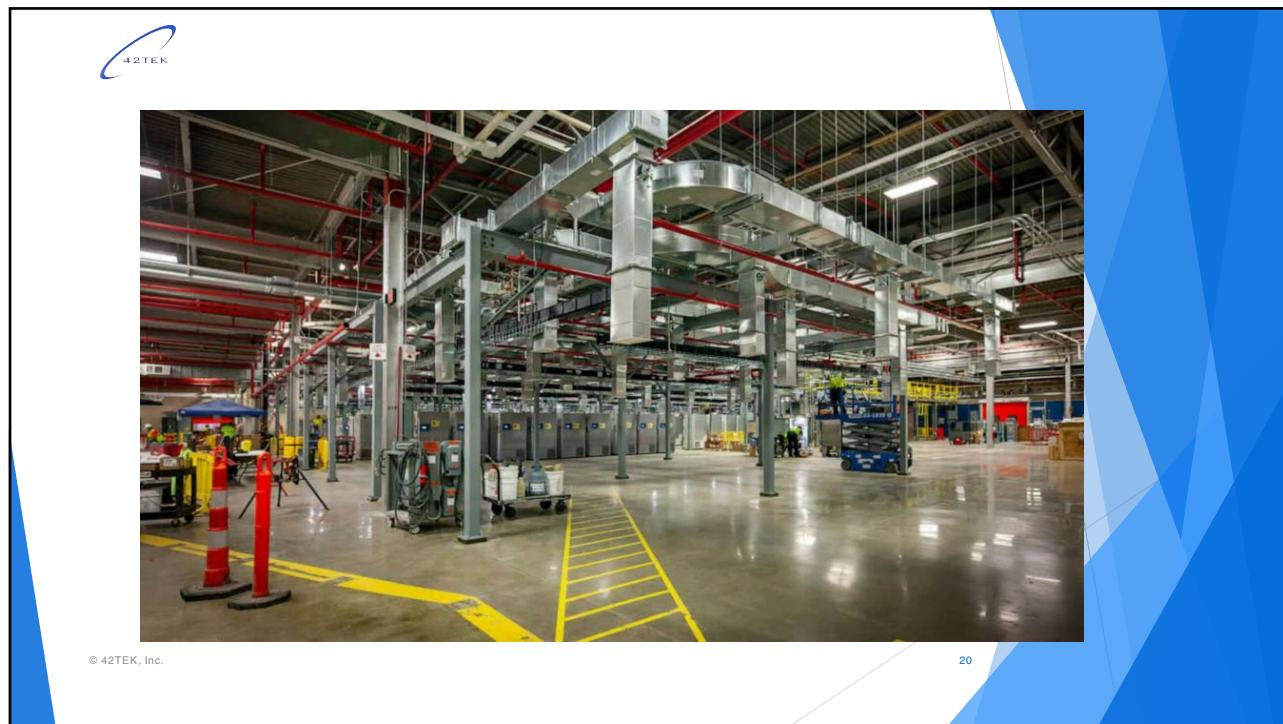
18

18



19

19



20

20



© 42TEK, Inc.

21

21



© 42TEK, Inc.

22

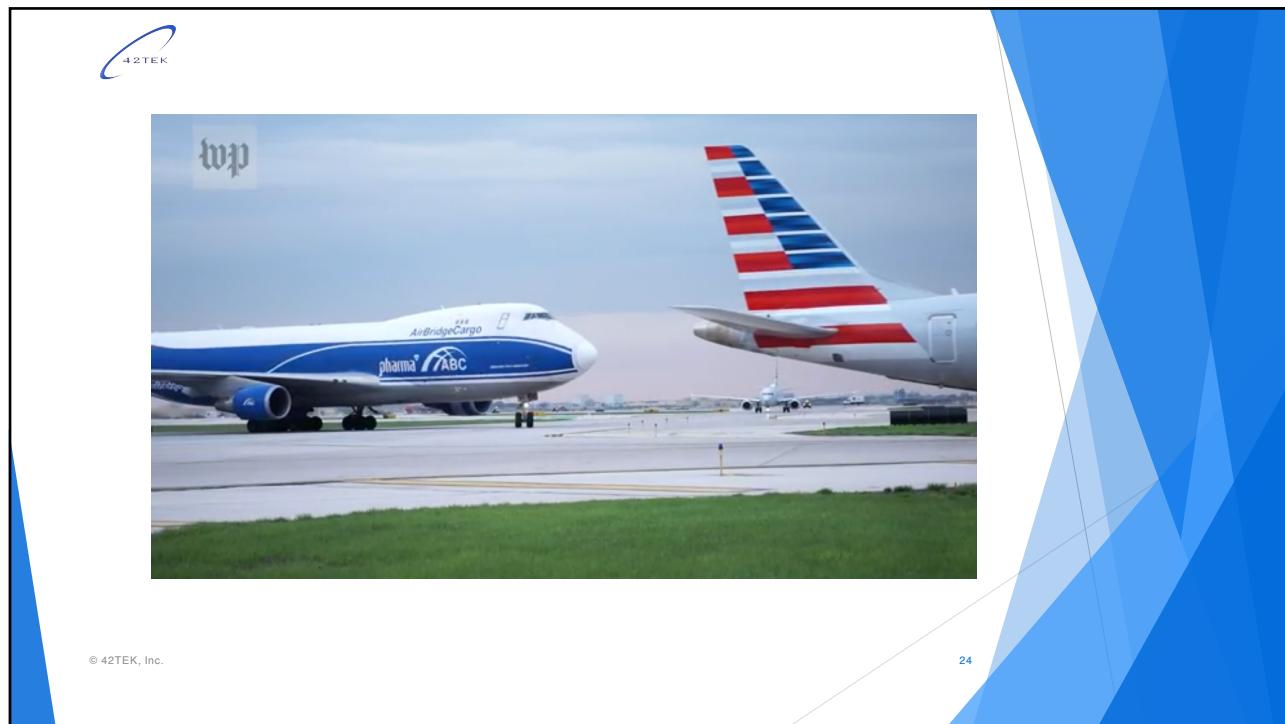
22



© 42TEK, Inc.

23

23



© 42TEK, Inc.

24

24



Gemini
DATA LOGGERS

**Tinytag Ultra 2
Temperature Logger
(-40 to +85 °C)**

TGU-4017

DATA SHEET

Issue 10
26th August 2019
EAS/CS

Tinytag Ultra 2 data loggers are ideally suited to monitor interior applications where there is little or no moisture.

