

# Analysis and Simulation of the Main Capabilities of Human-Machine Interface (HMI) and Related Specific Protocols (HTTP)

Vasile Florin POPESCU<sup>1</sup>, Tiberiu ION<sup>2</sup>, Marius Emil PÂRVU<sup>3</sup>, Sorin PISTOL<sup>4</sup>, Olivia COMȘA<sup>5</sup>

<sup>1,2</sup> National Defence University of Bucharest / Faculty of Security and Defense

<sup>3,4,5</sup> SAFETCH Innovations, Bucharest, Romania

[popescu.vflorin@unap.ro](mailto:popescu.vflorin@unap.ro), [ion.tiberiu@unap.ro](mailto:ion.tiberiu@unap.ro), [marius.parvu@safetech.ro](mailto:marius.parvu@safetech.ro),  
[pistolSORIN@icloud.com](mailto:pistolSORIN@icloud.com), [olivia.comsa@safetech.ro](mailto:olivia.comsa@safetech.ro)

**Abstract:** The general objective of this research was to conduct a study of the main capabilities of human-machine interface (HMI) simulators and validation in laboratory conditions of HMI simulators for distribution and testing.

The practical part and the results of this research are represented by the simulation of HMI and related specific protocols (HTTP) using a Siemens S7-1200 equipment.

**Keywords:** Human Machine Interfaces - HMIs, Remote Terminal Units – RTUs, Programmable Logic Controllers – PLCs, Conpot, HTTP

---

## INTRODUCTION

Human Machine Interfaces (HMI) are just as their name states - they serve as a way for humans to interact with machines. (Craig, 2018)

Human Machine Interfaces, more commonly known as HMIs, have been used since a personal computer arrived on the plant floor. (Schultz, 2021)

A HMI device is a software-based control system that uses network data to provide operators with a graphical user interface that allows them to monitor the performance of

multiple SCADA devices and issue process commands and settings on a dedicated screen, mobile device or any computer connected to the control network via a web browser.

The HMI allows operators to improve situational awareness, view mobility, to have access anytime, anywhere, and most importantly control over the settings that form a centralized view. The HMI collects data from RTUs (remote terminal units), PLCs (programmable logic controllers) and other control devices, such as flow meters and

temperature controllers, and presents them to an operator using the human-machine interface (HMI).

The HMI allows the operator to see what is happening in real time, including custom mime displays, alarms, trends, etc., in order to make decisions about adjusting any controls or settings of the machine. The HMI can also be connected to other devices, such as a server that stores audit files of the SCADA system to allow analysis of historical data on how it works. With the increased visibility that HMI offers, there are many applications for its use.

Cost control for manufacturing applications can be as important as machine control. As a result, cost-conscious manufacturers may hesitate to consider new automation and control technology investments. Upgrades to human-machine interface (HMI) hardware are no exception. (Reiner, 2018).

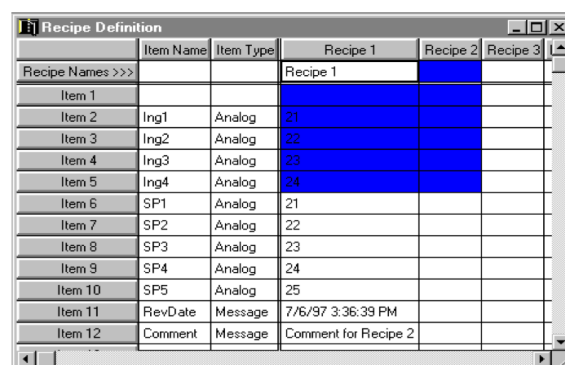
Industrial processes, such as those in manufacturing or generating electricity, infrastructure processes, such as water treatment or oil and gas pipelines, and installation processes, such as those that control heating and ventilation, are all suitable uses for HMI.

