

C5I®

Digitalization Partner



Claudio S. Malavenda  
DD/CDS use Cases

Commercial in Confidence

# CHI SIAMO



Siamo uno studio di ingegneria integrata con una solida rete di partnership formata da PMI innovative che offre servizi di progettazione e gestione programmi «chiavi in mano».





# Il Contesto

# MDO e il Bisogno della connessione



Con l'introduzione delle **Operazioni Multi-Dominio (MDO)**, si è aperta la strada a una collaborazione estesa con partner civili durante lo svolgimento delle Course of Action (COA).

Questa strategia riconosce l'importanza di **integrare** le capacità tra diversi settori per una gestione più efficace delle operazioni.

Le MDO richiedono il trasferimento sicuro di dati tra il settore militare e quello civile per migliorare la consapevolezza situazionale e ottimizzare l'uso delle risorse. Diventa cruciale garantire un'interoperabilità efficiente tra i sistemi militari e le reti civili



# CEMA nelle MDO



Le **CEMA (Cyber and Electromagnetic Activities)** sono una componente chiave delle MDO, poiché permettono la connessione e l'integrazione di dati provenienti da strati dello spettro elettromagnetico e del cyberspazio, che altrimenti sarebbero **invisibili** (non-material settings).



Questo include segnali, frequenze e dati criptati che, se raccolti e analizzati correttamente, offrono una consapevolezza situazionale unica. Grazie alle CEMA, è possibile correlare informazioni da diverse fonti per ottenere una visione globale e precisa dell'ambiente operativo, sfruttando e acquisendo obiettivi nei domini "non materiali".

# WARGAMING e connessione ai C&C



I sistemi di wargaming hanno acquisito crescente rilevanza tattica, non solo per pianificare in fase di Military Decision-Making Process (MDMP), ma anche per allineare piani durante la loro esecuzione.

Grazie all'integrazione di simulazioni avanzate e analisi in tempo reale, questi sistemi permettono di adattare le strategie operative rapidamente in risposta a cambiamenti sul campo. Ciò consente una maggiore flessibilità e precisione, migliorando la consapevolezza situazionale e ottimizzando le decisioni in corso d'azione, anziché limitarle alla fase di pianificazione iniziale.



# Il Crescente Bisogno di Automazione



Con l'aumento della complessità operativa e dei volumi di dati, l'**automazione** sta diventando una componente fondamentale. I sistemi automatizzati di C&C migliorano la velocità decisionale, consentendo analisi in tempo reale e azioni rapide.



L'automazione riduce il carico cognitivo umano, ottimizza l'efficienza e limita gli errori in contesti noti, ma non può soppiantare l'uomo nella Versatilità e in situazioni NON note.

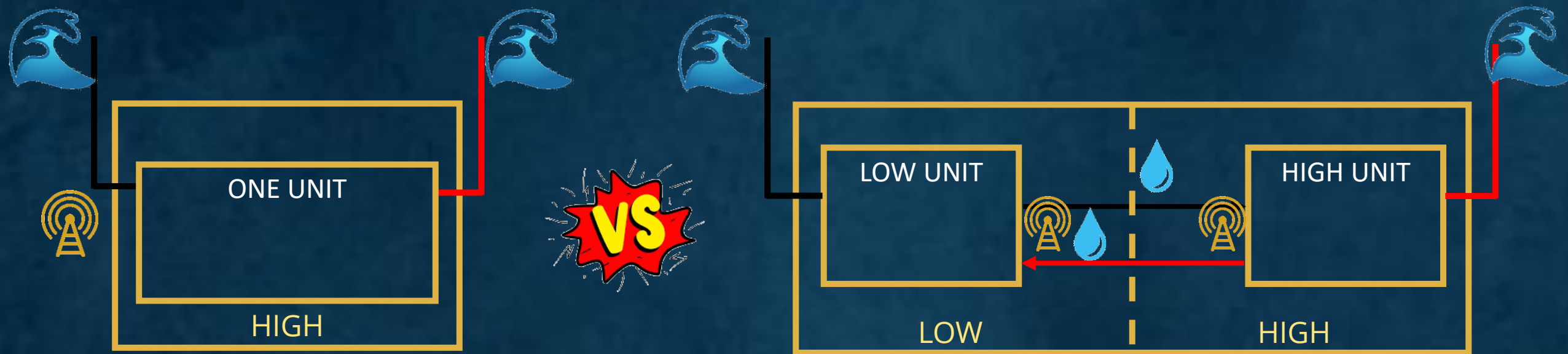


# Overview del Problema

# Cross Domain Evolution in Italia



# CROSS DOMAIN GATEWAY – Data flow



Il tipico CDS interfaccia l'intero flusso del lato LOW.

Se il lato basso è una connessione radio, il canale sarà inondato da un'enorme quantità di dati

Questo approccio architettonico può avere un'unità dedicata in LOW e una in HIGH. La quantità di dati scambiati è limitata ai dati da scambiare tra i domini

# TEMPEST – EM



Nel contesto del Cross Domain, dove sistemi con classifiche diverse interagiscono, le considerazioni TEMPEST non devono riguardare solo le emissioni elettromagnetiche verso l'esterno, ma anche il rischio di contaminazione EM **TRA** componenti **interni** con livelli di classificazione differenti.