Tinytag Ultra 2 data loggers have a high reading accuracy, high resolution, large memory, a fast offload speed and a low battery monitor.

The TGU-4017 is a self contained temperature recorder.

Popular Applications

- Office and housing monitoring
- Pharmaceutical manufacture
- Dry food storage
- Museum display and repository
- Incubators

Features

- Temperature recorder
- 32,000 reading capacity
- High accuracy
- High reading resolution
- Fast data offload
- Splash-proof case
- Low battery monitor
- User-replaceable battery




www.tinytag.info sales@tinytag.info

© 42TEK, Inc.

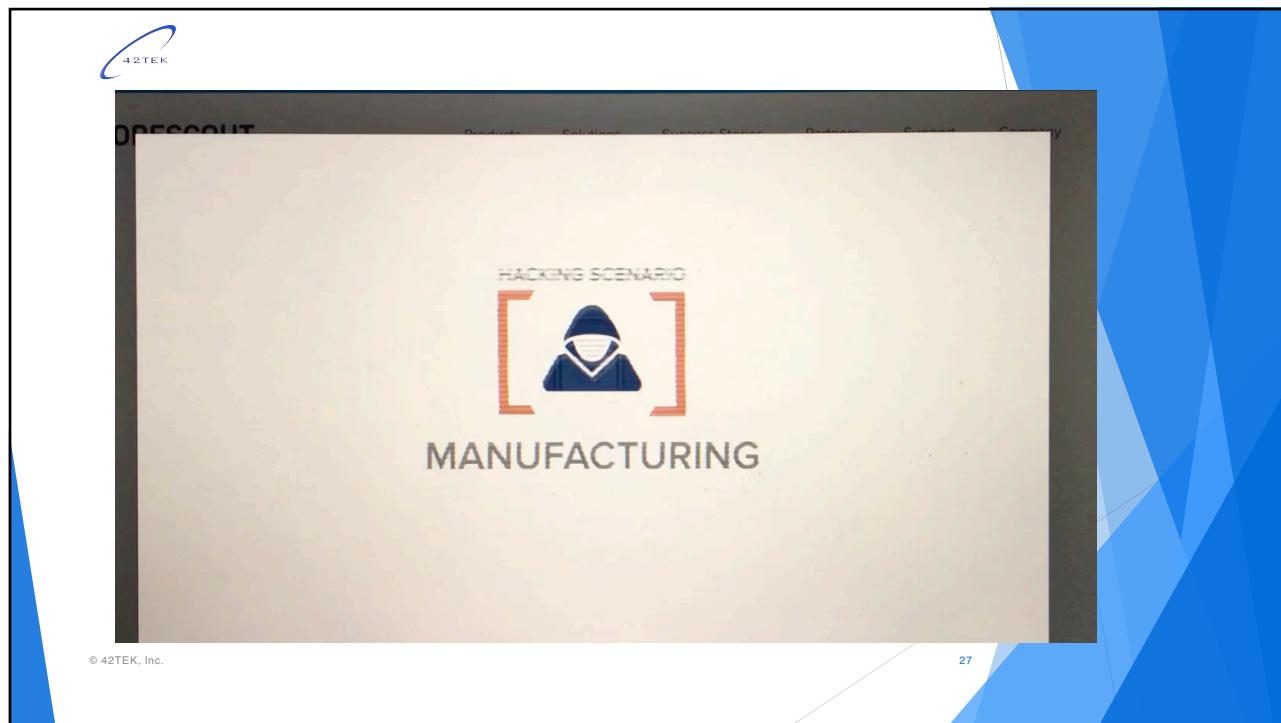
25



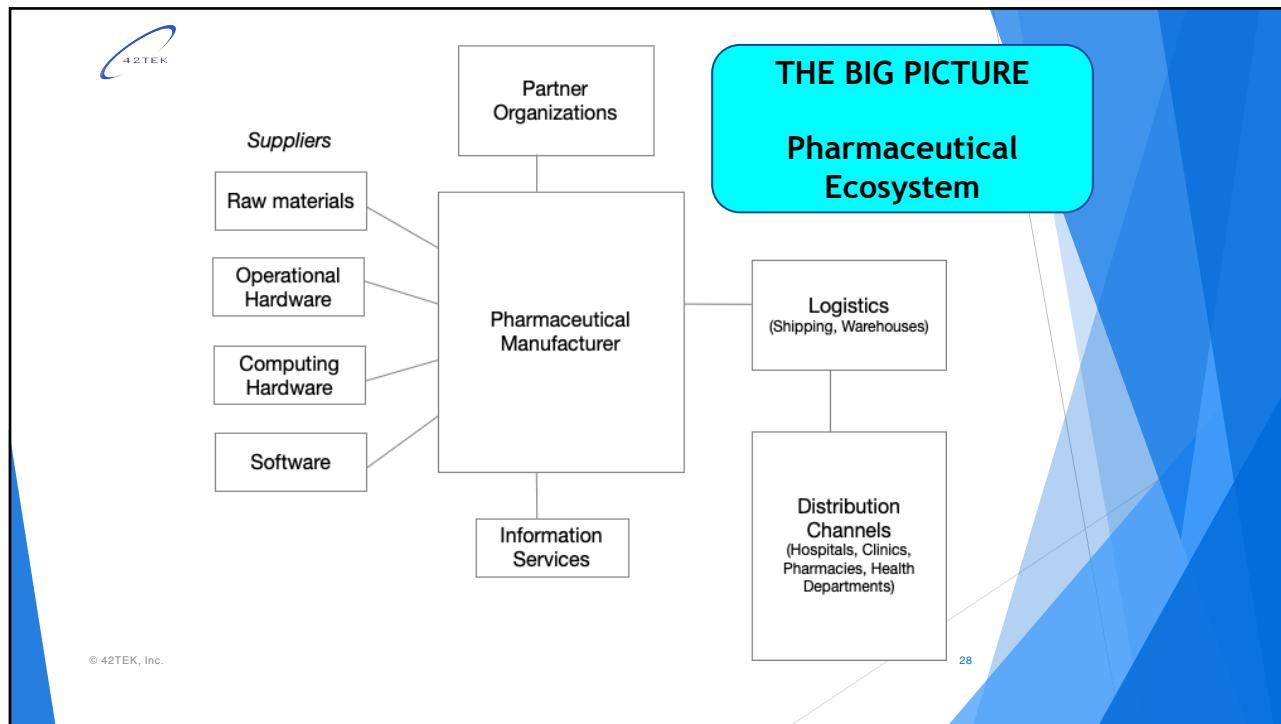
Security for Vaccine Production and Delivery

© 42TEK, Inc.

