

# סייבר במערכות תעשייתיות











Yosi Shavit MBA, CISM - Information Security & Cyber Expert

Cellular: 058-6662242

Mail: [yosish@gmail.com](mailto:yosish@gmail.com) , [yosish@sviva.gov.il](mailto:yosish@sviva.gov.il)

# נושאי הלימוד



- מונחים במערכות בקרה תעשייתיות 
- מה זה ICS ? 
- הרכיבים השונים המשתתפים במערכת ICS 
- מה זה SCADA , מה זה DCS ? 
- סוגי בקרים: PLC , RTU , IED 
- רכיבי שטח 
- כיצד בנויה רשת מפעלית זו מול OT 
- איומים וחולשות במערכות ICS 

# למה צריכים בכלל מערכות SA ?

## יתרונות

- ✓ אוטומציה של תהליכים ושיפור ביצועים בעבודה
- ✓ מזעור התערבות של גורם האנושי בתהליך ייצור
- ✓ התייעלות של ניהול
- ✓ השגת שליטה ובקרה בתהליכי הייצור
- ✓ הפחתת העלויות
- ✓ ריכוז הנתונים הנדרשים לצורך קבלת החלטות



## החסרון הגדול

❖ הגדלת משטח החשיפה לתקיפות סייבר

# ICS - Industrial Control Systems

מערכות בקרה תעשייתיות קיימות בתעשיות הבאות:



□ ייצור

□ תחבורה

□ טלקום ותקשורת

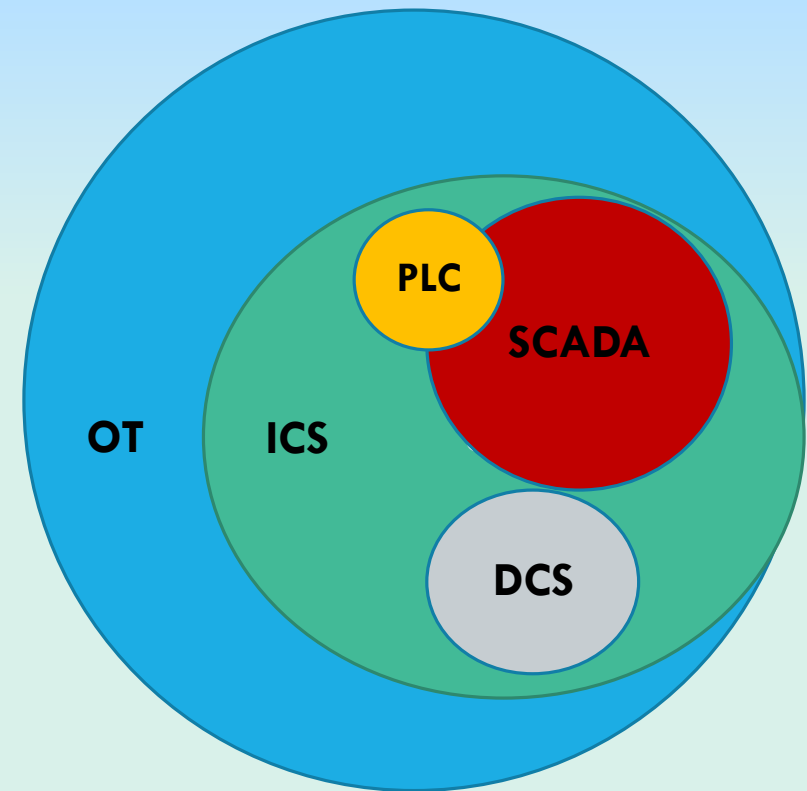
□ מערכות BMS (Business Management Systems)

מדובר במערכות בקרת מבנה

□ התעשייה הכימית – כולל תעשיית גאז ודלקים

# מונחים במערכות בקרה תעשייתיות

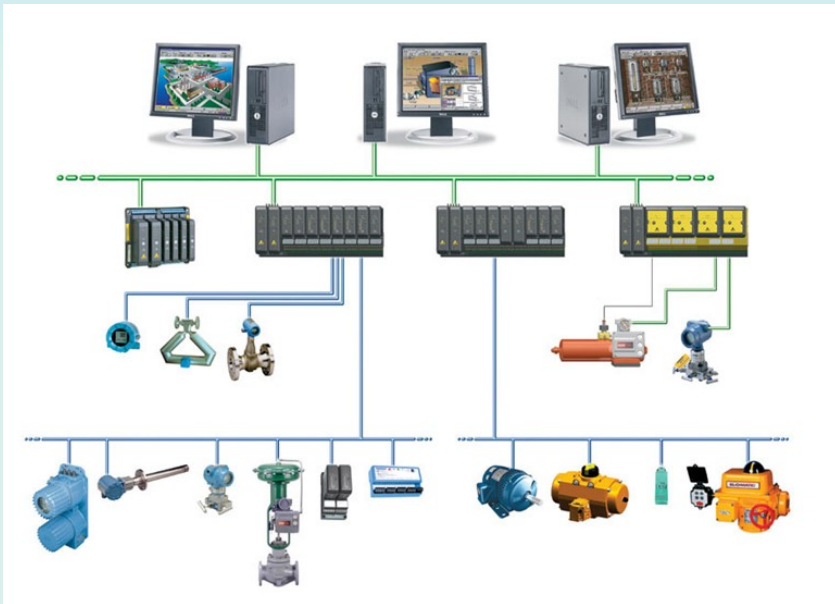
- ICS - Industrial Control Systems
- Scada - Supervisory Control and Data Acquisition
- DCS - Distributed Control System
- OT - Operation Technology
- PLC - Programmable Logic Computer



רשתות ומערכות שליטה ובקרה שמטרתם לתמוך בתהליכים התעשייתיים  
קיימים 2 כווני עבודה:

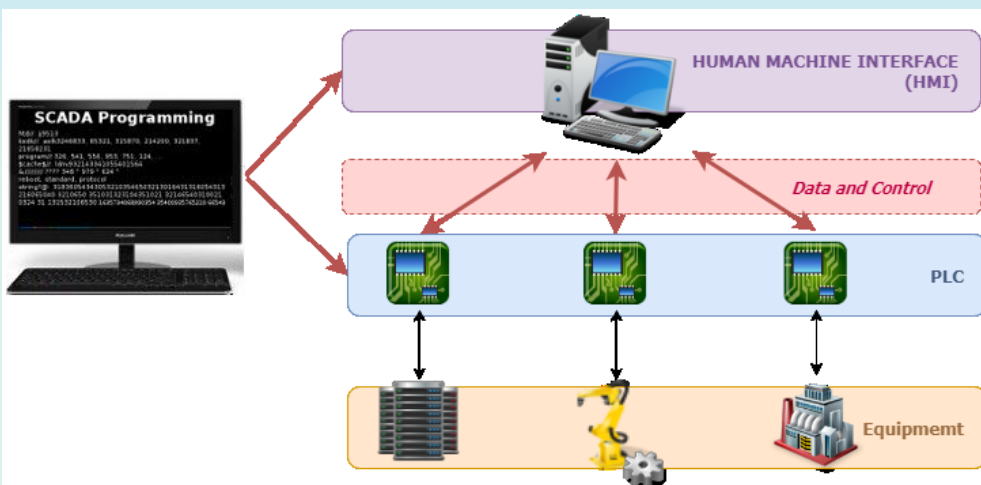
1. פקודות מהבקר אל מערכת הייצור: שינוי לחץ, שינוי טמפ, פתיחת ברז

2. קבלת אינדיקציה על נתוני רצפת ייצור: ערכי לחץ, טמפ, זרימה



## SCADA – Supervisory Control and Data Acquisition

מקרה פרטי של ICS



SCADA היא מערכת המבוססת על **מידע נתונים ועל ארועים** ולא על תהליך

מערכת SCADA כוללת בדרך כלל את התת-מערכות הבאות:

- ממשק אדם-מכונה HMI שמציג מידע על התהליך למפעיל, וכך מאפשר למפעיל לנתר ולבקר את התהליך.
- מערכת פיקוח, שצוברת מידע על התהליך ושולחת הוראות כדי לבקר את אותו תהליך.
- יחידות מסוף רחוקות (RTU) שמתחברות לגששים הממירים את אותות הגששים לנתונים דיגיטליים, ושולחים את הנתונים הדיגיטליים למערכת הפיקוח.
- בקרים לוגיים שניתנים לתיכנות (PLC)
- שרת HISTORIAN אשר אוגר עבור המערכת את המידע
- תשתית תקשורת, שמקשרת את מערכת הפיקוח ליחידות RTU