La protezione deve essere progettata per prevenire che le informazioni classificate trasmesse all'interno dell'apparato possano interferire con elementi non classificati, creando potenziali vulnerabilità. Questo richiede un approccio rigoroso alla schermatura interna e alla segregazione dei percorsi EM per garantire la sicurezza delle informazioni.

Dormiresti tranquillo appena fuori casa se al suo interno ci fosse un festa scatenata?

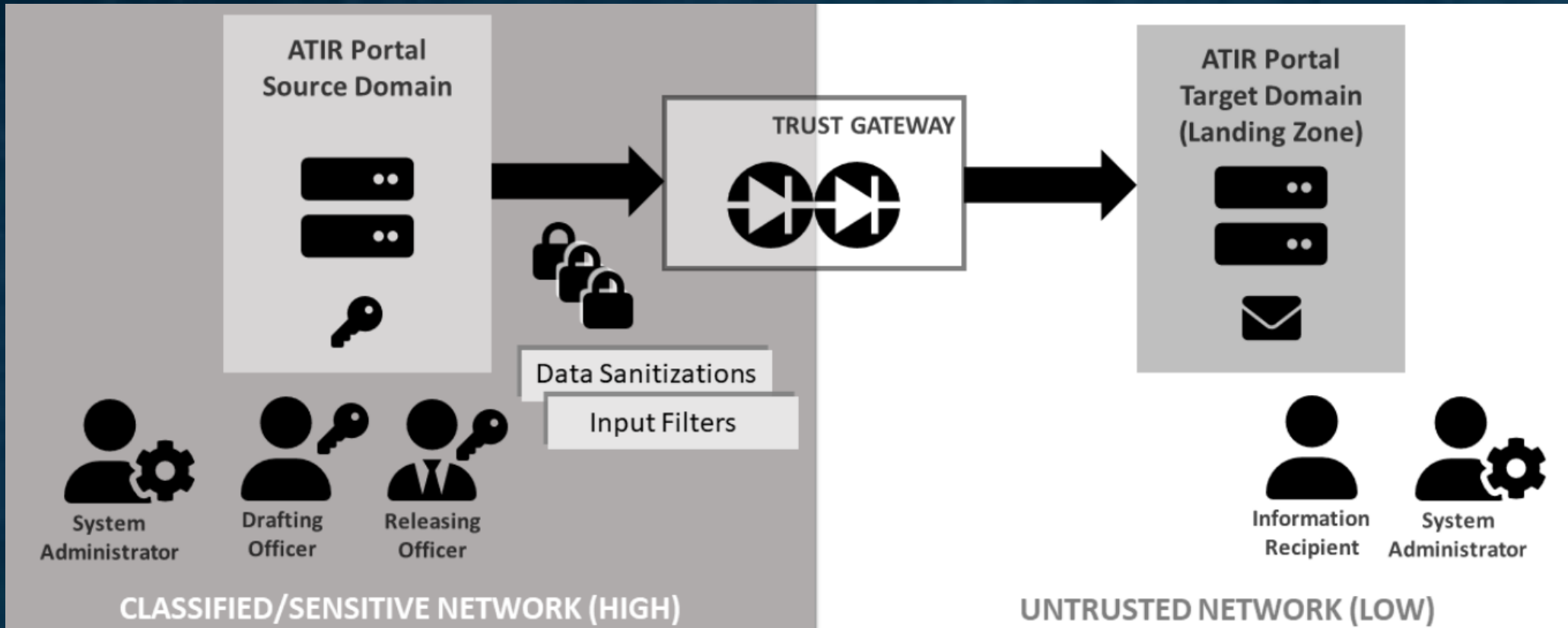




# Casi d'USO

# Dati Non Strutturati

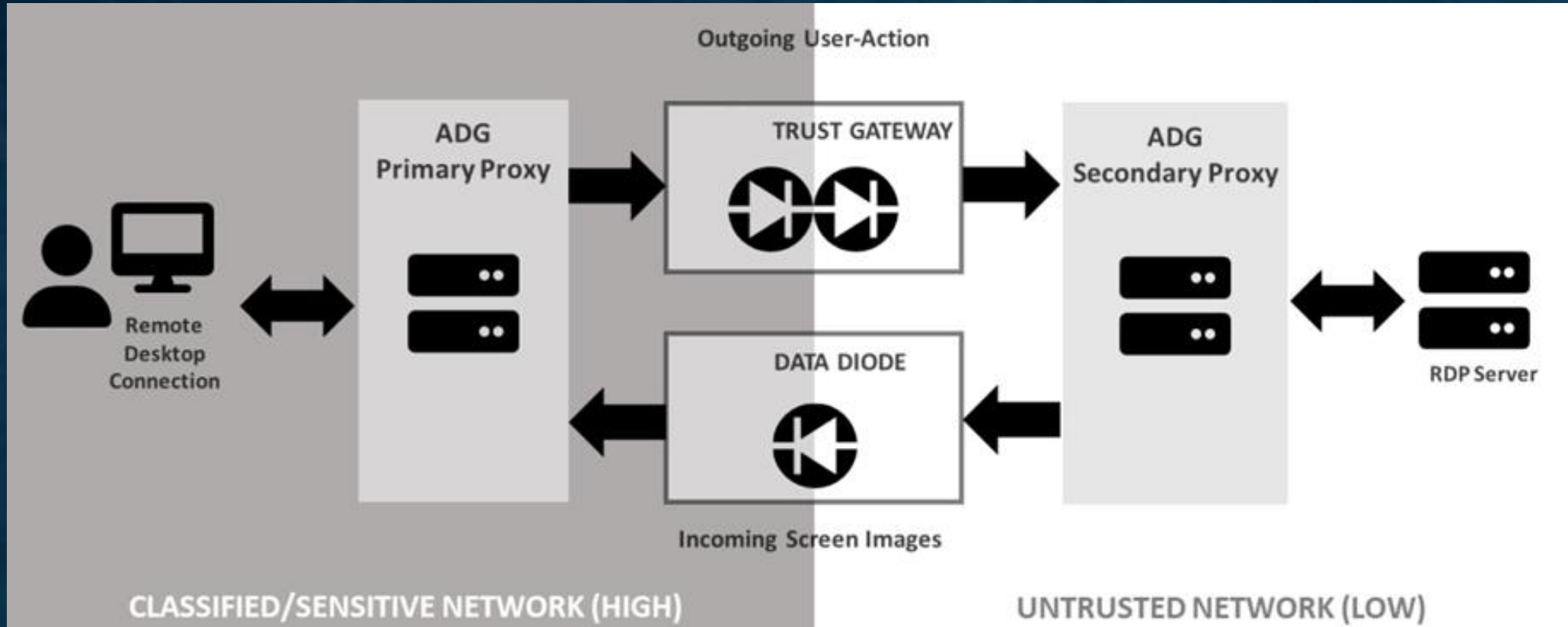
- E' possibile scambiare anche di dati non strutturati, utilizzando 'etichette' (es. STANAG 4774/8)
- Digital signature su tutte le transazioni