26



27



28



Deep Dive into Manufacturing and Then Back Up to Ecosystem Level

© 42TEK, Inc.

29

29



Industrial Control Systems (aka Industrial Automation and Control Systems)

“An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.” --

<https://csrc.nist.gov/glossary/term/ICS>

© 42TEK, Inc.

30

30

42TEK

Manufacturing Equipment

A sensor converts a physical attribute to an electrical signal. An actuator does the opposite: it changes an electrical signal to physical action.

- ▶ Sensors
 - ▶ Temperature, pressure, flow, pH, voltage, current, vibration, high level alarms (when tank gets too full), etc.
- ▶ Actuators
 - ▶ Motor-operated valve, solenoid switch, etc.

▶ Controllers

- ▶ Programmable logic controllers, remote terminal units

Sensors, actuators, and controllers work together to automate the work of manufacturing equipment.

▶ Machines

- ▶ Pumps, bioreactors, heaters, refrigerators, dispensers, conveyors, etc.

Programmable Logic Controller: an industrial computer control system that **continuously monitors** the state of input devices and **makes decisions** based upon a custom program to **control the state of output devices**

© 42TEK, Inc.

31

31

42TEK

Process Analysis and Control P&ID Handout Page 17 Lecture 4, Week 3, 2012

CYBER-PHYSICAL SYSTEMS

Mix of analog and digital

The diagram illustrates a Cyber-Physical System (CPS) architecture. It shows a flow indicating controller (FIC 123) at the primary location, which performs a square root flow calculation. This controller is connected via a data link to a field-mounted temperature indicating controller (TIC 123). The TIC 123 is connected to a PLC (Programmable Logic Controller) via a data link. The PLC is also connected to a YIC 123 (PLC indicating controller) and a TT 123 (Temperature Transmitter). The system includes a flow transmitter (FT 123) connected to an impulse tubing assembly, a pneumatically-actuated valve, and an electrically-actuated valve. A temperature computer is also present. The PLC is connected to a TY 123 (Temperature Computer Output) and a TT 123 (Temperature Transmitter).

FIC – Flow Indicating Controller
TIC – Temperature Indicating Cont.
YIC – PLC Indicating Controller
TY – Temperature Computer Output
FT – Flow Transmitter
TT – Temperature Transmitter

© 42TEK, Inc.

32



Information Technology vs Operational Technology

- ▶ The main difference between OT and IT devices is that OT devices control the physical world, while IT systems manage data.
- ▶ The increased use of network-connected industrial control systems is blurring this distinction.

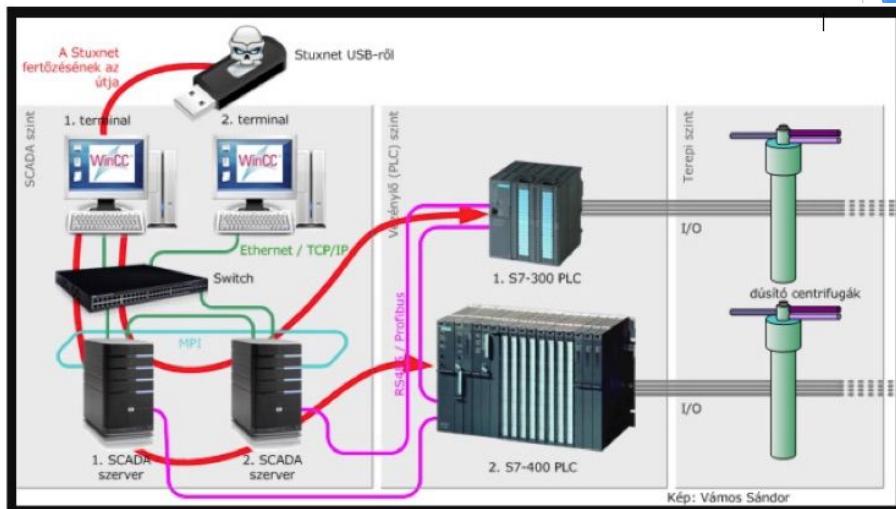
© 42TEK, Inc.

33

33



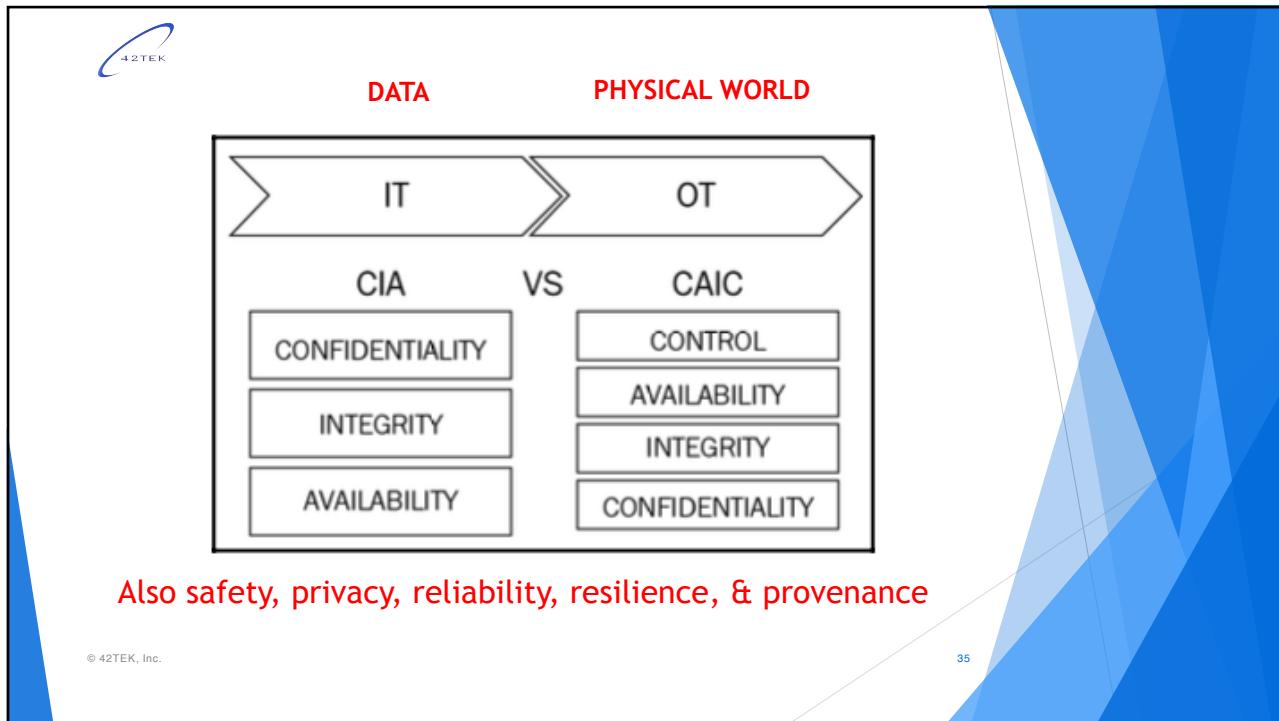
Stuxnet



© 42TEK, Inc.