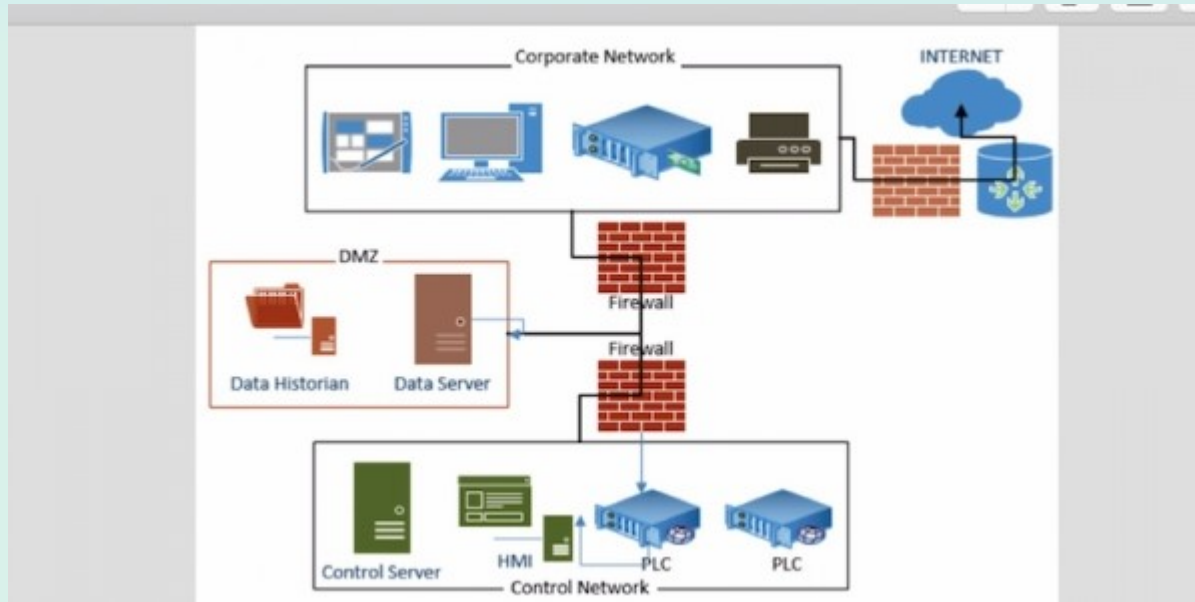
# שרת היסטוריאן HISTORIAN SERVER

אוגר את כל המידע והלוגים המתקבלים ממערכת הסקאדה

בדרך כלל מדובר במערכות בסיסי נתונים ייעודיות (proprietary) שלא תמיד מתמשקות לבסיסי נתונים נפוצים.

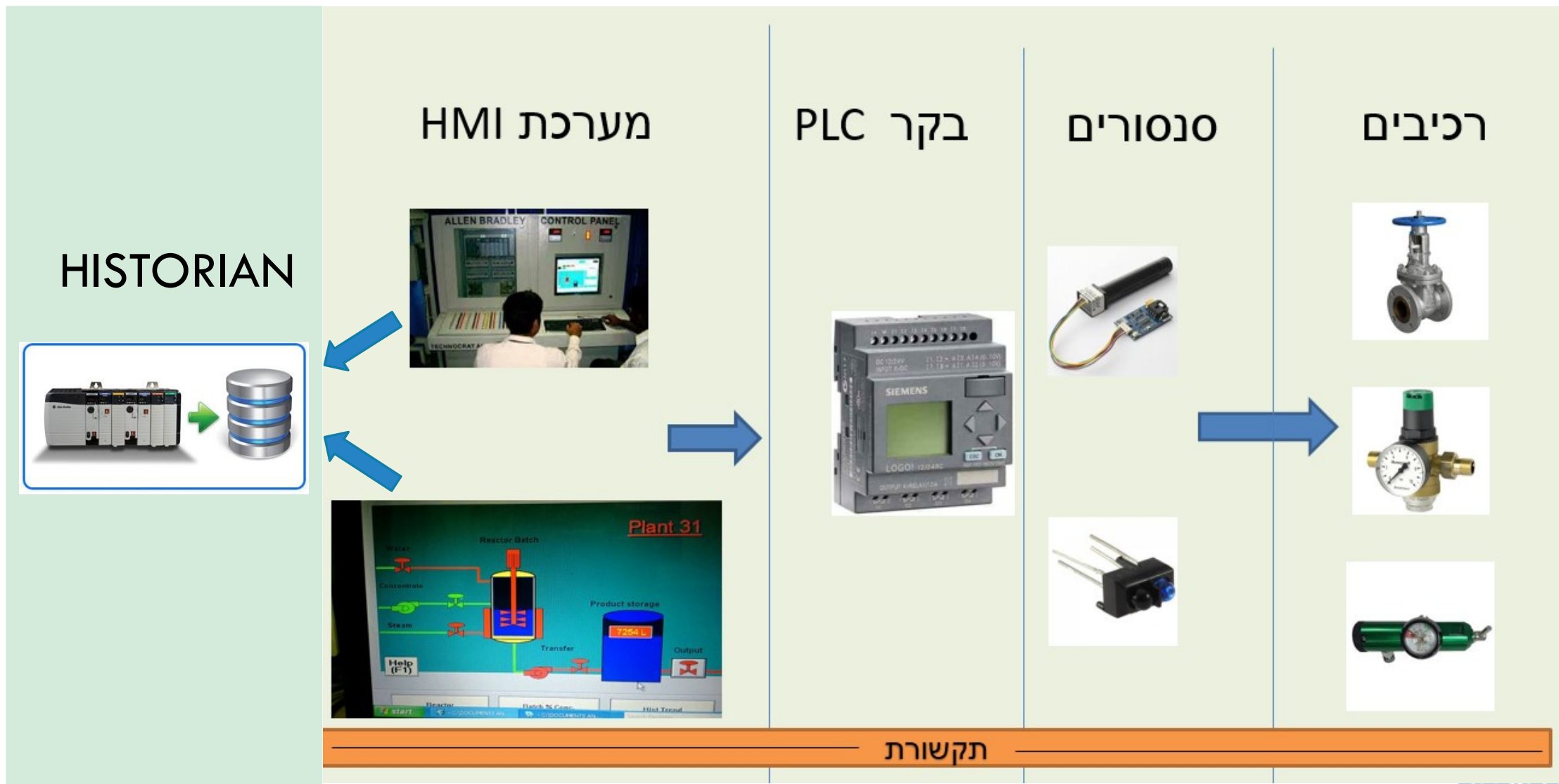
○ ביצועי קריאה וכתובה חייבים להיות גבוהים מאוד ברמות של **mili second** כי מערכת בקרת הייצור מבוססת וניזונה ממידע בזמן אמת.

○ יכולת דחיסה גבוהה. מדובר בכמויות גדולות של מידע, יש לדחוס ככל האפשר על מנת לחסוך מקום אחסון.



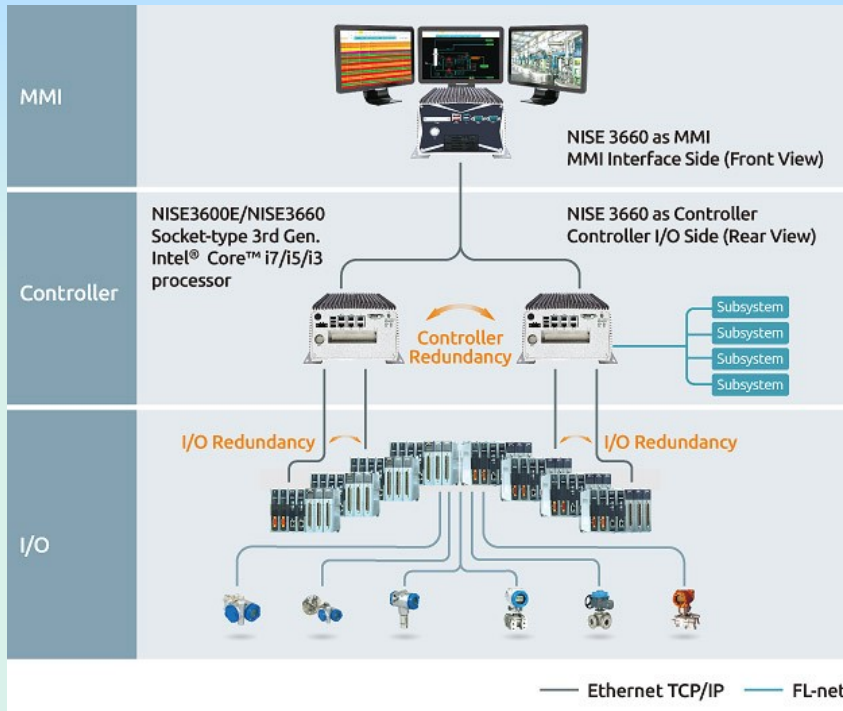


# מערכת סקאדה טיפוסית



תקשורת

מקרה פרטי של ICS



○ DCS זוהי מערכת בקרת תהליכים שמשמשת בתקשורת להתחבר לחיישנים (SENSORS), מפעילים (ACTUATORS), בקרים ומערכות פיקוח

○ היא מערכת בקרה **מבוססת תהליך** - בשימוש בתהליכים בעלי תקשורת מהירה מאד.

○ DCS באופן טיפוסי מכיל מחשב או 2 לשליטה ומשתמש בפרוטוקולים ייעודיים (proprietary) ליצירת תקשורת

○ יותר מהירה ויעילה בייצור המוני

○ ניתן למצוא פתרון DCS במערכות הבאות:

- \* Electrical power grids and electrical generation plants
- \* Environmental control systems
- \* Traffic signals
- \* Water management systems
- \* Refining and chemical plants
- \* Pharmaceutical manufacturing

# PLC vs DCS

<https://www.automationworld.com/products/control/article/13311313/plc-vs-dcs-which-is-right-for-your-operation>

# DCS vs SCADA

DCS ו-SCADA הם מנגנוני ניטור ובקרה המשמשים לפיקוח ובקרה על תהליכים וציוד במכשירים תעשייתיים כדי להבטיח שהכל פועל בצורה חלקה ושום ציוד לא יעבוד מעבר למגבלות שצוינו