Rilascio delle informazioni a due fattori dalla rete HIGH.

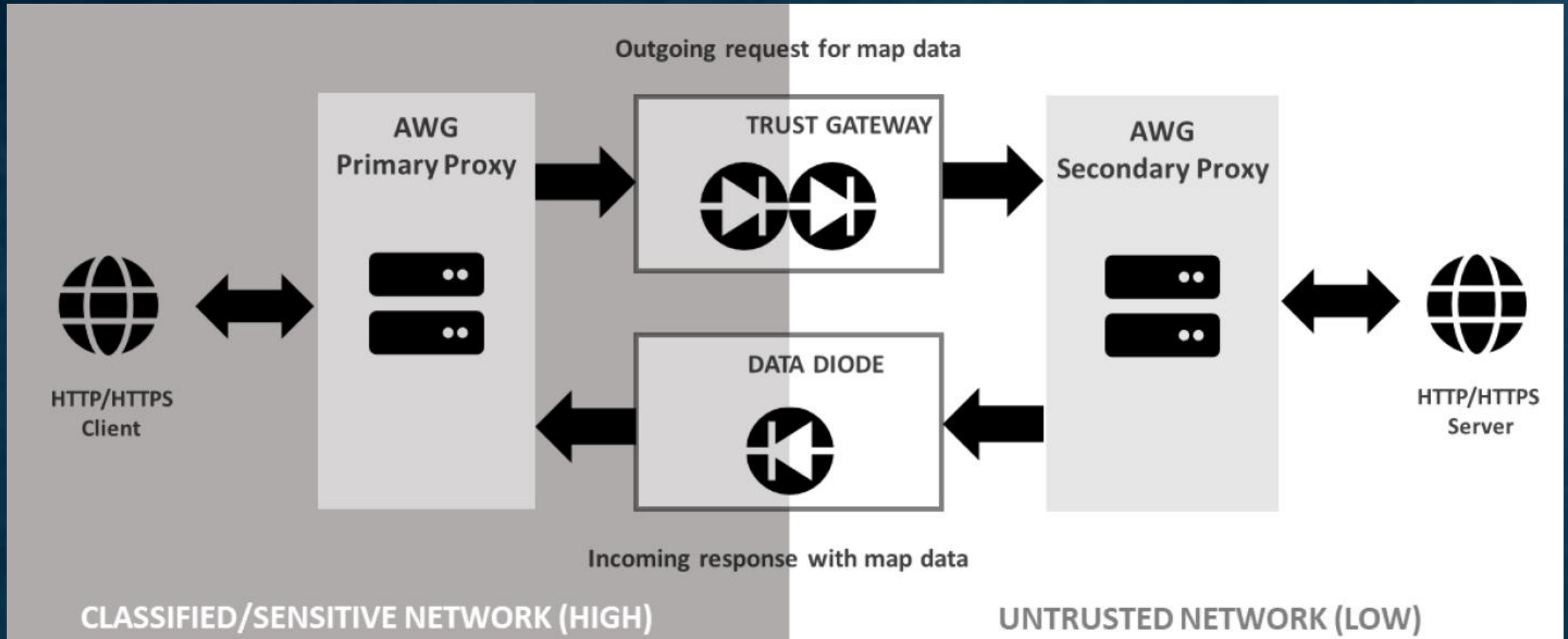
In questo caso i dati non strutturati possono essere organizzati, sanitizzati e filtrati con policy configurabili

# Caso d'uso – Remote Desktop



Accedo ad una postazione «LOW» da una Postazione «HIGH»

