Cyber-Physical Risks: When Data Attacks Meet Physical Stats and Facts

FACTS

- **Compromised Control Systems:** Cyberattacks on industrial control systems can alter equipment behavior, leading to unsafe movements, shutdown failures, or uncontrolled energy release.
- **Unauthorized Remote Access:** Intruders gaining access to connected equipment or safety systems can override controls and disable protections without worker awareness.
- **Sensor and Data Manipulation:** Altered or false data from sensors can mislead operators, resulting in unsafe decisions and delayed hazard recognition.
- **Shutdown and Safety System Failure:** Attacks targeting safety interlocks or emergency shutdown systems can prevent critical protections from activating during incidents.
- **Delayed Response to Hazards:** Disrupted communication systems can slow emergency response, increasing the severity of incidents.
- **Dependence on Connected Systems:** Increased reliance on digital systems means failures or breaches can directly impact physical operations and worker safety.
- **Human Error Under Cyber Stress:** Confusion during cyber incidents can lead to incorrect actions, increasing the risk of physical injury.

STATS

- In the United States, **approximately 32% of industrial organizations reported cyber incidents affecting operational technology (OT) systems**, increasing the risk of physical safety impacts (IBM Security & industry reports, 2023–2024).
- U.S. data shows that **over 40% of cyberattacks targeting critical infrastructure involve attempts to disrupt physical operations**, including energy, manufacturing, and utilities sectors (CISA and DHS reports, 2022–2024).
- In North America, around 25% of organizations reported that cyber incidents had direct operational or safety-related consequences, including equipment shutdowns or unsafe conditions (SANS Institute, 2023).
- U.S. reports indicate that **over 50% of industrial cybersecurity incidents involve compromised control systems**, which can directly affect machinery and worker safety (Dragos Industrial Cybersecurity Report, 2023–2024).
- In Canada, approximately 30% of critical infrastructure organizations reported cybersecurity incidents impacting operations, including disruptions that could affect worker safety (Public Safety Canada, 2022–2024).
- U.S. data shows that **ransomware attacks accounted for over 20% of cyber incidents in industrial sectors**, often causing shutdowns and unsafe operating

conditions (FBI IC3 Report, 2023).