SCADA	DCS
מעקב ואיסוף נתונים יתמקדו יותר באיסוף נתונים ומידע והתייחסות לבקרת ביצועים.	ממוקד: מכוון לתהליך מכיוון שהוא מתמקד בתהליכים בכל שלב של העבודה
מבוסס על אירועים. מצפה ששינוי ערך באירוע או ברכיב בודד יתחיל בפעולה כלשהי. חריגה מה-SET-POINT אמורה להיות מתוקנת	עובד פרוצדוראלי: מבצע את כל הפונקציות שלה ברצף ואינה מתעדת אירועים
עדיפה כאשר כל המערכת פרוסה במקום גיאוגרפי גדול	מבוסס פעולה אינדיבידואלית: מפעל אחד / תהליך אחד
עובד גם בתקשורת פחות אמינה כשרכיבי השטח מנותקים. עושה זאת על ידי הקלטת כל הערכים הנוכחיים, כך שתחנת הבסיס תוכל לספק את הערכים האחרונים שהוקלטו, גם אם אין לה גישה למידע חדש ממקום מרוחק.	חייבת להיות תמיד מחוברת ל I / O - של המערכת תמיד חייבת קלט פלט בזמן אמת .
יותר גמיש	פחות גמיש
יותר OVERHEAD - תכנות חוזר ונשנה בבקרים	פחות התעסקות – שגר ושכח

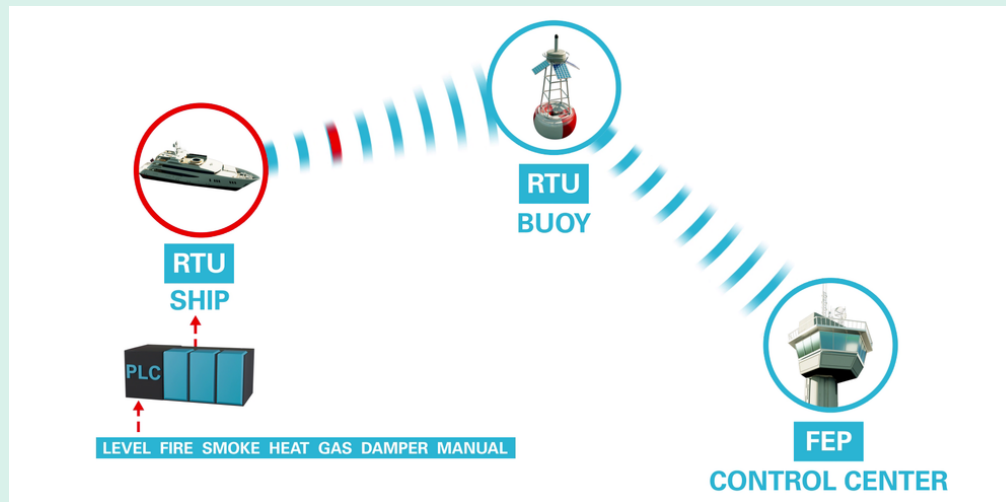
## Programmable logic controller

# מה זה PLC ?

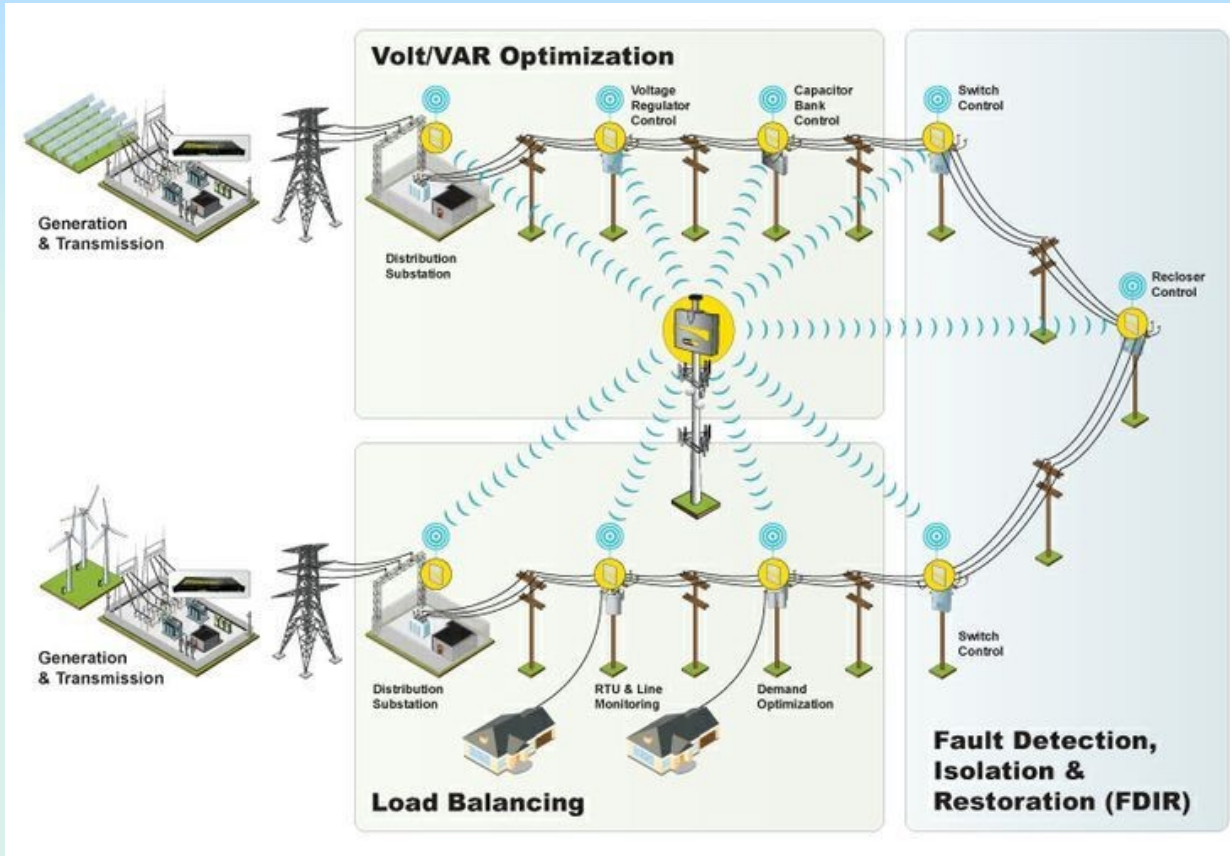
- מחשב זעיר בעל כניסות ויציאות של מידע בינארי המשמש לאוטומציה של תהליכים אלקטרומכניים
- מתוכנן לפעילויות רבות של פלט / קלט (I/O)
- הבקר מתוכנת לרוב בלוגיקה קבועה מראש, אשר תאפשר פעילות ללא התערבות מפעיל בשגרה.
- הבקר יבנה לרוב מחומר עמיד וקשיח שכן קיימים מקרים בהם תידרש עמידות לטמפרטורות לא שגרתיות ולתנאים סביבתיים קשים.
- לבקר תוכנה וחומרה אשר ניתנים לעדכון ושינוי
- חלק מהפונקציות של בקרים הם; בקרת תהליכים, בקרת ממסר, בקרת תנועה, רשתות וכו



- מכשיר אלקטרוני שבשליטת מיקרו-מעבד
- מממשק עצמים בעולם הפיזי (חיישנים) למערכת בקרה או SCADA מבוזרת על ידי העברת נתונים כדי לשלוט על עצמים מחוברים.
- משימתו העיקרית היא שליטה ורכישת נתונים מצידוד תהליכים במיקום המרוחק והעברת נתונים אלה בחזרה לתחנה המרכזית.
- מתאים יותר לטלמטריה גיאוגרפית רחבה יותר משום שהוא משתמש בתקשורת אלחוטית
- פועלים היטב ברשתות מהירות גבוהה ונמוכה כאחת
- מספקים יכולות רישום נתונים משמעותיות כך שהנתונים נשמרים במהלך הפסקות תקשורת או למטרות דיווח



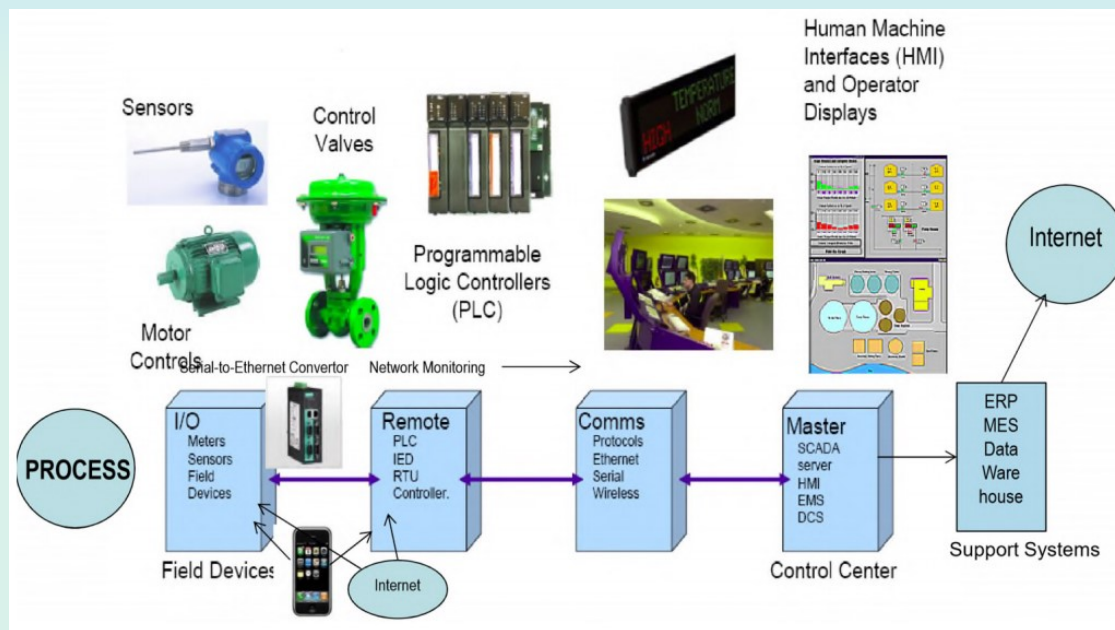
- בקרים המשמשים בעיקר לעולם החשמל
- ניטור בקרה ומדידה של מערכות מתח וחשמל



