





Andrey Zolotavin

Snr. RTS Engineer/Specialist

KOC



Industrial cybersecurity as key
for sustainable production

Bill Gates – rules of the technology

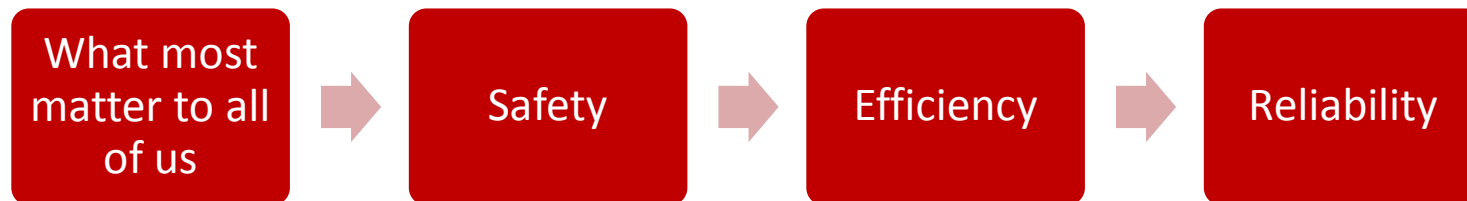


The first rule is that **automation** applied to an efficient operation will magnify the efficiency.

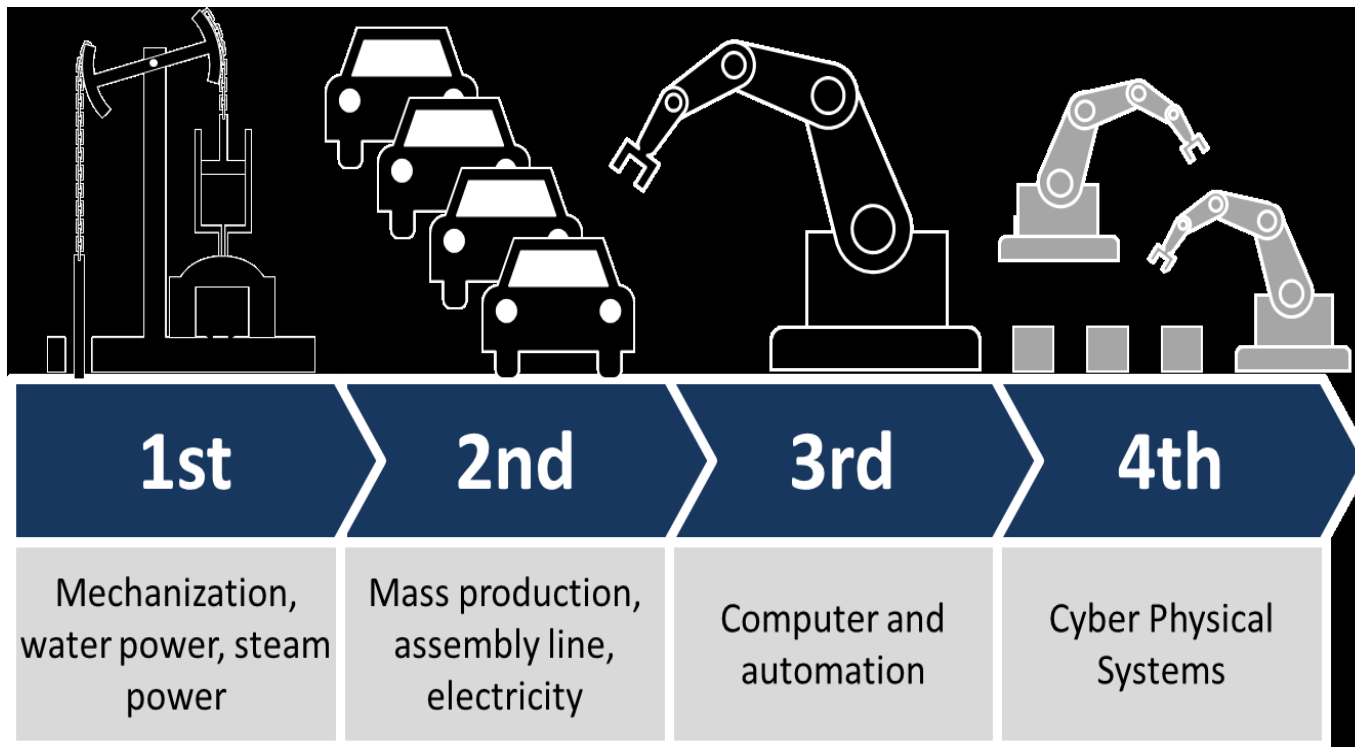
The second is that **automation** applied to an inefficient operation will magnify the inefficiency.