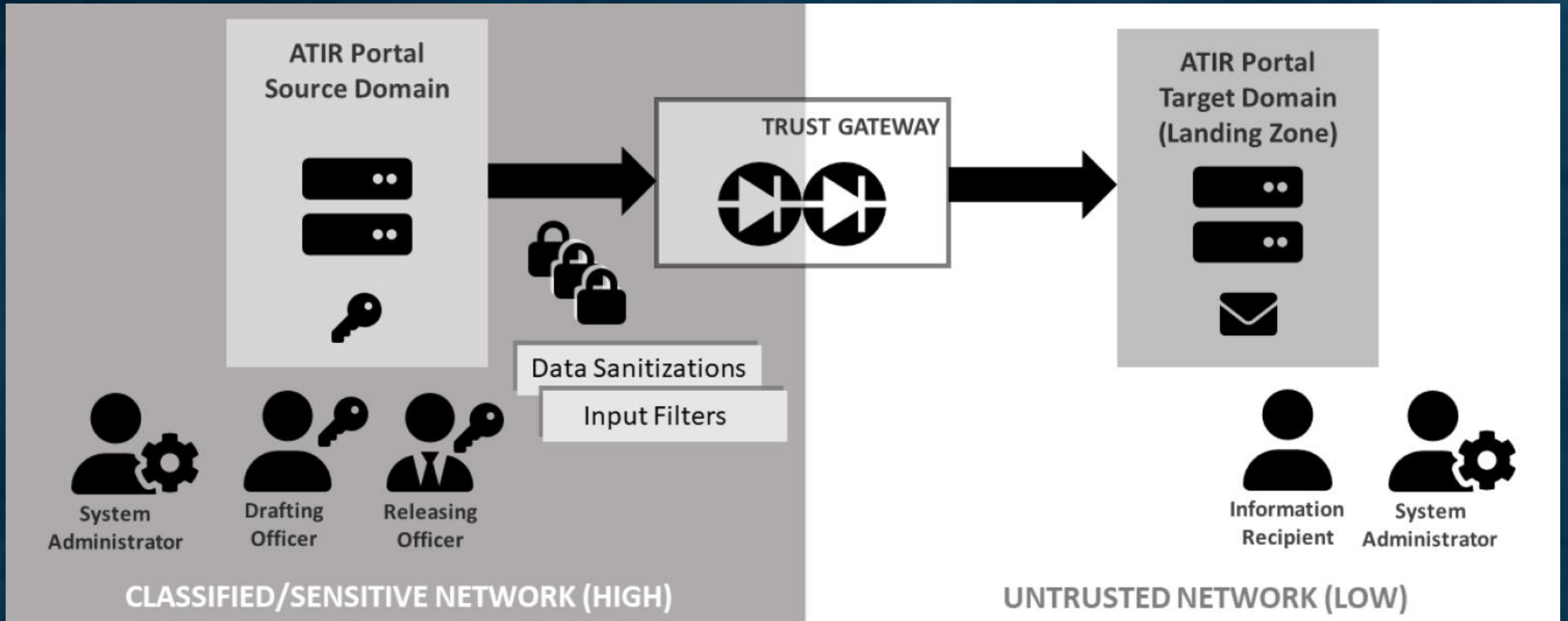
# Caso d'uso – Web Gateway



Accesso HTTP/HTTPS da una rete HIGH. Accedo a Web services o Web Map ottenendo aggiornamenti trasferiti in modo sicuro da LOW a HIGH