# רכיבי שטח - FIELD DEVICES

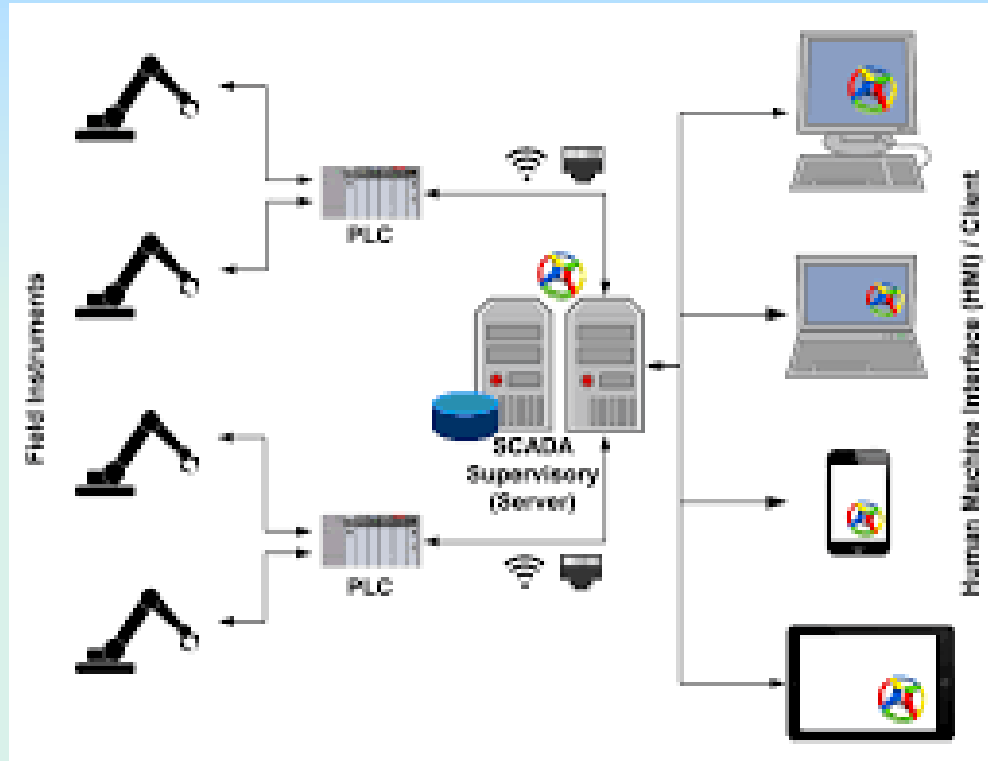
SENSORS, ACTUATORS - חיישנים, מפעילים

- מאפשרים את החיבור בין עולם הבקרה לעולם הפיסי.
- חיישן יכול להיות לדוגמא מודד רמת חומציות PH, או חיישן שמזהה דליפות בצנרת הולכת דלקים
- מפעיל יכול להיות מנוע חשמלי או משאבה אשר מבצעת פעולה בהינתן פקודה ע"י הבקר.
- החיישן מעביר מידע לבקר ואילו המפעיל מקבל מידע מהבקר.





# פקודות מהבקר אל מערכת הייצור:



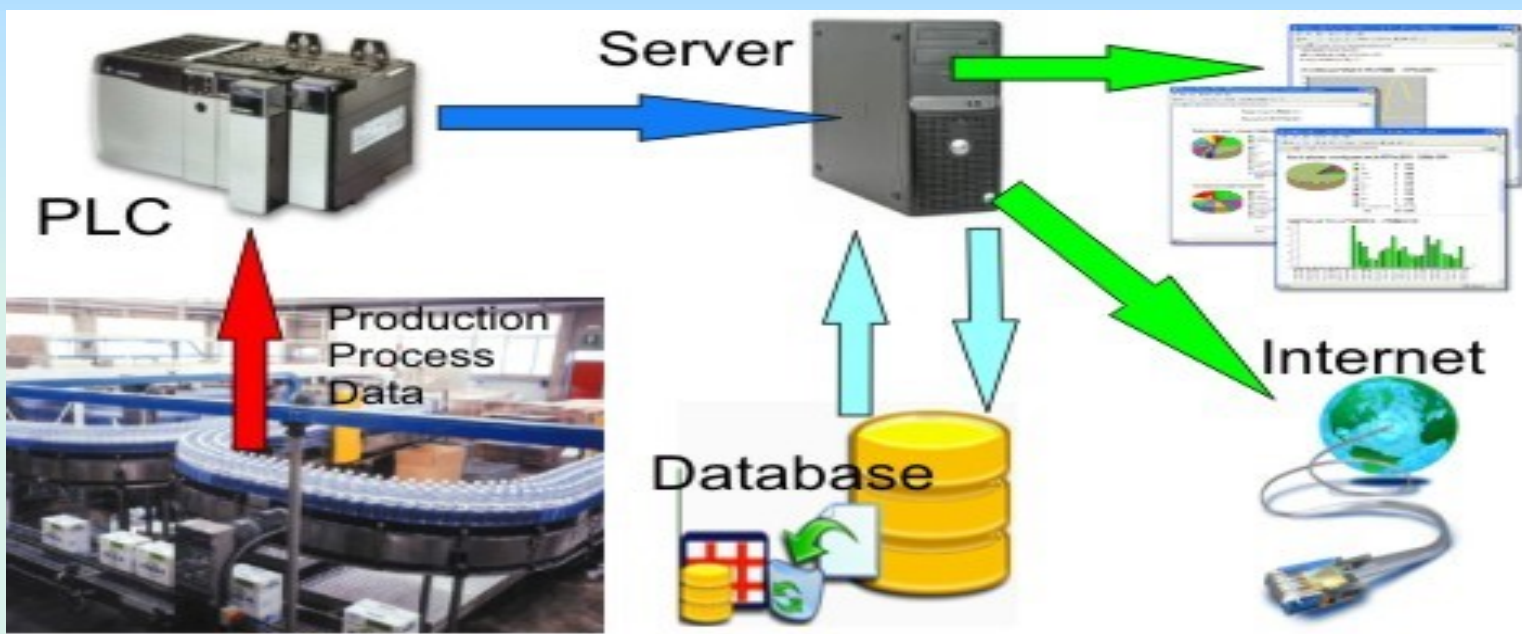
מחשב נייד

מחשב נייד

טלפון נייד

LOCAL PANEL

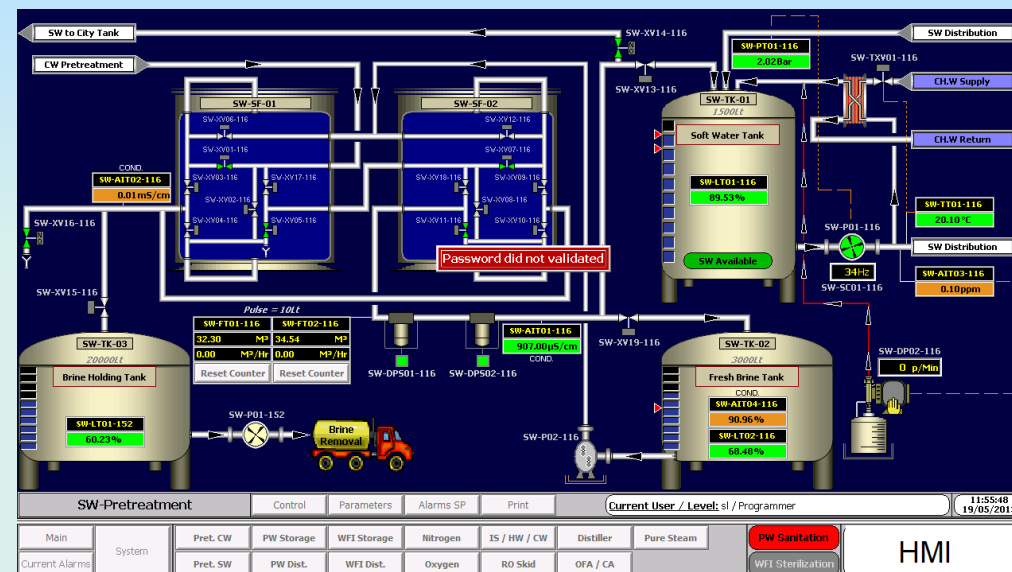
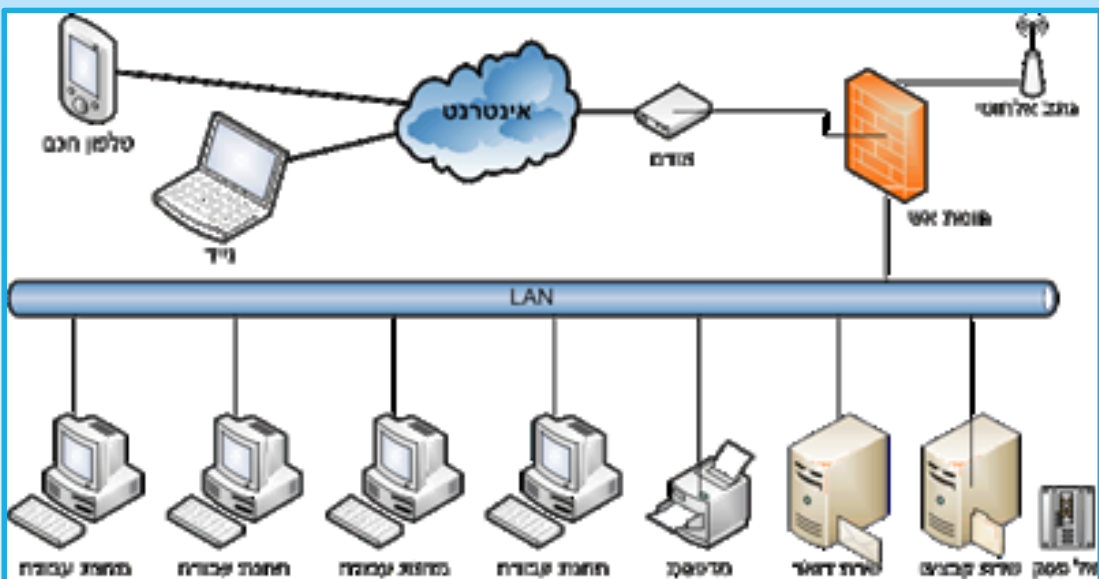
# קבלת אינדיקציה על נתוני רצפת ייצור: ערכי לחץ, טמפ, זרימה