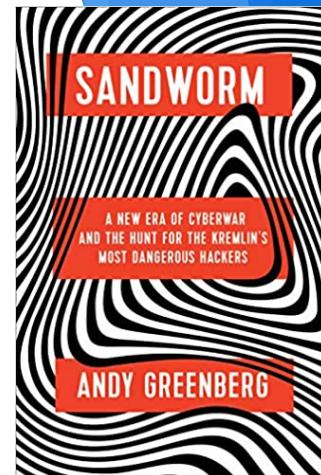
34

34



35

- ▶ ICS cyber-attacks represent a real risk as ICS become more integrated with other IT systems
 - ▶ Unauthorized access can allow an attacker to execute malicious commands without uploading malware (e.g., start/stop devices, change control settings)
 - ▶ Denial of service at a critical time can allow unsafe conditions to go unnoticed (e.g., missed alarms) or prevent operators from adjusting equipment settings (e.g., unable to start/stop motors, open/close valves, etc.)



© 42TEK, Inc.

36

36

 BSI Publications on Cyber-Security | Industrial Control System Security -
Top 10 Threats and Countermeasures

Top 10 Threats	Trend since 2016
Infiltration of Malware via Removable Media and External Hardware	↗
Malware Infection via Internet and Intranet	↗
Human Error and Sabotage	↑
Compromising of Extranet and Cloud Components	↑
Social Engineering and Phishing	↘
(D)Dos Attacks	↑
Control Components Connected to the Internet	↗
Intrusion via Remote Access	↗
Technical Malfunctions and Force Majeure	↘
Compromising of Smartphones in the Production Environment	↗

https://www.altian-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005E.pdf;jsessionid=5E57EB96FDCA87289C76418DDA37CD48.1_cid501?__blob=publicationFile&v=9

© 42TEK, Inc.

37

37



Potential Damage

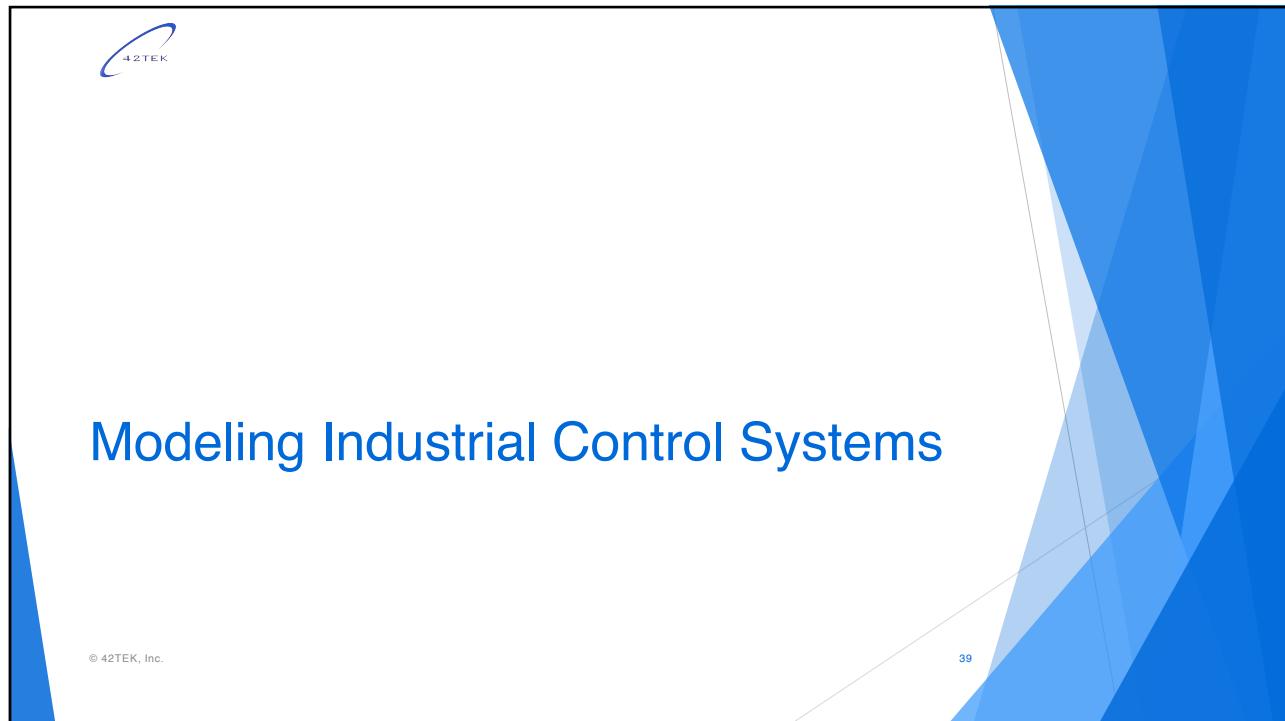
- ▶ Loss of availability of the ICS / loss of production
- ▶ Data leakage / loss of know-how (intellectual property)
- ▶ Physical damage to facilities
- ▶ Triggering of safety procedures or interfering with safety systems
- ▶ Deterioration of product quality

© 42TEK, Inc.