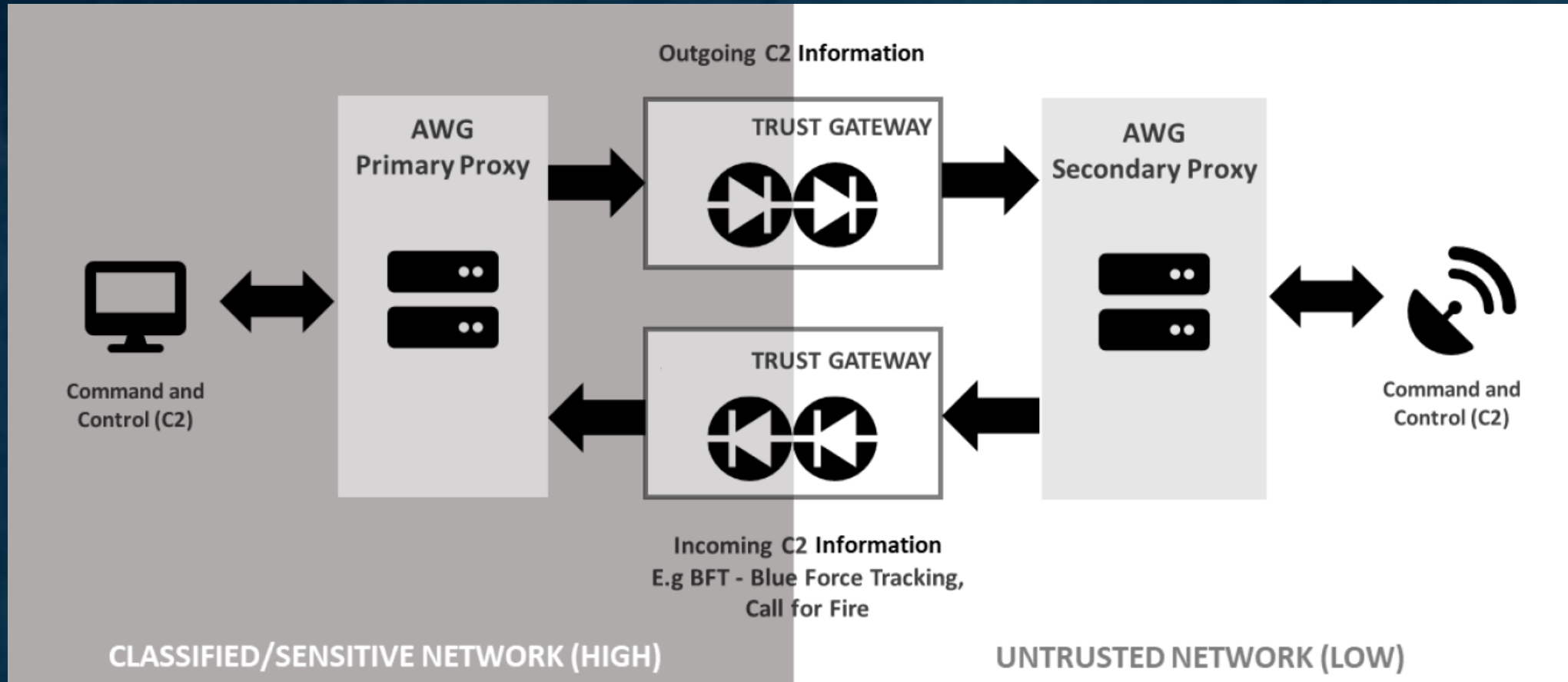
# Caso d'uso

## Rilascio Informazione da rete HIGH



Rilascio a due fattori di dati da una rete HIGH verso una LOW

# Installazione Rugged su veicoli



Abilita lo scambio di informazioni strutturate tra diversi sistemi di C&C, da LOW a HIGH e da HIGH a LOW

# USE CASE – GOV - 1



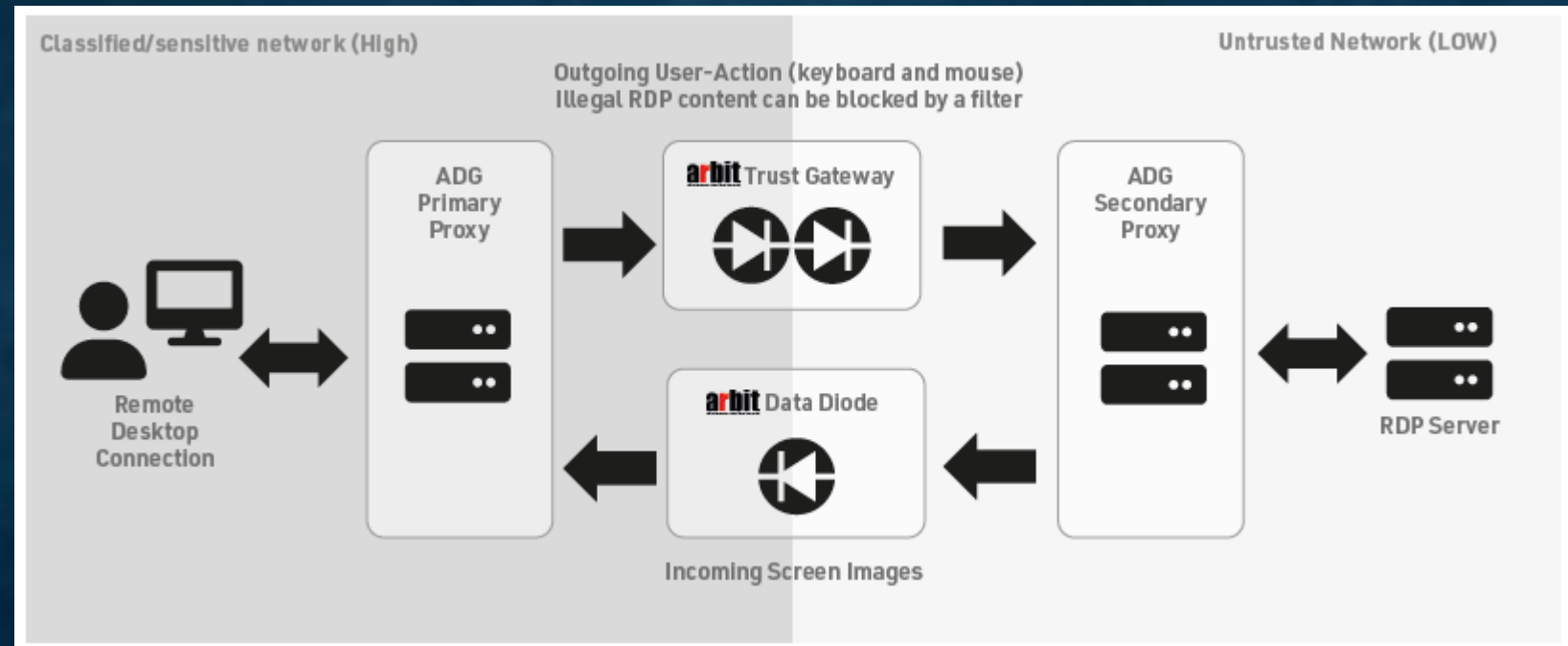
RED



Internet

The user wants to surf internet from a secure network

- ARBIT solution allows the mouse and keyboard to be passed out the secured network and the return of the input video images