## ANALYSIS OF CHARACTERISTICS AND CAPABILITIES WHICH A COMPLETE HMI SOFTWARE / HARDWARE SHOULD HAVE:

**a. Simulation facility included** – creating an easy-to-use simulator will result in an efficient design and reduce development time. The software must allow the simulation of the entire project on a computer, without being connected to a touch panel or PLC / PAC. A good simulator should provide a perfect representation of the pixels, of how the project will appear on the physical HMI panel. A method for editing the relevant tag data in the project should also be provided for all tag names listed on each screen displayed in the simulator. In addition, it must allow the use of peripherals on the

computer screen to simulate fingering on a real HMI. Thus, the values of the labels should be updated in real time. For example, if you want to see how an analog meter moves based on dynamic data in the PLC / PAC, you should allow the value to change and you can watch how the meter moves on the simulation screen. Finally, it should be very easy to switch back and forth from the simulation environment to the screen development mode. You should not waste time configuring the simulation or stopping and starting the development system. This feature will be used every few minutes during project development.

**b. Ease use for networks** – Recipes should make it easier to make a large number of changes to the label (data value) at the touch of a button. Recipes are very useful, not only for traditional process industries (i.e. mixing ingredients), but also for the configuration values of machines and other data sets. The operator must be able to modify and save the recipes during the manufacturing process (only if the operator has the appropriate level of access). It should also allow the rapid import and export of recipe data into a spreadsheet for further handling or archiving purposes.



Item Name	Item Type	Recipe 1	Recipe 2	Recipe 3
Recipe Names >>>		Recipe 1		
Item 1				
Item 2	Ing1	Analog	21	
Item 3	Ing2	Analog	22	
Item 4	Ing3	Analog	23	
Item 5	Ing4	Analog	24	
Item 6	SP1	Analog	21	
Item 7	SP2	Analog	22	
Item 8	SP3	Analog	23	
Item 9	SP4	Analog	24	
Item 10	SP5	Analog	25	
Item 11	RevDate	Message	7/6/97 3:36:39 PM	
Item 12	Comment	Message	Comment for Recipe 2	

**Fig. 1:** Print screen: Representation of a recipe from a HMI simulator - Software used: Aveva InTouch  
<https://www.aveva.com/en/solutions/operations/operations-control-hmi/>

The recipe manager is an additional component of the Aveva InTouch HMI software that simplifies the process of creating manufacturing recipes. (Visualize, Control and Optimize Your Operations, 2021)

The following figure summarizes how the Recipe Manager obtains information from recipe templates to manage a process that creates a product.

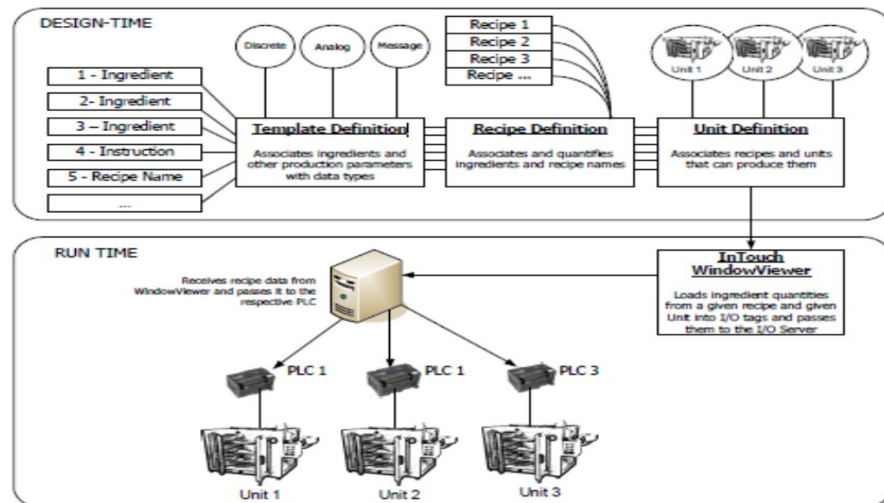


Fig. 2: Illustration of the recipe manager included in the Aveva InTouch HMI software <https://www.aveva.com/en/solutions/operations/operations-control-hmi/>

**c. Ease of handling events** – This utility offers three important features:

c1. Detailed analysis of process trends:

- Data selection by drag and drop method (Tag Picker);
- Absolute or relative time scaling (Time Picker);
- Working mode with static or real time data;

- Sequential rendering of production history;
- Track simple or stacked chart. X-Y dispersion trends;
- Strong resizing, panning, zoom, cursor and annotation capabilities;
- Flexible time horizon;
- The possibility of a detailed analysis.