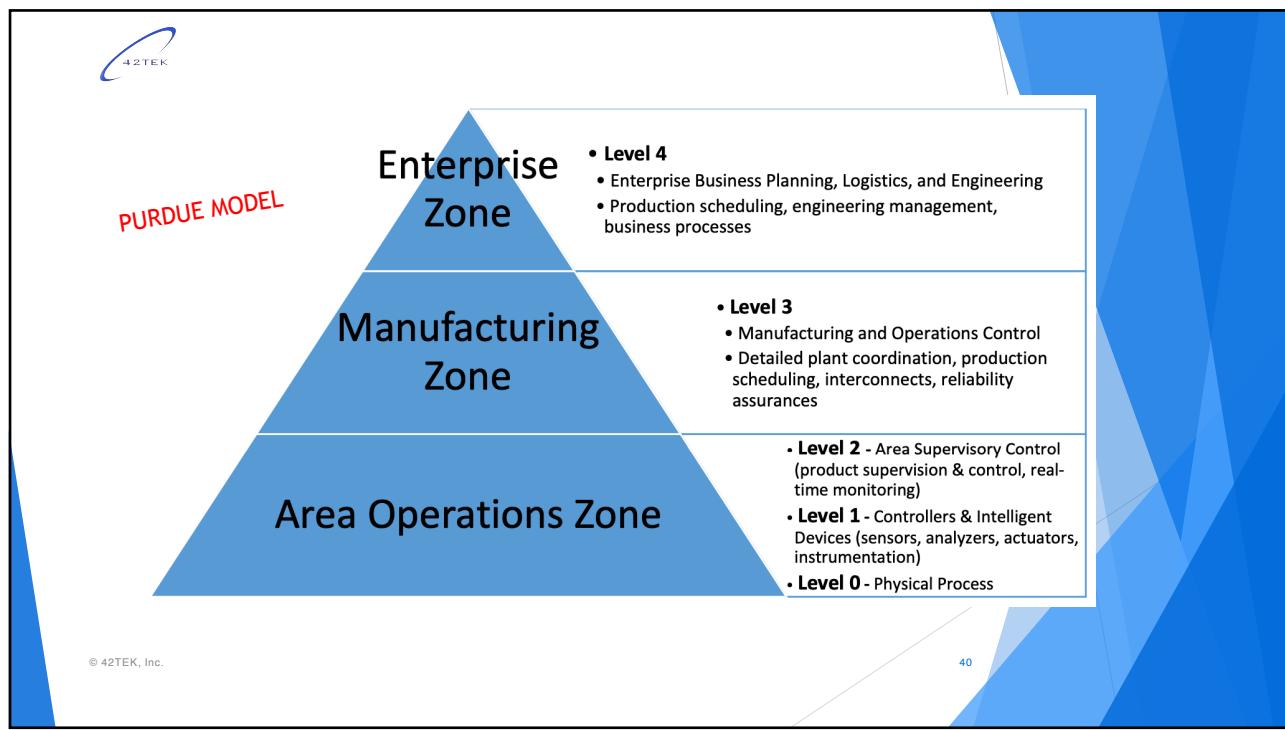
38

38

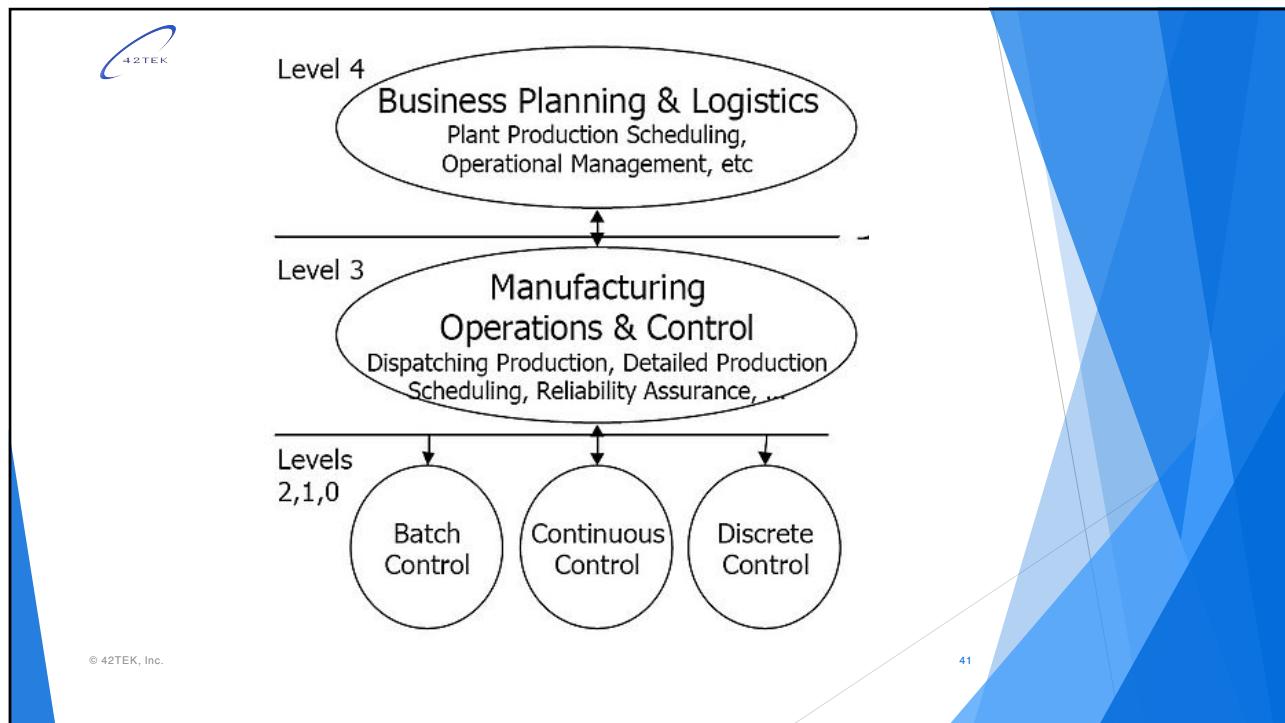
19



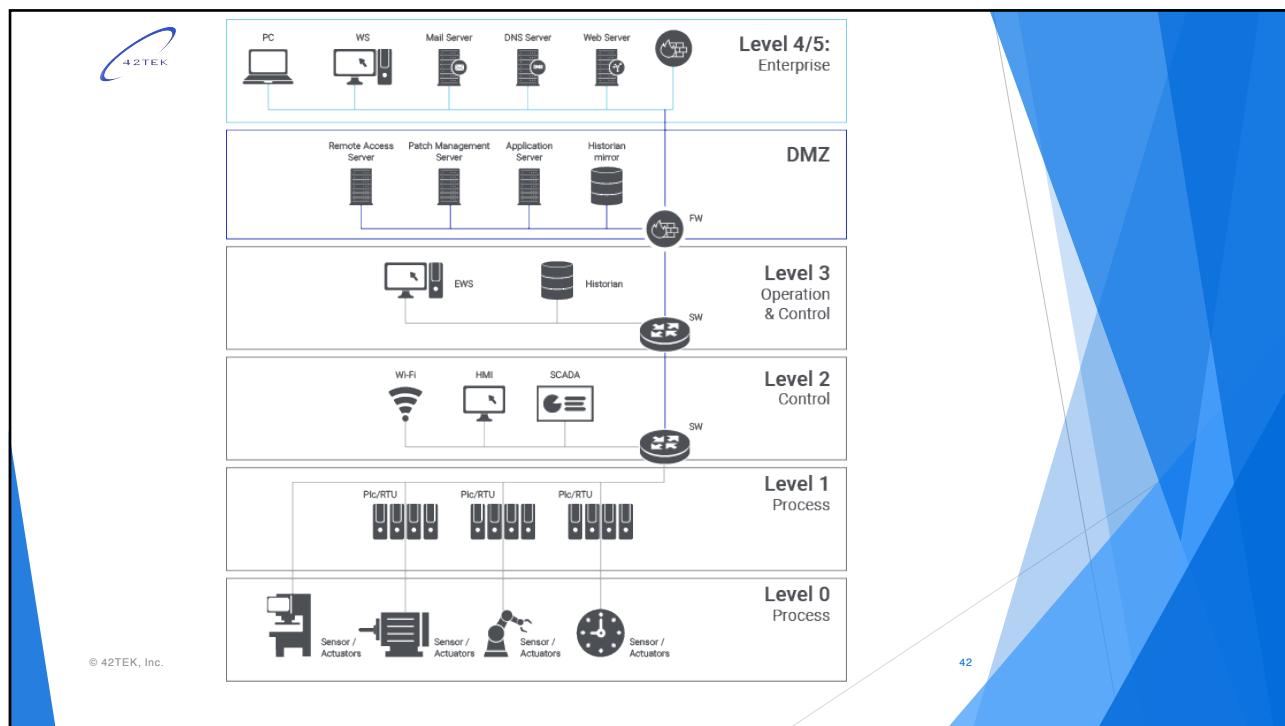
39



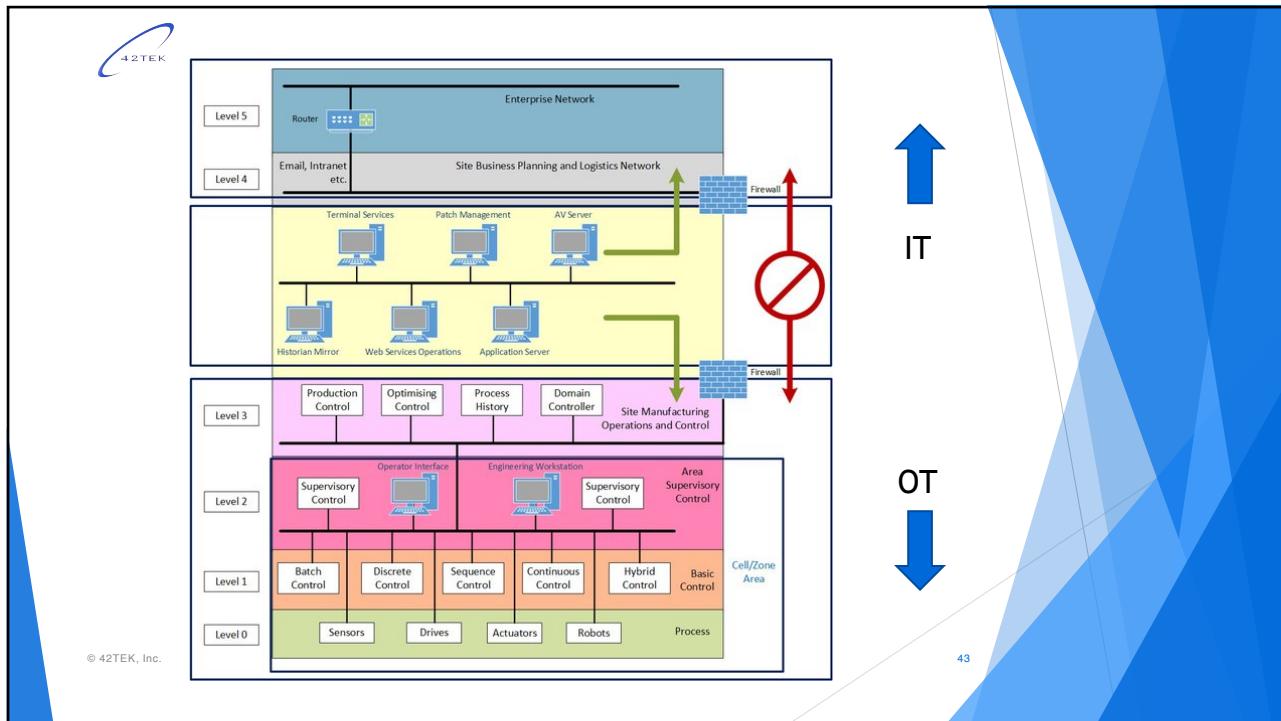
40



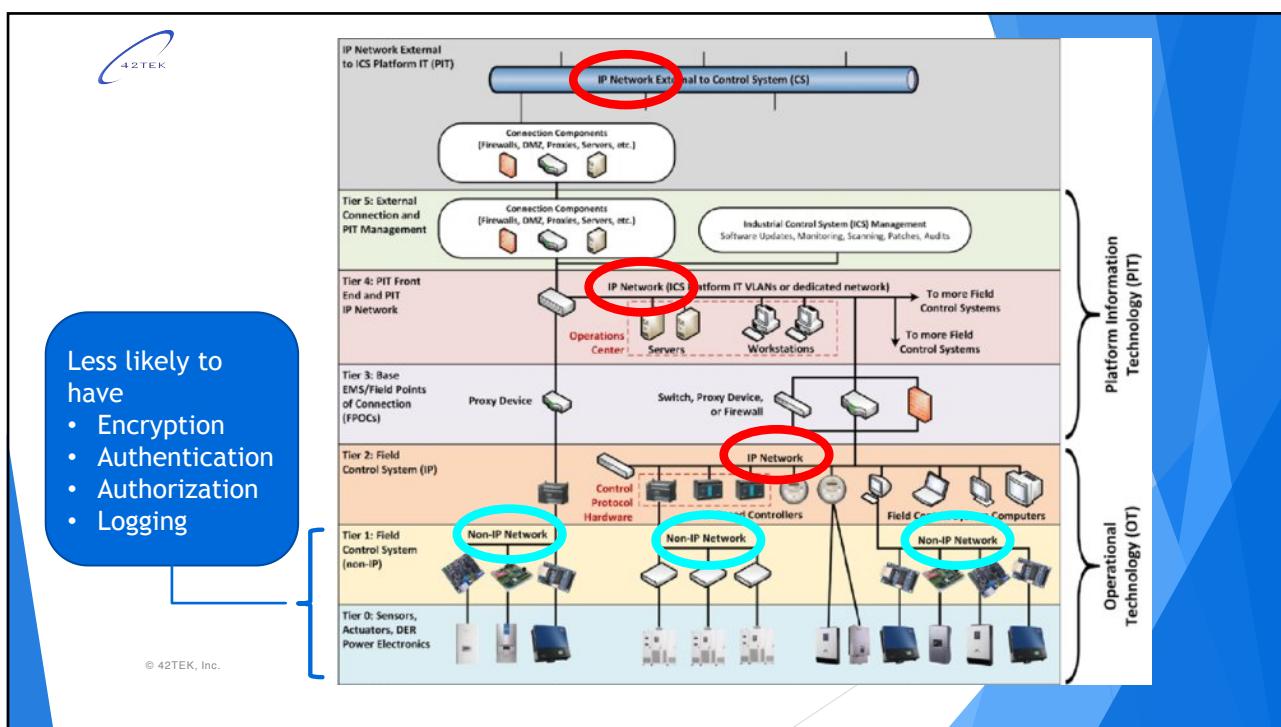
41



42



43



44



Attacking an ICS

© 42TEK, Inc.

45

45



Attack Demonstration

© 42TEK, Inc.

<https://engineering.purdue.edu/VAAMI/ICS-modules.pdf>

46

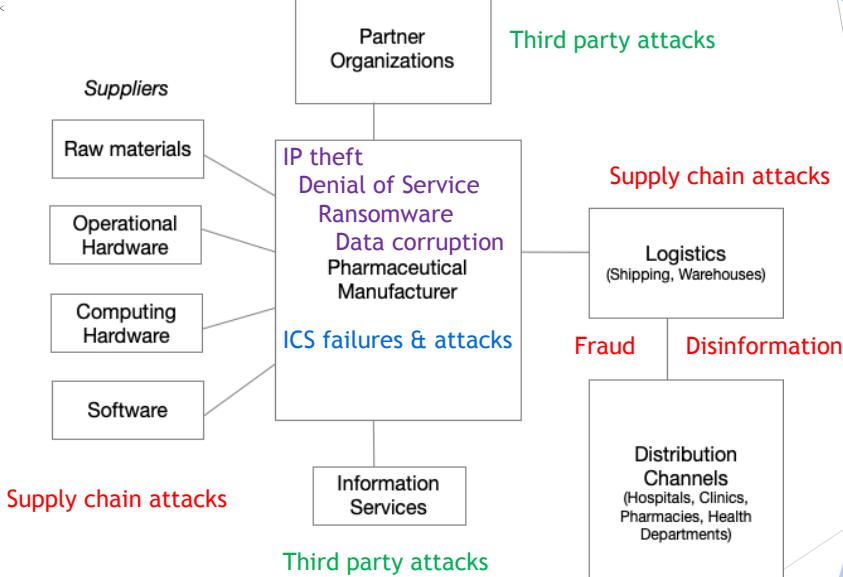


Attacking the Ecosystem

© 42TEK, Inc.

47

47



© 42TEK, Inc.

48

48



What's Happening Now

© 42TEK, Inc.

49

49



INTERPOL warns of organized crime threat to COVID-19 vaccines

2 December 2020

LYON, France – INTERPOL has issued a global alert to law enforcement across its 194 member countries warning them to prepare for organized crime networks targeting COVID-19 vaccines, both physically and online.

"The INTERPOL Orange Notice outlines potential criminal activity in relation to the falsification, theft and illegal advertising of COVID-19 and flu vaccines, with the pandemic having already triggered unprecedented opportunistic and predatory criminal behaviour. It also includes examples of crimes where individuals have been advertising, selling and administering fake vaccines."