Industrial cybersecurity as key Enterprise risk

- Industrial technology into Industry 4.0
- Cyber risks in Enterprise Risk management
- Issues with industrial cybersecurity
- Differences and commons between Industrial and traditional cybersecurity
- Risk mitigation in cyber sphere

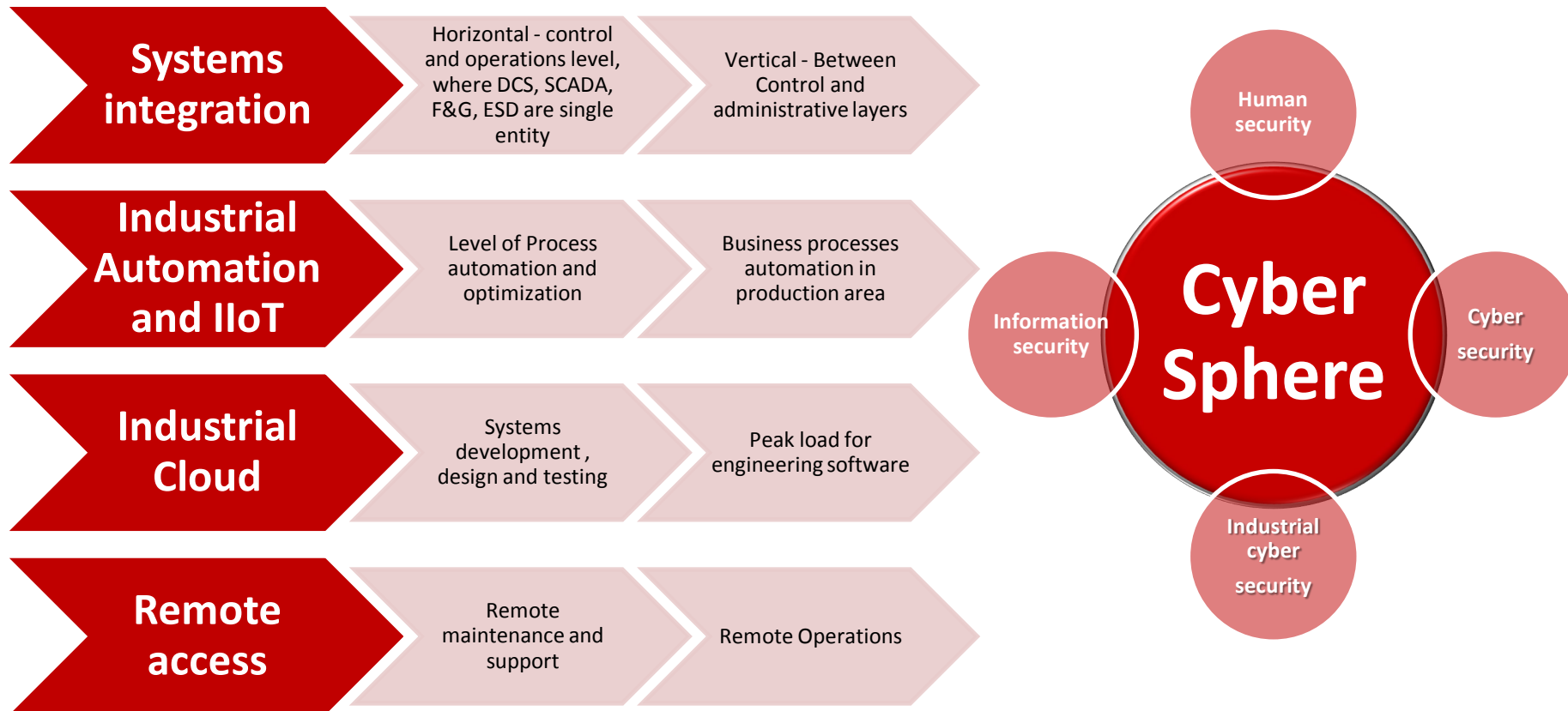


Industry 4.0 – digital transformation



- Competitiveness accomplished by efficient , agile and flexible production.
- Cannot be achieved without ever increased automation, as in process and business life
- Merge machines with intelligence

Industrial technologies into Industry 4.0



Cyber sphere risks vs Cybersecurity



- **Industrial cybersecurity** – more vital than corporate cybersecurity
- **Corporate cybersecurity** – can contribute to Industrial, but might limit business and production effectiveness
- **Information security** - reduce information leakages from industrial systems
- **Human Security** - prevent from wrongdoing and protect employee
- Many policies set from formal perspective
- Complex Cyber sphere approach – can address enterprise risks for sustainable production