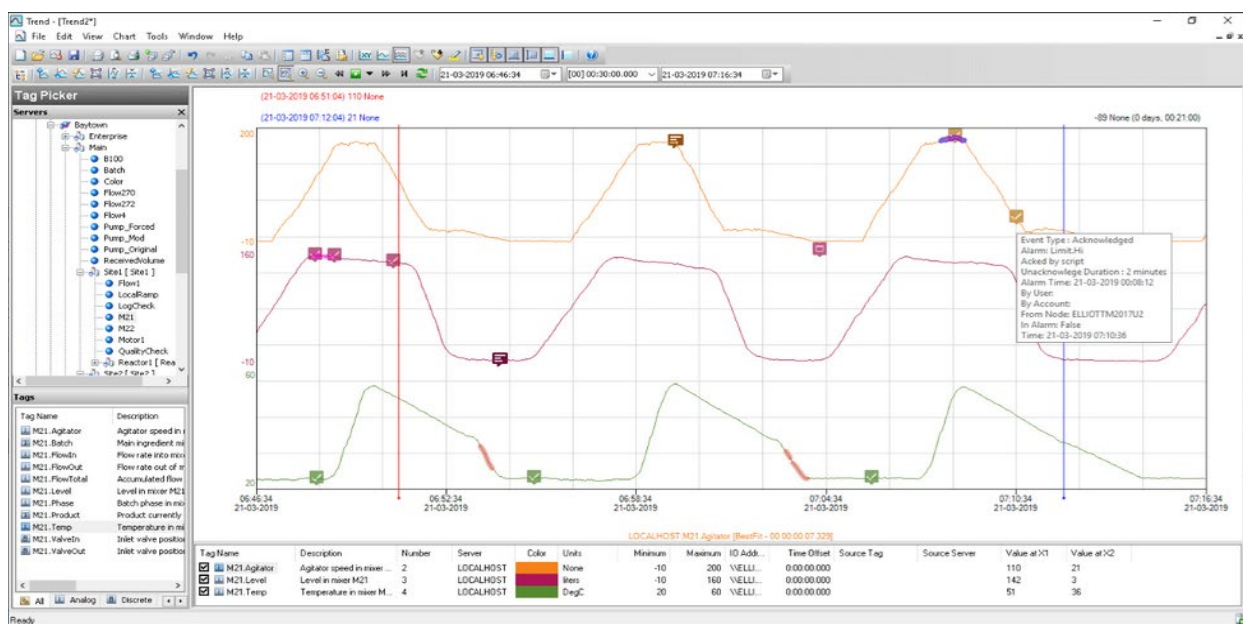


Fig. 3: Detailed analysis of process trends by AVEVA Historian <https://www.aveva.com/en/solutions/operations/operations-control-hmi/>

c2. Quick and easy data query:

- Create your own data queries with over 20 types of „out of the box” queries;
- No SQL skills required, save queries and use them in other applications.

c3. Analysis and reporting using Microsoft Office Add-ins:

- Data analysis and reports, Excel add-on program, Word add-on program via the Microsoft Office utility;
- Creating data reports using functions, formulas, queries and wizards.