<https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-organized-crime-threat-to-COVID-19-vaccines>

© 42TEK, Inc.

50

50

42TEK

Microsoft says three APTs have targeted seven COVID-19 vaccine makers

The three state-sponsored hacker groups (APTs) are Russia's Strontium (Fancy Bear) and North Korea's Zinc (Lazarus Group) and Cerium.

<https://www.zdnet.com/article/microsoft-says-three-apts-have-targeted-seven-covid-19-vaccine-makers/>

OPINION

The COVID-19 vaccine's logistics will be targeted. Vet the supply chain.

A burst of activity and demand will create openings for providers of transportation and warehouse facilities that may have poor security practices.

By Tony Pelli
Published Nov. 24, 2020

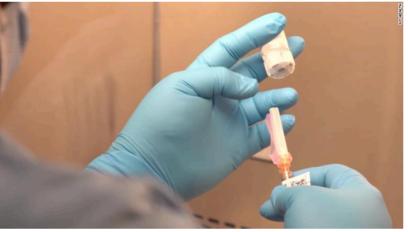
© 42TEK, Inc.
<https://www.supplychaindive.com/news/COVID-19-coronavirus-vaccine-logistics-preparing-for-theft-black-market/589223/>

51

42TEK

Hackers targeting key actors in vaccine supply chain

By Brian Fung, CNN
Updated 9:26 AM ET, Thu December 3, 2020



“Since September, attacks by unknown attackers have sought to compromise “select executives in sales, procurement, information technology and finance positions” at organizations responsible for ensuring that the vaccines are transported in the correct temperature-controlled conditions, IBM said in a blog post.”

© 42TEK, Inc.
<https://www.cnn.com/2020/12/03/politics/hackers-covid-vaccine/index.html>

52



Disinformation & Misinformation

- ▶ “Disinformation: (noun) False information deliberately and often covertly spread in order to influence public opinion or obscure the truth.”
- ▶ “Misinformation: (noun) Incorrect or misleading information inadvertently sent ...
- ▶ to influence public opinion or obscure the truth.”

© 42TEK, Inc.

<https://www.yonder-ai.com/resources/misinformation-vs-disinformation-whats-the-difference/>

53



 CISA
CYBER-INFRASTRUCTURE

MAY 2020



CISA INSIGHTS

COVID-19 Disinformation Activity

False and misleading information related to the coronavirus (COVID-19) are a significant challenge. This CISA Insight provides an overview of coronavirus disinformation and steps that can be taken to reduce the risk of sharing inaccurate information with your friends and family.

“...false claims about the origins of the virus in an attempt to shift blame overseas and divide free societies against themselves.”

“...false narratives that 5G technology suppresses immune systems and that 5G spectrum bands spread the virus.”

