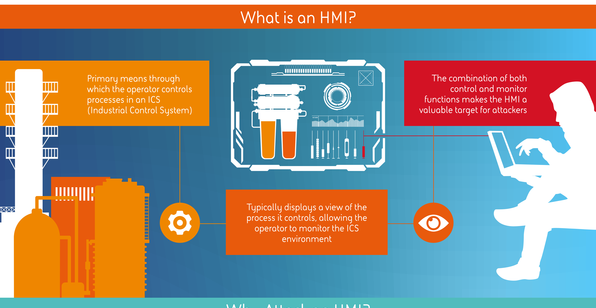
Digital Intelligence

BAE SYSTEMS

Helping Protect the Human Machine Interface

A Human Machine Interface (HMI) allows operators to interact with equipment which enables industrial processes to happen. It is also a valuable target for cyber threat actors. What can be done to help?

What is an HMI?



Why Attack an HMI?

Attackers may be motivated to target industrial systems to achieve the following two main goals

To disrupt industrial processes

To conduct industrial espionage

For both of these goals, HMIs present an attractive target. The boxes below discuss techniques which an attacker may employ against an HMI in order to achieve one or both of these goals.

Manipulation

An attacker could connect remotely to the HMI and manipulates industrial processes through its interface

Enumeration

An attacker can harvest architectural diagrams and industrial process information for reconnaissance to enable a future disruptive attack, or for industrial espionage purposes

Connection

An HMI could be used to gain a foothold in the network, which could provide attackers an opportunity to pivot to other systems

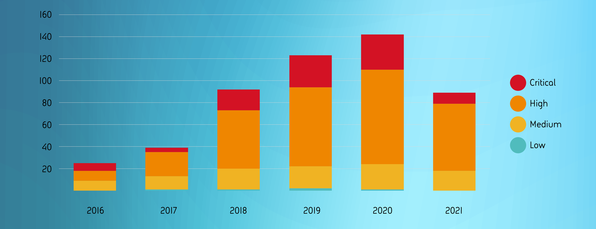
Deception

Attackers may deceive the operator by ensuring that the HMI shows a process operating as usual when this is not the case

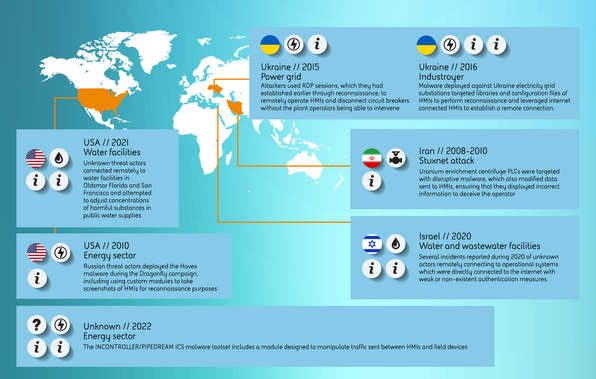
HMI Vulnerabilities

Since 2016 the number of CVEs associated with a selection of identified HMI products has been trending upwards

Source:
National Vulnerability Database: https://nvd.nist.gov/



Noteworthy Attacks Involving HMIs



Ukraine // 2015
Power grid
Attackers used RDP sessions, which they had established earlier through reconnaissance, to remotely operate HMIs and disconnect circuit breakers without the plant operators being able to intervene

Ukraine // 2016
Industroyer
Malware deployed against Ukraine electricity grid substations targeted libraries and configuration files of HMIs to perform reconnaissance and leveraged internet connected HMIs to establish a remote connection.

USA // 2021
Water facilities
Unknown threat actors connected remotely to water facilities in Oldsmar Florida and San Francisco and attempted to adjust concentrations of harmful substances in public water supplies

Iran // 2008-2010
Stuxnet attack
Uranium enrichment centrifuge PLCs were targeted with disruptive malware, which also modified data sent to HMIs, ensuring that they displayed incorrect information to deceive the operator

USA // 2010
Energy sector
Russian threat actors deployed the Havex malware during the Dragonfly campaign, including using custom modules to take screenshots of HMIs for reconnaissance purposes

Israel // 2020
Water and wastewater facilities
Several incidents reported during 2020 of unknown actors remotely connecting to operational systems which were directly connected to the internet with weak or non-existent authentication measures

Unknown // 2022
Energy sector
The INCONTROLLER/PIPEDREAM ICS malware toolset includes a module designed to manipulate traffic sent between HMIs and field devices

Recommendations

Industrial environments should be physically or logically segregated from IT networks, with DMZ and firewalls in place appropriately, and HMIs only accessible from within the industrial environment

Review remote access implementations. Ensure they are configured securely

Implement network detection, asset and vulnerability enumeration tools with care

Employ a risk-balanced approach to patching – considering security, safety and operational factors

Locate HMIs in secure areas, with physical security and access control measures in place to ensure that they are only operated by trained and authorised personnel

Subscribe to relevant threat intelligence feeds to inform your strategic risk management processes and security operations

BAE SYSTEMS

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

learn@baesystems.com baesystems.com/threatintel twitter.com/BAES_Digital