LSI listens

CYBERSECURITY

## How We Work

- To support our clients' cybersecurity needs, LSI's team of experts starts by listening, learning, and understanding our clients' processes and business drivers.
- By combining that understanding with our knowledge and experience of ICS/OT cybersecurity frameworks, industry regulations, and acceptable practices to assess the environment's cybersecurity posture, we can implement the needed remediation.
- The result is a custom solution, tailored to the needs of that client's process and environment, that reduces the attack surface and hardens the environment against cyber threats.

## Contact LSI

*Let's start a conversation. Call or email our cybersecurity experts today.*


***877-735-6905***

***sales@logicalsysinc.com***

***www.logicalsysinc.com***


# What is an Industrial DMZ?

### How does it protect my manufacturing assets and network from attacks on my enterprise network?

In today's dynamic threat landscape, many standards and regulatory bodies agree that organizations should segment their enterprise business networks from industrial plant networks to improve their cyber security posture. However, organizations have become more dependent on the exchange of data between enterprise and industrial environments, so industrial security standards (e.g., NIST 800-82, ISA/IEC 62443, etc.) and regulatory entities recommend the use of an Industrial Demilitarized Zone (IDMZ) to mitigate security risks.

## The Industrial DMZ

An IDMZ is an additional network security layer between the Enterprise IT and OT (Operational Technology) networks. The IDMZ provides a buffer zone between untrusted security zones (e.g., Enterprise) and trusted security zones (e.g., Industrial) to broker the connections so that no direct network communications are allowed between untrusted and trusted security zones. The IDMZ infrastructure consists of various network devices, including but not limited to the following: security appliances/firewalls, IDMZ servers, virtual private network (VPN) server, switches, and routers.

## Designed to Protect

- Zones and Conduits - Critical assets are segmented into separate security zones, and conduits are utilized to restrict network access based on organizational security policies.
- Segmentation - Multiple security zones are established in the IDMZ to allow servers with different security classifications to be logically positioned in different security zones.
- Zero Trust - All network traffic to and from the industrial security zones is denied by default and allowed only by exception.
- Function as Buffer Zone - All traffic originating from trusted or untrusted networks terminates in the IDMZ, thus allowing it to function as buffer zone between trusted and untrusted zones.
- Design for Industrial Control System (ICS) Autonomy - The IDMZ is designed to allow ICS services to operate autonomously, such that process operations would continue if the IDMZ network segment has been disconnected to support Incident Response (IR), as shown below.