# USE CASE – GOV - 2



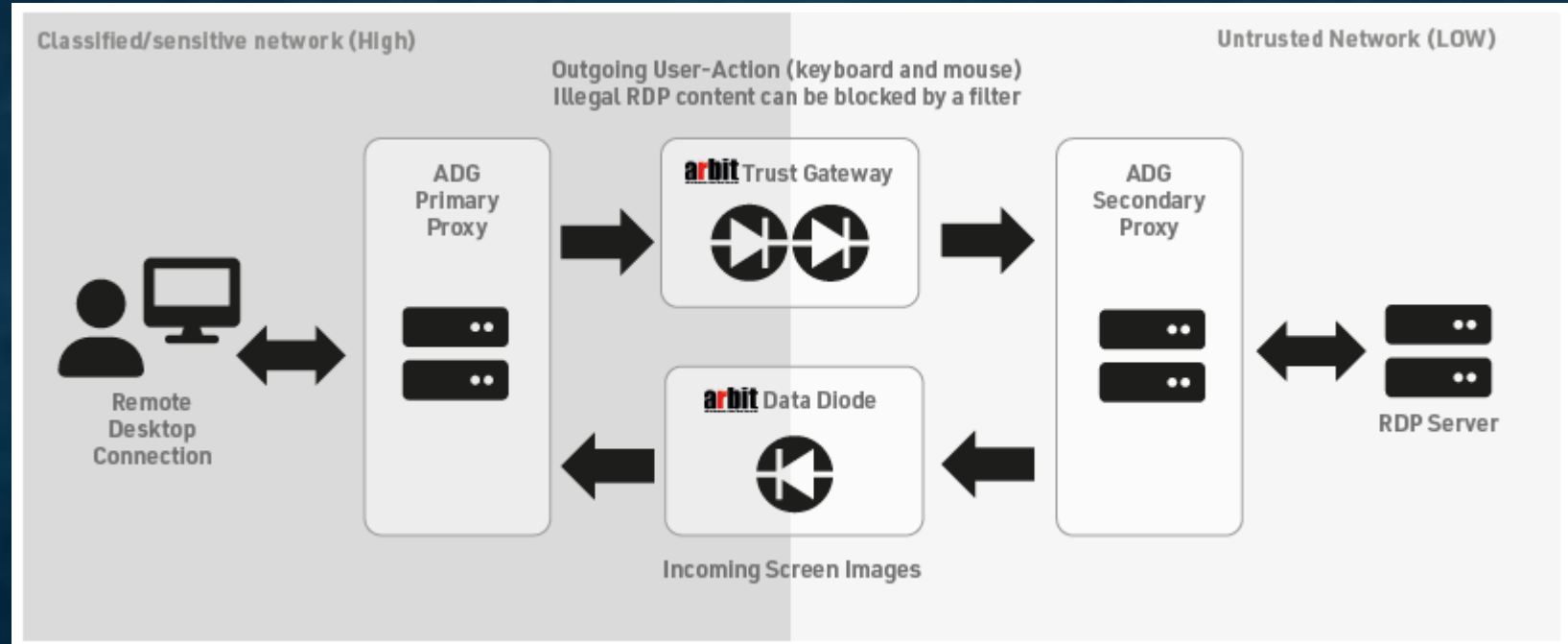
RED



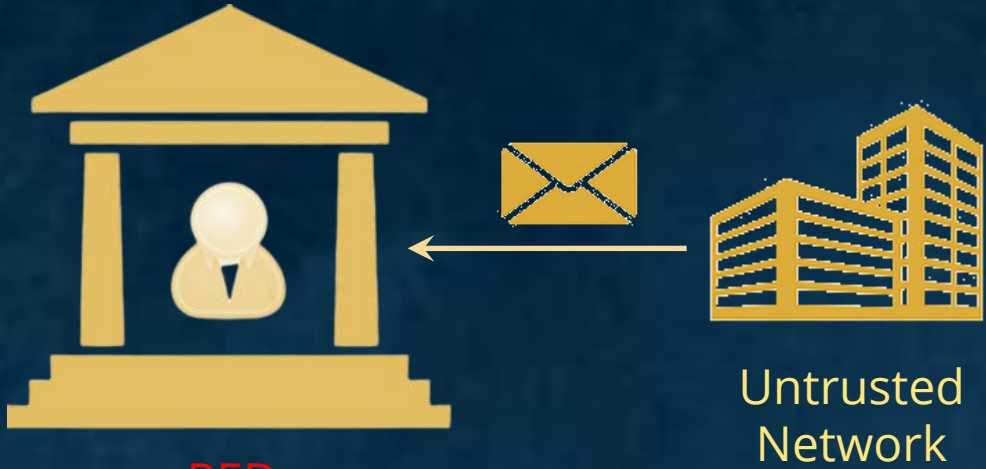
Untrusted  
Network

The user is a network admin and aim to manage and setup networks outside its secured perimeter

- ARBIT solution allows the mouse and keyboard to be passed out the secured network and the return of the input video images



