आज़ादी का अमृत महोत्सव

G20 भारत 2023 INDIA

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF HOUSING AND URBAN AFFAIRS

स्वच्छ भारत
एक कदम स्वच्छता की ओर

CYBERSECURITY

D K SINHA

CEO/MML3 (O&M)/DMRC

16th Urban Mobility India Conference & Expo 2023

CONTEXT

1. Computer systems footprint is ever increasing in Railway network - in the control centres, drivers' cabins, track equipment, traveller information systems.
2. Railway digitization brings added intelligence to railway networks, both in terms of their development and operational needs and of their maintenance requirements.
3. Computer based metro train control system operate as a closed network – taken as a basis for safety assessment before approving system for use. This closed network assumption is no longer sustainable or realistic.
4. We have entered the era of cybersecuity: in the railway world, the attacks are still rare; as the network modernize, exposure increase apace.

INSTANCES OF BREACH

1. Ransomware, DDOS, Vulnerability exploitation. Majority of cyber attack targeted railways IT system affecting ticketing system, mobile app and passenger information system.
2. DDOS attack in 2017 on Swedish transportation network – customers during this time were unable to make reservation or get updates about delays.
3. Ransomware: In Mar 22 Italian state railway faced a ransomware attack where customers were unable to buy tickets.
4. Service disruption on Danish railway network in Oct ’22 when safety critical IT system affected through cyber attack.
5. Post Ukraine war, DDOS attack on East European railways have been reported mostly affecting their ticketing services.

OPERATOR NEEDS

1. Secured connection for onboard maintenance in real time, secured communication between train and trackside, secured links between train and passengers.
2. Secured gateway between information technology and operation technology – keeping both data security and system security.
3. IoT presently is being used for collecting data from sensors. In future when command and control will be attached, then security will have to be enhanced.
4. Driverless trains will have more attack surface and will require extra risk analysis.
5. Security measures should not compromise efficient operation of the system –criticality of response time.

CHALLENGES

1. Incompatibility of railway systems and computer systems: product lifetime – IT 3 to 5 years; Railway 10-20 years.
2. Railway systems development follow design freeze.
3. Cyber critical equipment will require to be updated more regularly than other train components/ equipments.
4. Standards for railway cybersecurity are evolving.
5. Insurers have limited historical data.

FRAMEWORK FOR BUILDING RESILIENCE

- Risk analysis from the day the project is taken up –lessons from similar industry viz aerospace.
- Addressing the Key processes along the entire value chain. Data security as well as System security.
- Secure the weakest link; defence in depth.
- Legacy product – mitigation; newer product – built in cybersecurity features.
- Grant least privileges, Avoid redundancies and overlapping of functionalities, Triple A.
- Load Balancing, Mirroring.

FRAMEWORK FOR BUILDING RESILIENCE

- Use of Standards: IEC 62443 -a standard for secure development of products used in Industrial automation and control system. Railway specific- Cenelec TS50701.
- Business continuity planning if mission critical system go down.
- Continuing task –engineered and in collaboration between suppliers, customers and regulatory agencies.
- Auditing, Training
- Insurance

BEST PRACTICES

Few Best practices as per information available in public domain:

- CBTC OEMs have started system and product development with in-built cybersecurity features.
- Separation of IT and OT system through unidirectional gateway.
- Cybersecurity policy at organization level and regular auditing.
- Centralized database creation through NCIIPC.

THANK YOU

FOR

GIVING ME AN OPPORTUNITY

FOR SHARING MY VIEWS

16th Urban Mobility India Conference & Expo 2023