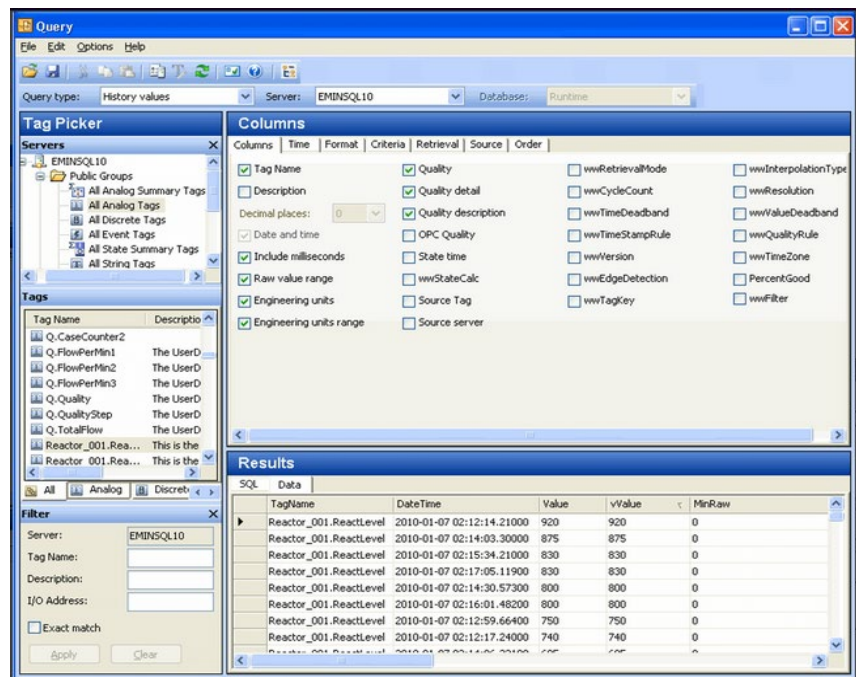


Fig. 4: Presentation of queries by AVEVA Historian

<https://www.aveva.com/en/solutions/operations/operations-control-hmi/>

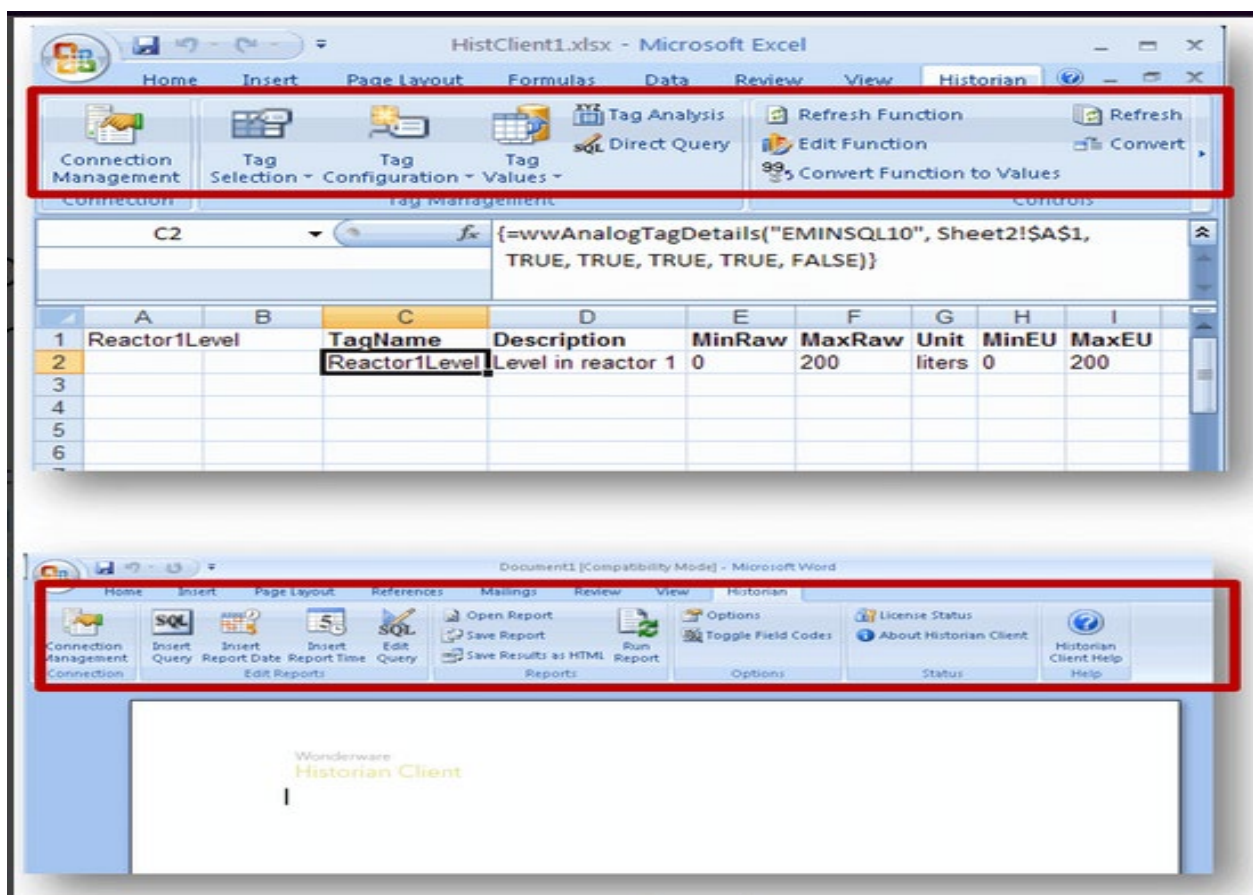


Fig. 5: Representation of the Historian utility for Microsoft Office



**d. Ease of remote access** – Allows access and control of the HMI from any connected computer (complete control, just like a physical HMI). The interaction with the interface should be done through the browser, without purchasing any additional computer software.method (Tag Picker);

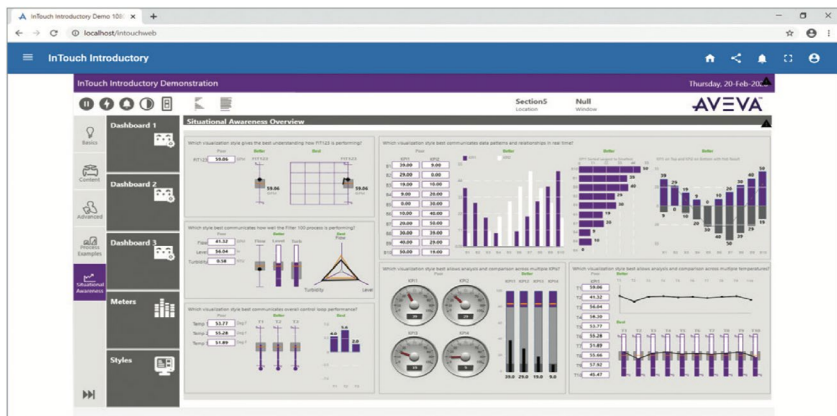
Authorized PC users should be able to interact remotely as follows:

- Monitoring and controlling the on-screen operations of the panel, as if touching the panel itself;
- Testing and troubleshooting the HMI project;
- View, enlarge, print, and save screenshots of active screens.

In addition, remote access should also work on mobile devices such as smartphones or tablets.