# USE CASE – GOV - 3



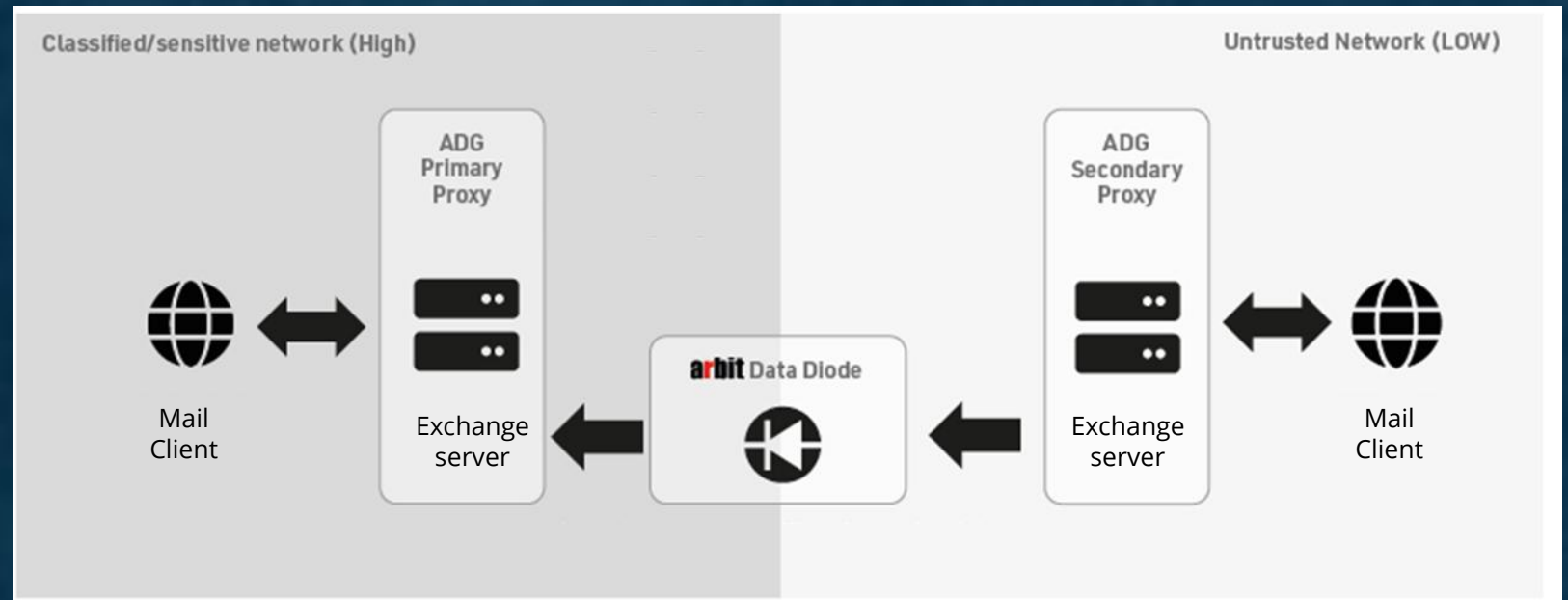
RED

The user wants to receive emails with users outside the security perimeter

- ARBIT Solution, together with OPSWAT, filters emails from untrusted network by sanitizing their content

The incoming content can be validated by the OPSWAT System integrated with the CDS and DD: only the contents that pass all the controls are presented to the user in a secure area

OPSWAT.



# USE CASE – GOV - 4



RED



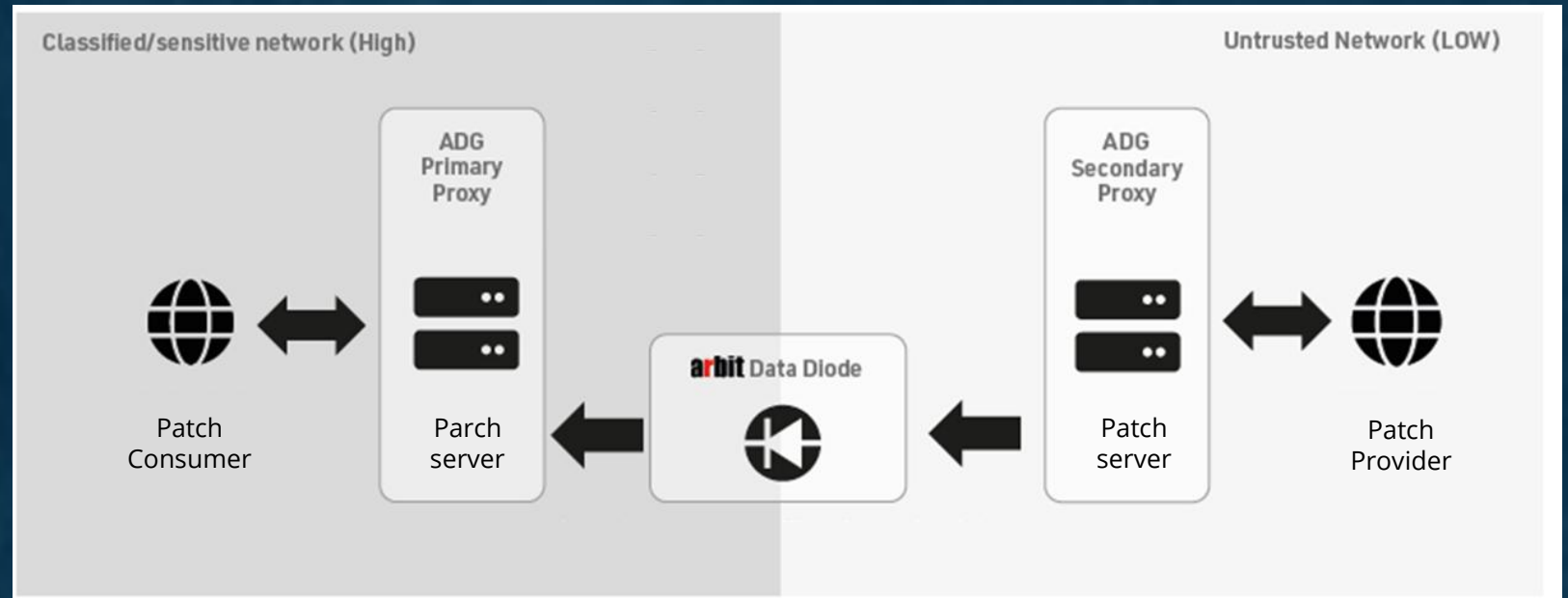
Patch in Internet

The user wants to get patches from the internet for the programs he has in the red area.