“...harmful suggestions to drink bleach or chlorine dioxide, to use vitamin C or boiled garlic, or that illicit drug activity can “cure” the virus.”

© 42TEK, Inc.

54



Social media is feeding the anti-vaccination movement

Research shows U.S. adversaries like Russia are pedaling fake health propaganda on sites like Twitter and Facebook.

By Julian Cardillo '14
Nov. 3, 2020

Disinformation about vaccines is on the rise on social media and leading to decreases in vaccination rates over time, according to a new study co-authored by Brandeis **politics** professor Steven Wilson. Now, he's calling on countries like the U.S. to step up the fight against bogus health-related propaganda showing up online.

The study, titled "**Social media and vaccine hesitancy**," which Wilson compiled with global health professor Charles Wiysonge of **Stellenbosch University in South Africa**, says much of the vaccine talk on sites like Twitter and Facebook consists of fake information pedaled by bots and promulgated by foreign adversaries like Russia.

<https://www.brandeis.edu/now/2020/november/social-media-vaccine-disinformation.html>

© 42TEK, Inc.

55



Another Key Data Piece

In addition to protecting vaccine production processes and the supply chain for getting vaccines to locations where they can be administered, there is the issue of **tracking who has been inoculated**. The task is daunting.

© 42TEK, Inc.

56

(CNN) — The Department of Defense released the first images of a Covid-19 vaccination record card and vaccination kits Wednesday.

- **"Vaccination clinics will also be reporting to their state immunization registries what vaccine was given, so that, for example, an entity could run a query if it didn't know where a patient got a first dose."**
- **"...many places are planning to ask patients to voluntarily provide a cell phone number, so they can get a text message telling them when and where their next dose is scheduled to be administered."**
- **"Every dose administered will be reported to the US Centers for Disease Control and Prevention..."**

If we only had a national patient identifier, like many developed countries...

keep track of Covid-19 shots, said Dr. Kelly Moore, which is supporting frontline workers who will administer

[/health/covid-19-vaccination-kit-record-card/index.html](https://health/covid-19-vaccination-kit-record-card/index.html)

COVID-19 Vaccination Record Card

Please keep this record card, which includes medical information about the vaccines you have received.
Por favor, guarde esta tarjeta de registro, que incluye información médica sobre las vacunas que ha recibido.

Last Name	First Name	MI	
Date of birth			
Patient number (medical record or IIS record number)			
Vaccine	Product Name/Manufacturer Lot Number	Date	Healthcare Professional or Clinic Site
1 st Dose COVID-19		/ /	/ / yy
2 nd Dose COVID-19		/ /	/ / yy
Other		/ /	/ / yy
Other		/ /	/ / yy

57

(CNN) — The Department of Defense released the first images of a Covid-19 vaccination record card and vaccination kits Wednesday.

Vaccination cards will be used as the "simplest" way to keep track of Covid-19 shots, said Dr. Kelly Moore, associate director of the Immunization Action Coalition, which is supporting frontline workers who will administer Covid-19 vaccinations.

<https://www.cnn.com/2020/12/02/health/covid-19-vaccination-kit-record-card/index.html>

- **What if person does not have a medical record number and wants to exercise their right to opt out of the state's Immunization Information System?**
- **What happens if the person switches care provider or moves between states during the period between the 1st and 2nd dose?**
- **How will counterfeiting and other fraud be deterred/prevented?**

If we only had a national patient identifier, like many developed countries...

COVID-19 Vaccination Record Card

Please keep this record card, which includes medical information about the vaccines you have received.
Por favor, guarde esta tarjeta de registro, que incluye información médica sobre las vacunas que ha recibido.

Last Name	First Name	MI
Date of birth		
Patient number (medical record or IIS record number)		
Vaccine	Product Name/M Lot Number	Date / Fecha
1 st Dose COVID-19	Covid-19 vaccine Vacuna contra el COVID-19	/ / mm dd yy
2 nd Dose COVID-19		/ / mm dd yy
Other		/ / mm dd yy
Other		/ / mm dd yy

Reminder! Return for a second dose!
¡Recordatorio! ¡Regrese para la segunda dosis!

Bring this vaccination record to every vaccination or medical visit. Check with your health care provider to make sure you are not missing any doses of routinely recommended vaccines.

For more information about COVID-19 and COVID-19 vaccine, visit cdc.gov/coronavirus/2019-nCoV/index.html.

You can report possible adverse reactions following COVID-19 vaccination to the Vaccine Adverse Event Reporting System (VAERS) at vaers.hhs.gov.

Lleve este registro de vacunación a cada cita médica o visita médica. Consulte con su proveedor de atención médica para asegurarse de que no le falte ninguna dosis de las vacunas recomendadas.

Para obtener más información sobre el COVID-19 y la vacuna contra el COVID-19, visite espanol.cdc.gov/coronavirus/2019-nCoV/index.html.

Puede notificar las posibles reacciones adversas después de la vacunación contra el COVID-19 al Sistema de Notificación de Reacciones Adversas a las Vacunas (VAERS) en vaers.hhs.gov.

58



More on CDC Databases

Covid-19 Vaccine Safety Efforts to Feature App Tracking of Vulnerable Groups; Measures to track first cohort of people to get the coronavirus shot aim to fill gaps in existing vaccine surveillance

Loftus, Peter . Wall Street Journal (Online) ; New York, N.Y. [New York, N.Y]05 Nov 2020.

[ProQuest document link](#)

FULL TEXT

Government health officials and drugmakers plan to roll out extra tools to detect whether Covid-19 vaccines cause any serious side effects once the shots are cleared for widespread use, aiming to fill gaps in existing safeguards given the expected speed and scope of the rollout.

The measures include surveys tracked through a smartphone app developed by the Centers for Disease Control and Prevention and special monitoring for groups including pregnant women and the elderly, according to health officials and company executives involved in the plans.

© 42TEK, Inc.

59

59



COVID-19 Vaccines Cybersecurity Summary

- ▶ Complex Ecosystem
- ▶ Data-Intensive Manufacturing and Distribution
- ▶ Industrial Control Systems Cybersecurity ≠ IT Cybersecurity
- ▶ Attacks and Disinformation Already Occurring

© 42TEK, Inc.

60

60



We are at a moment in history.

“Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning.”

-- Winston Churchill (November 10, 1942)

© 42TEK, Inc.

61

61



42TEK, Inc.

*Program management & product development
for data security, healthcare systems,
critical infrastructure, and
electronic payments.*

Q & A

David Snyder, MBA, PE, CISSP, CSM

www.42tek.com david@42tek.com

62