# כיצד בנויה הרשת המפעלית ?

## רשת מנהלתית - רשת זו

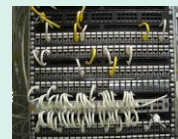
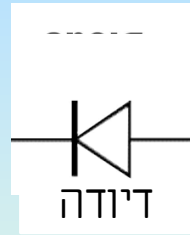
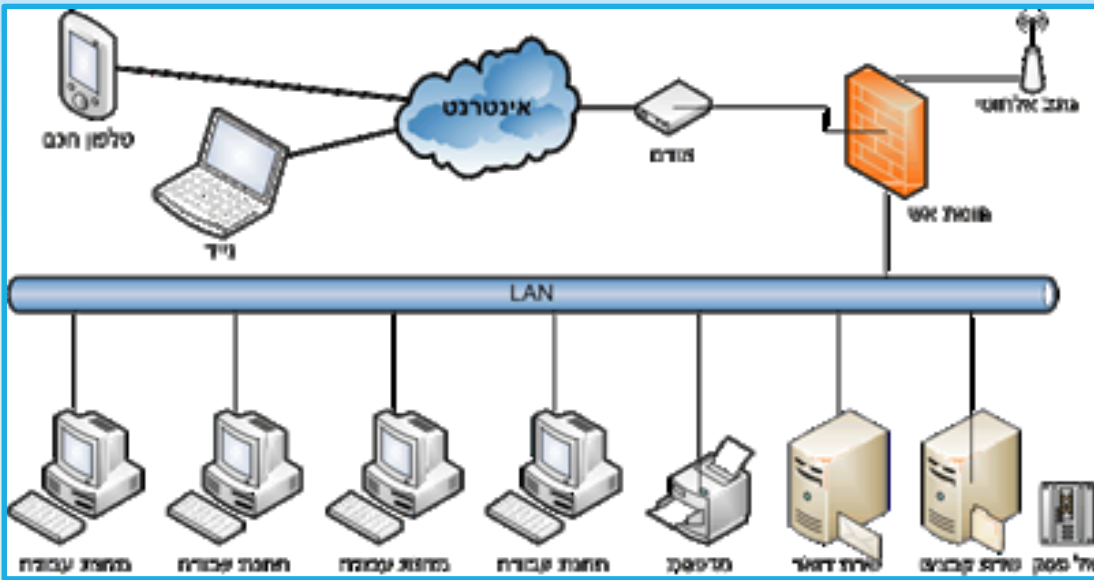
## רשת תפעולית - רשת זו