- ARBIT solution constantly searches for a new patch via a patch server in the Low area. When a new one is issued, the patch is pushed through the data diode that isolates the HIGH network and scanned for malware and viruses. The patch is then made available on a patch server in the high area.

The incoming Patch is validated by the OPSWAT System integrated with the DD: only the contents that pass all the controls and more than 30 anti-malware engines are presented to the user in a secure area

OPSWAT.



# USE CASE – GOV - 5



RED



Untrusted Network

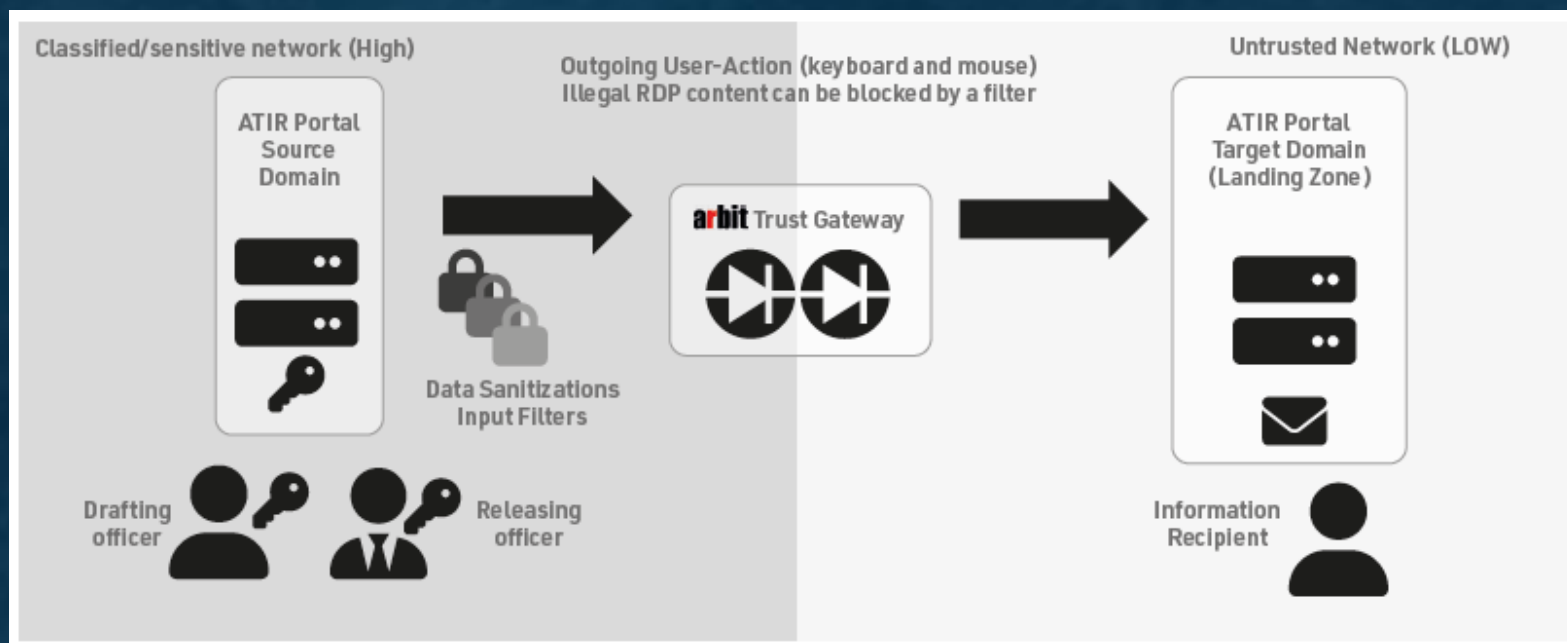
The user wants to release data from a secured area to an untrusted network.

Content to be released  
is prepared by Drafting Officer and  
released by Releasing Officer

Every time message is signed.  
Outgoing messages will have sign  
from:

- ATIR portal
- Drafting Officer
- Releasing Officer

In each signing passage is possible  
to add notes for the subsequent  
signatory



# Domande



# Pubblicazioni



People and Data: The Heart of Intelligence Essential for CEMA



La Sicurezza del Software

Exploiting the MIL-STD-1553 avionic data bus with an active cyber device



Cyber Electromagnetic Activities and Signals Intelligence: a Command and Control framework

Wireless and Ad Hoc Sensor Networks: An Industrial Example Using Delay Tolerant



Effective Surveillance for Homeland Security: Balancing Technology and Social Issues

A Cooperative Time-Frequency Approach to Detect, Recognize and Track Drones with Audio Sensor Networks



# CONTATTI



[WWW.C5I.INFO](http://WWW.C5I.INFO)



[INFO@C5I.INFO](mailto:INFO@C5I.INFO)



## GRAZIE PER L'ATTENZIONE