Issues with industrial cybersecurity



- Non systematic efforts due to typical very complex architecture and systems variety
- Frequently not aligned efforts
- Tense relations between Production/Operation and IT departments
- Automation companies selling cyber security as additional service
- Rare cases of established Industrial IT units
- Typical case – level of industrial system cybersecurity is unknown
- Policies are very vague, no detailed instructions are set for the Industrial systems
- Wide usage of commercial version of known OS, with lot of vulnerabilities
- **Most important – un-orchestrated efforts are very expensive and improve cybersecurity slightly from Industry perspective.**

Cyber risks in Enterprise Risk management

- Automation and integration between vertical and horizontal layers amalgamate our Production and business systems into single entity
- This single entity can name as Cyber sphere, as it is based on computerized technologies connected with measurements and controls
- Process disruption vs Cyber sphere risk
- Shall we stop development?
- Typical risks channels are:
 - Human - various styles hackers, disgruntled employees knowledge.
 - Network – as means of accessing and manipulate with targeted systems
 - Control and Information systems – when system is targeted by Human or network
- Machine never harms other machine, if not programmed by human to do so

Industrial Cyber Sphere risk bigger, as can cause process disruption.

No! Available tools and methods helping to mitigate risks

Risks mitigation in cyber sphere



- Level of risk to your country and industry
 - Periodic/event based exercise, which can be automated
- Informing on your Cyber readiness
 - Is it better to keep secret? Or reveal it ?
 - “strong muscle” attitude
- Don’t rely on single entity
 - Mistakes of over centralization
 - Attack vectors – distribution of targets
 - Setting decoy targets
- Increase use of hardcoded technologies
 - In key areas between main operation zones/units
 - Data diodes
 - Hardcoded on non-rewritable media

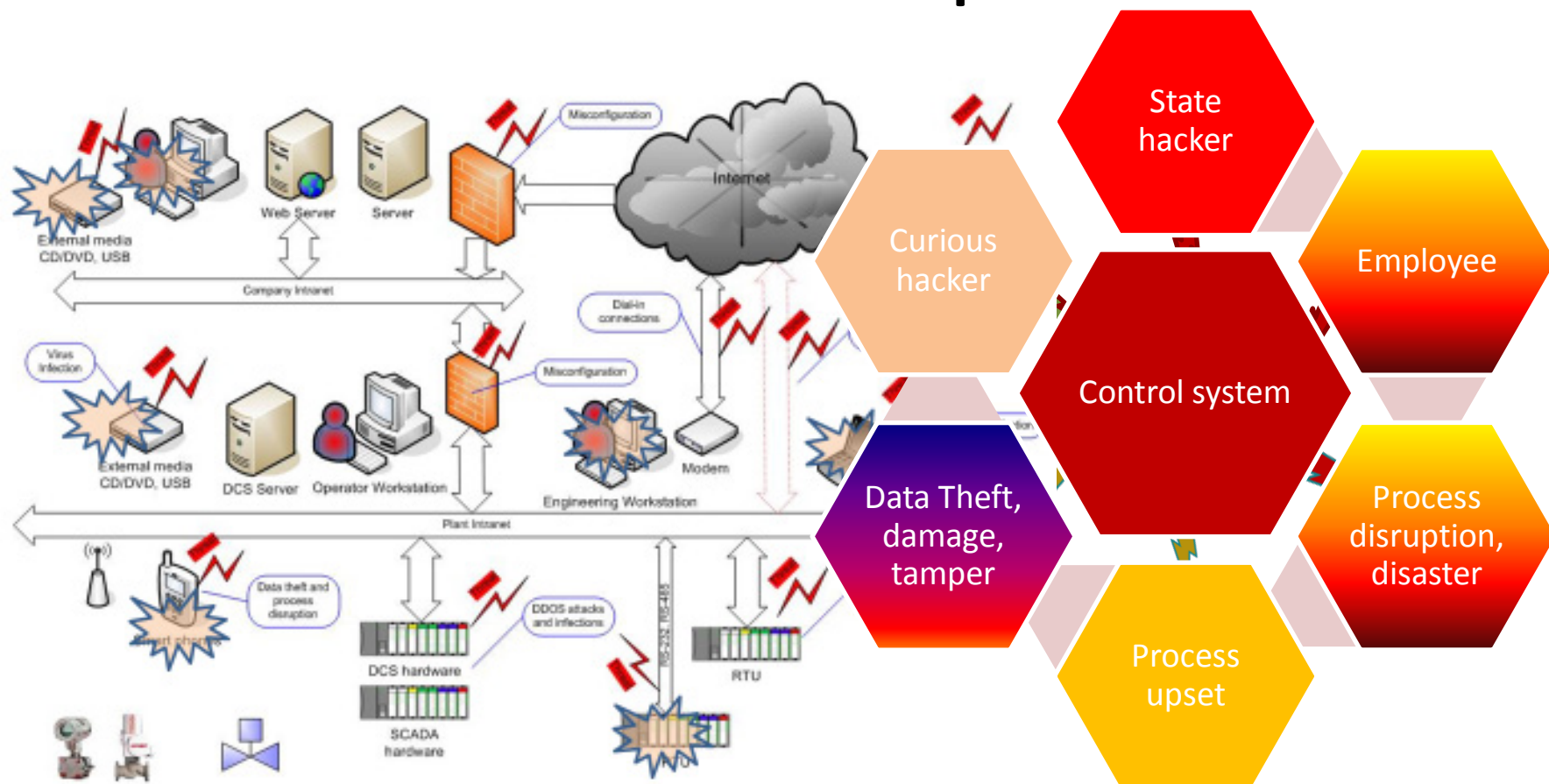
Set Industrial IT division within Operation/Maintenance