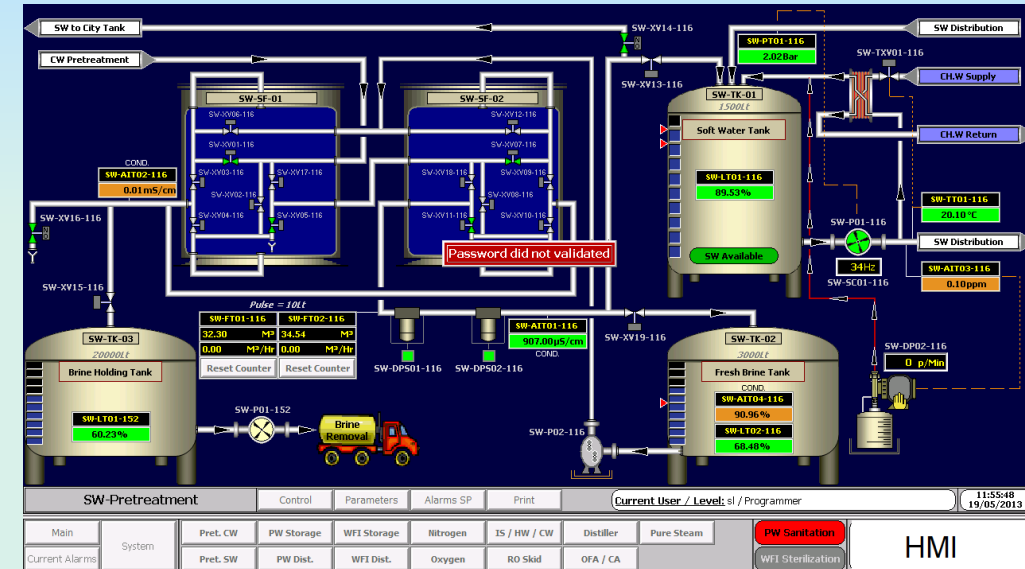
# אמצעים להפרדת רשתות

## רשת מנהלתית - רשת זו

## רשת תפעולית - רשת זו

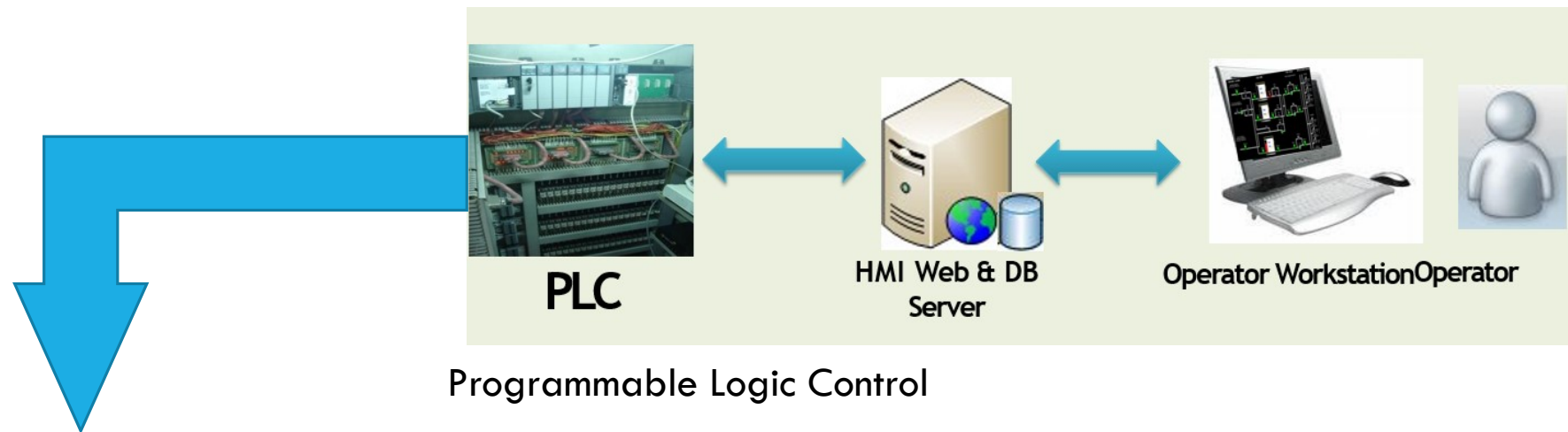


הפרדה פיזית

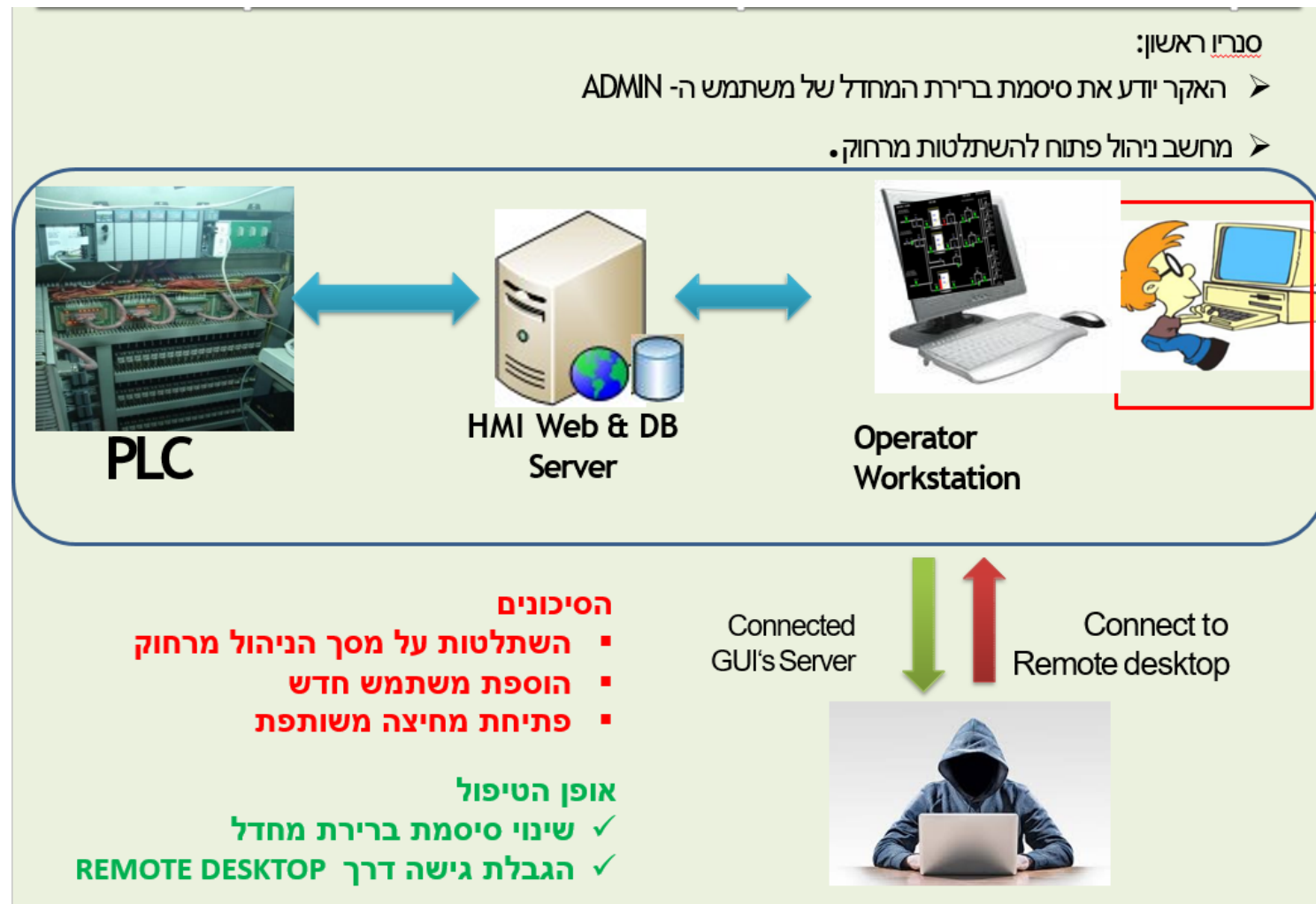


# תקיפות על מערכת ICS

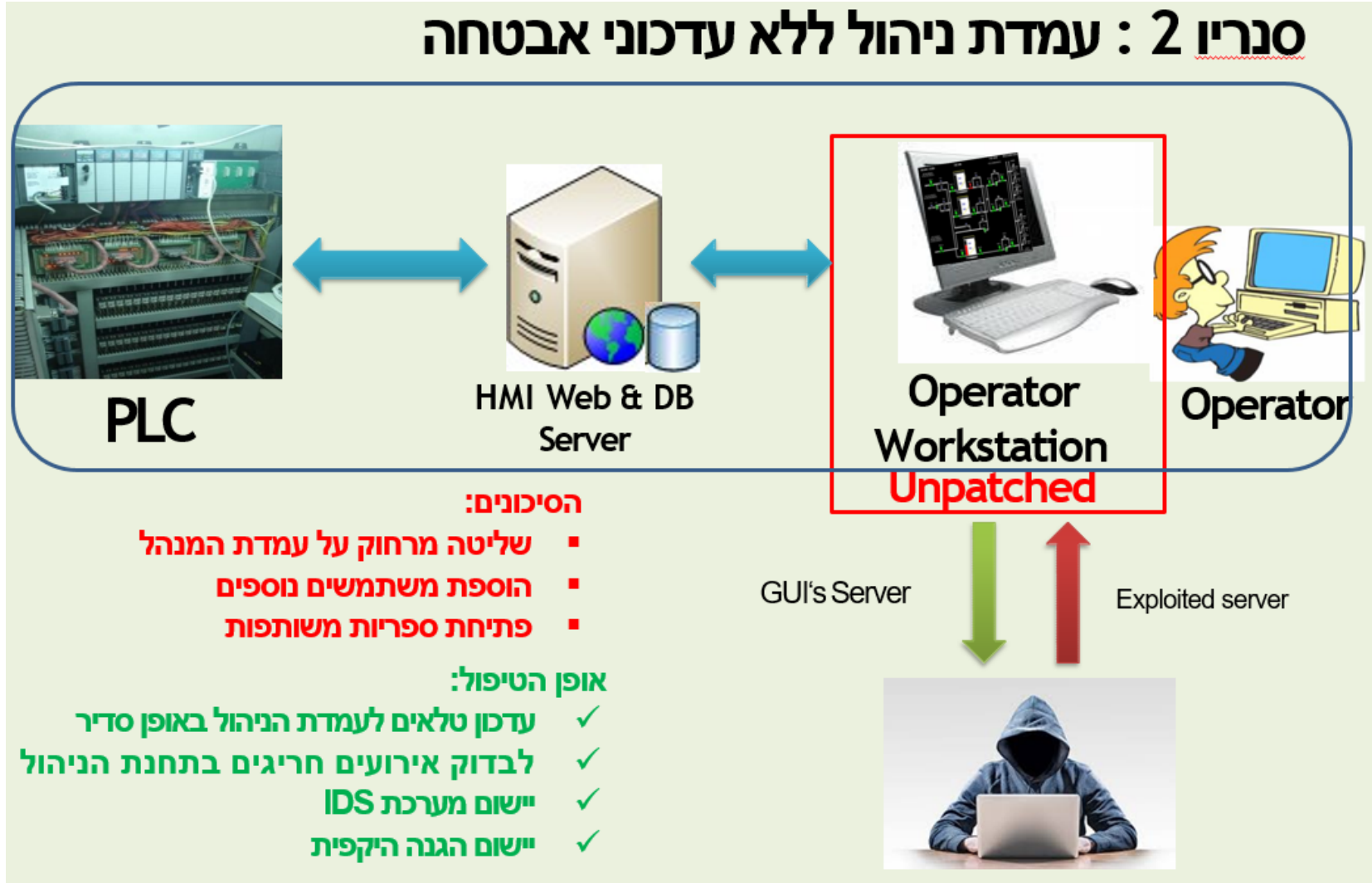
תהליך העבודה במערכת ICS



# תקיפת עמדת הניהול דרך מנהל המערכת



## סריו 2 : עמדת ניהול ללא עדכוני אבטחה



### הסיכונים:

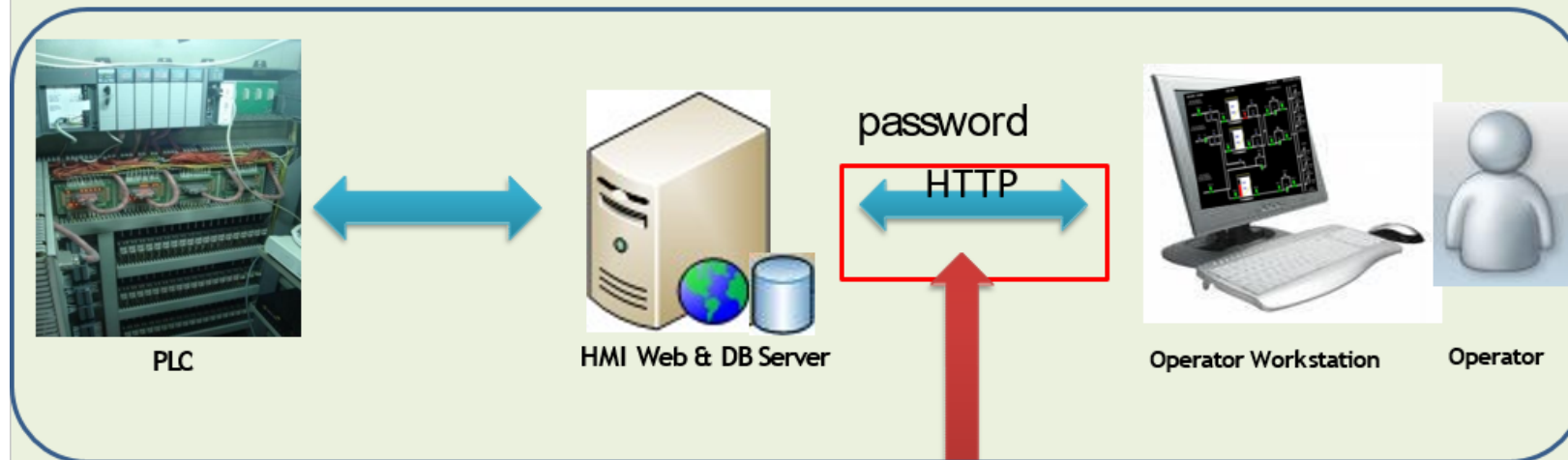
- שליטה מרחוק על עמדת המנהל
- הוספת משתמשים נוספים
- פתיחת ספריות משותפות

### אופן הטיפול:

- ✓ עדכון טלאים לעמדת הניהול באופן סדיר
- ✓ לבדוק אירועים חריגים בתחנת הניהול
- ✓ יישום מערכת IDS
- ✓ יישום הגנה היקפית