- Help to reduce overall decision process
- Shall consist Control and IT experts in one unit
- Help fast response in cyber events on 24/7 base

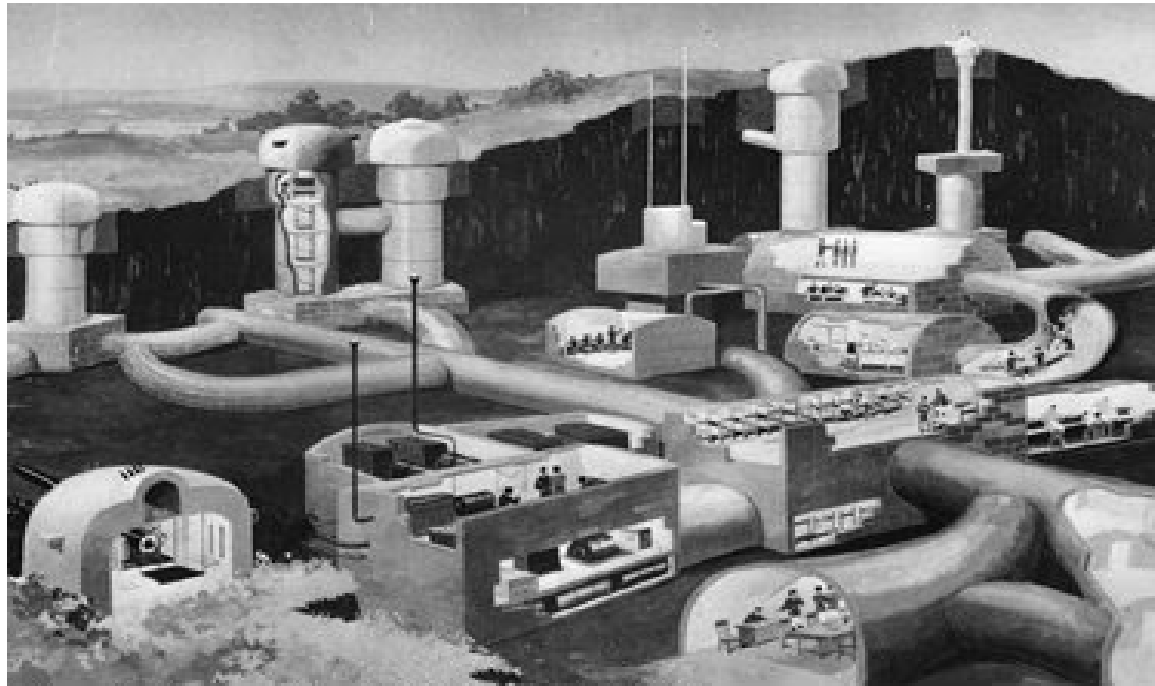
- Change or set industrial practices

- Every Industrial system configuration rules
- System maintenance procedures and practices
- System images for faster recovery

Attack vs impact



Maginot line



©Bowring Cartographic, 1997 (Tel. 703-527-7828)

Built at enormous expense (over 3 billion francs), the Maginot line was not a continuous fortification but a series of strong points.

There are 142 fortresses, 352 casemates, 78 shelters, 17 observatories and around 5,000 blockhouses in the entire Maginot Line. Pictured above is an fortress.

Germans decided not to smash through the Maginot. They just bypass it and invaded France. **Maginot line remain intact**



Thanks for
Attention