# תקיפת התווך בין מנהל המערכת לשרת

## סריו 3 : הסגפת הסימא



### הסיכונים:

- תקשורת לא מוצפנת מאפשרת גילוי הסימא
- האקר יכול להזדהות למערכת עם סימא חוקית

### אופן הטיפול:

- ✓ שימוש ב-HTTPS במקום HTTP
- ✓ הטמעת IPS לזיהוי ניסיונות SNIFING

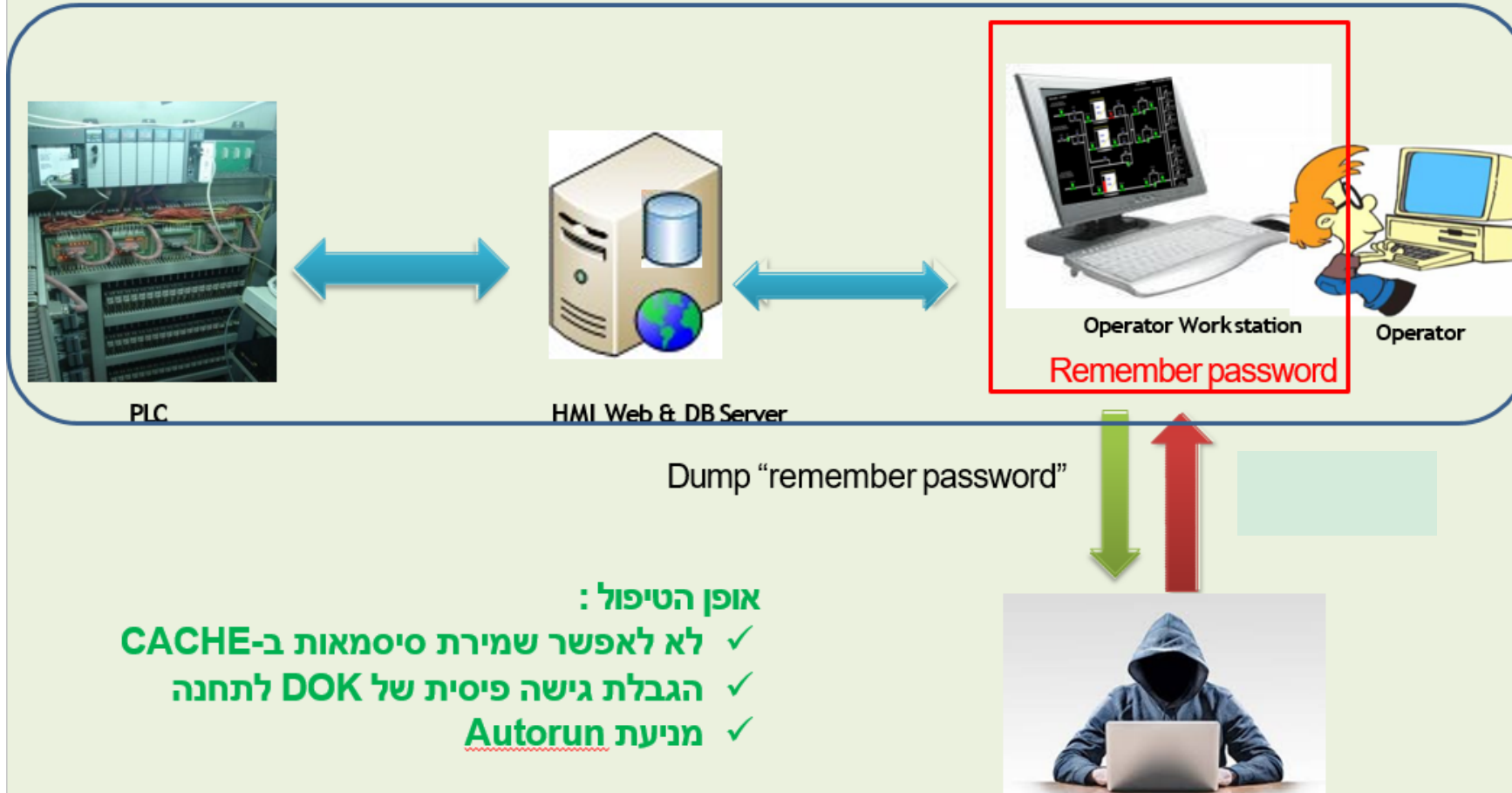


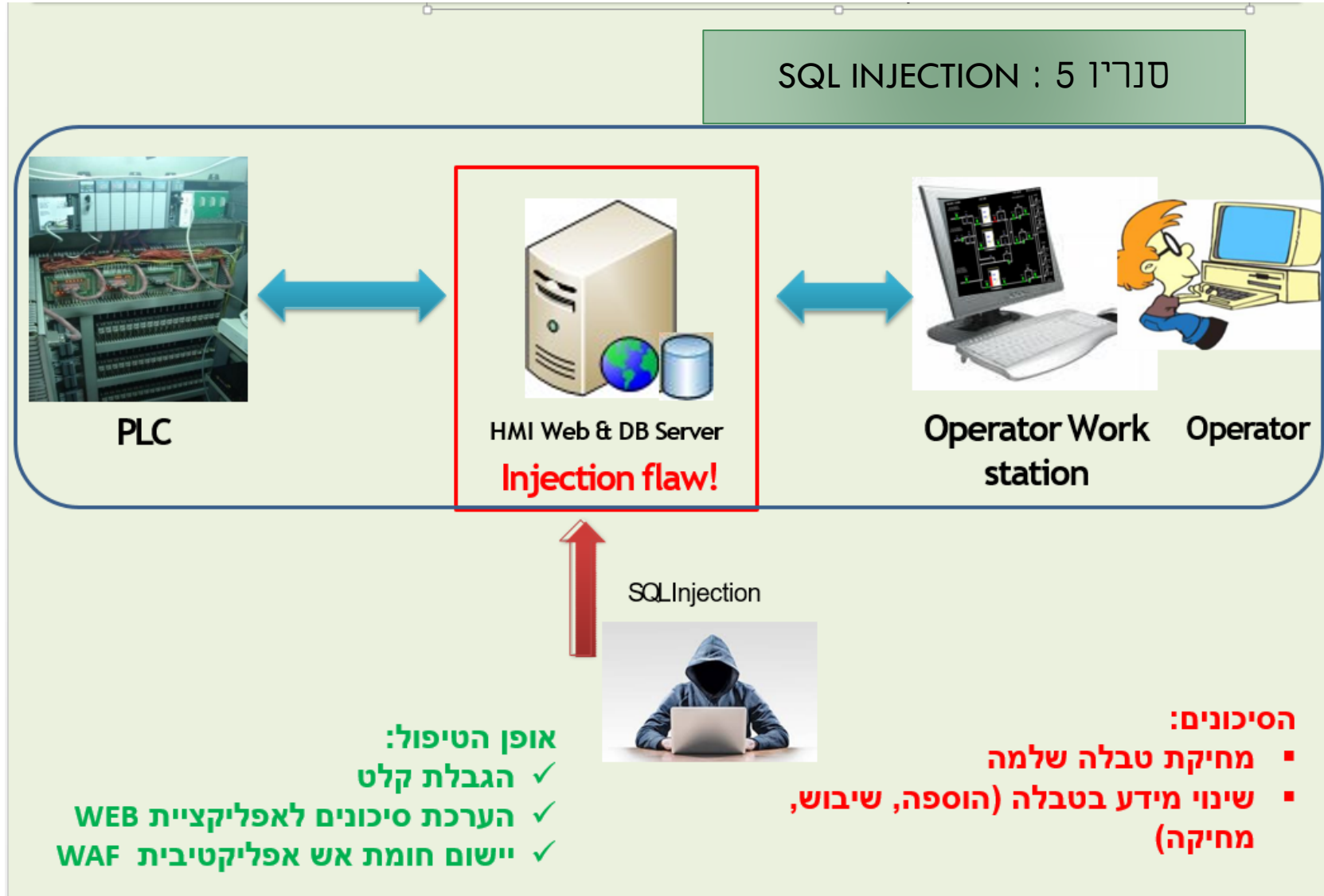
Sniff password  
in the network



# ביצוע האקינג לעמדת הניהול

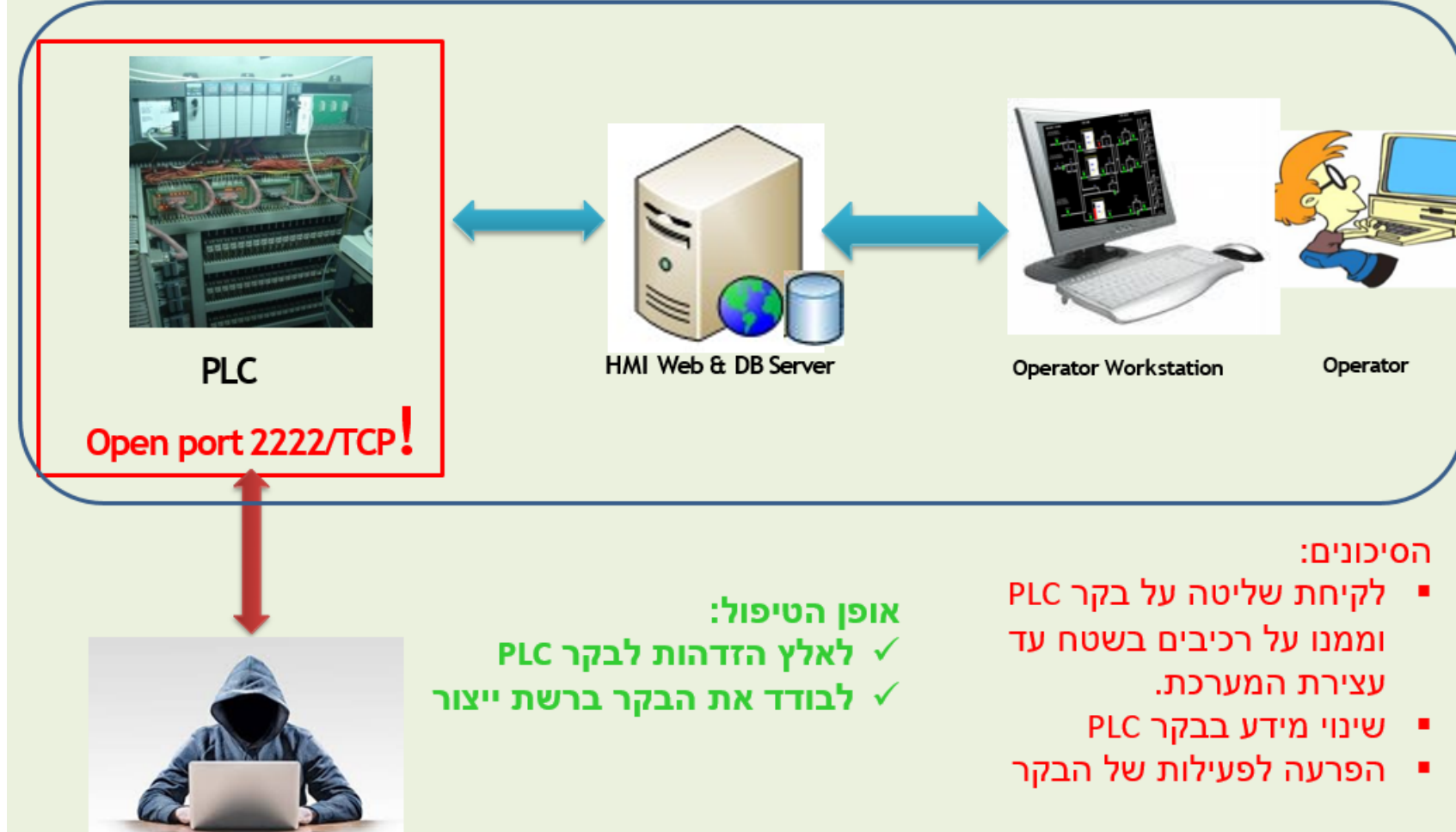
- סנריו 4 :
- הסיסמא נשמרת ב-CACHE של המערכת
- הכנסת DOK
- הרצת קובץ מתוך DOK





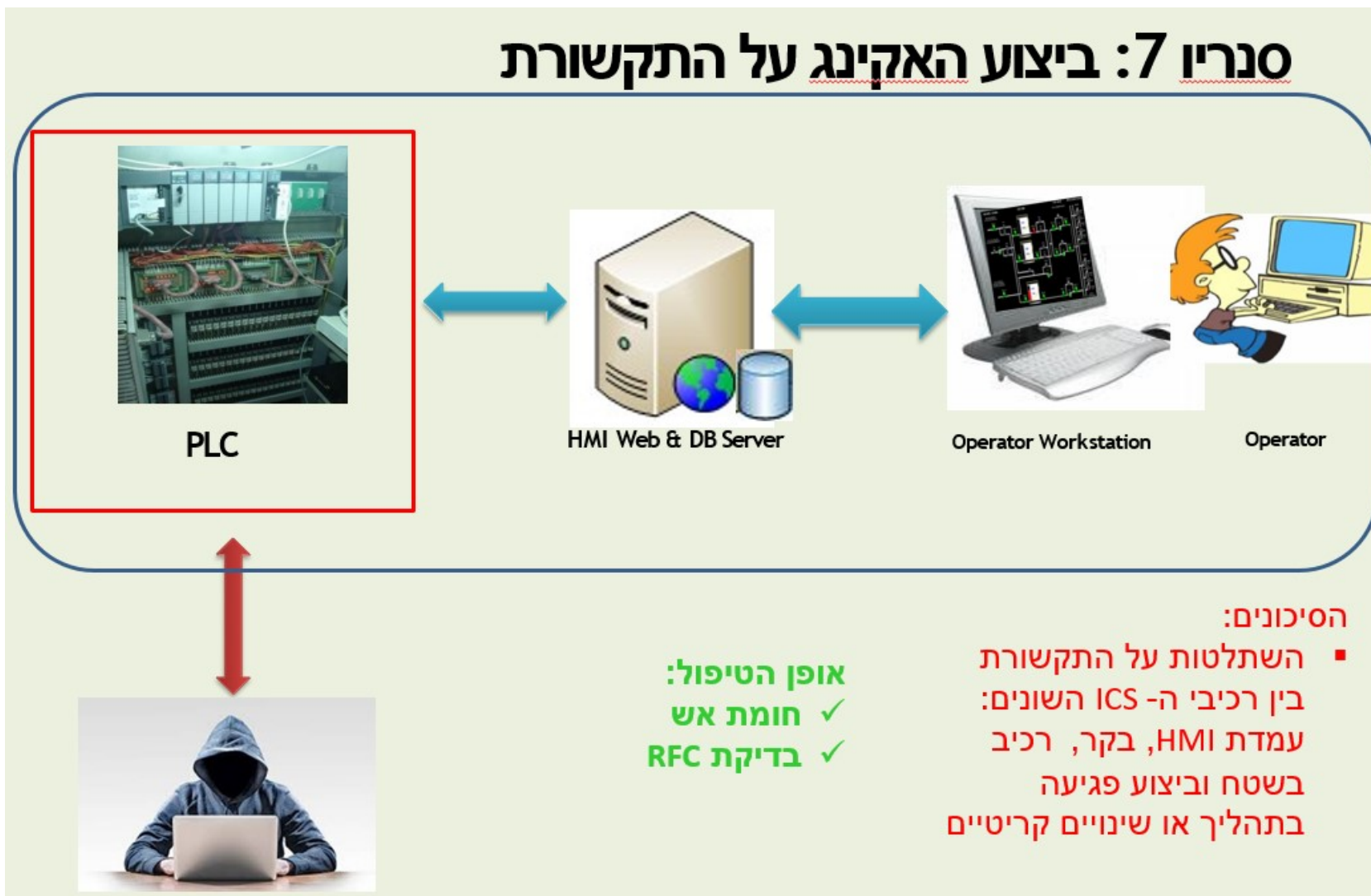
# ביצוע האקינג על הבקר עצמו

## סריו 6: ביצוע מניפולציה ישירה על בקר PLC



# ביצוע האקינג על התקשורת בין רכיבי ICS

## סריו 7: ביצוע האקינג על התקשורת



הסיכונים:

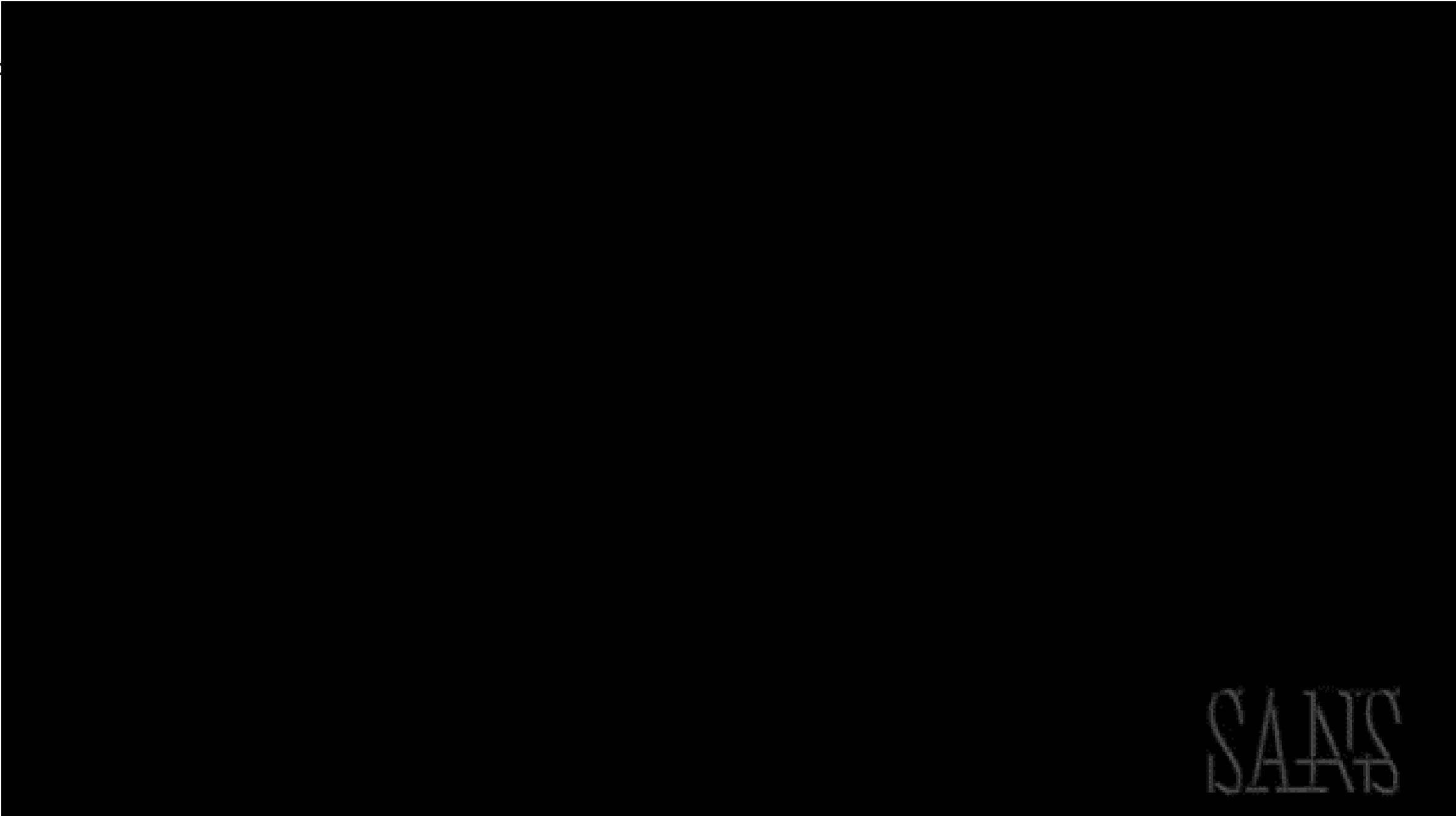
- השתלטות על התקשורת בין רכיבי ה-ICS השונים: עמדת HMI, בקר, רכיב בשטח וביצוע פגיעה בתהליך או שינויים קריטיים

אופן הטיפול:  
 ✓ חומת אש  
 ✓ בדיקת RFC

# סרטון – אנטומיה של תקיפת מתקן ייצור אנרגיה המכיל מערכות ICS



<https://www.youtube.com/watch?v=eNB1gq5gbA>



SANS  
SANS



# שאלות ותשובות