**Fig. 7:** . Representation of the HMI simulator which was accessed remotely using the mobile device (Software used: Aveva InTouch HMI)  
<https://www.aveva.com/en/solutions/operations/operations-control-hmi/>



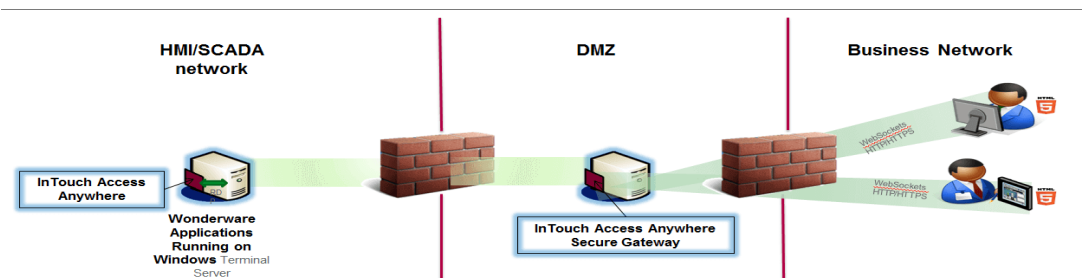
**Fig. 6:** Representation of the HMI simulator which was accessed remotely, using the computer browser (Software used: Aveva InTouch HMI)  
<https://www.aveva.com/en/solutions/operations/operations-control-hmi/>

Authorized users on iPhone, iPad, or Android mobile devices must include:

- Monitoring and controlling the operation of the panel screen as if touching the panel itself;
- Users should be able to save screenshots for review, email, or print;
- It should allow zooming, allowing the user to zoom in on certain objects and then save screenshots, if necessary;
- It should allow Multi-Level Logon Security;
- It should allow simultaneous access for multiple users;

Aveva presents security specifications on how to access users remotely, such as:

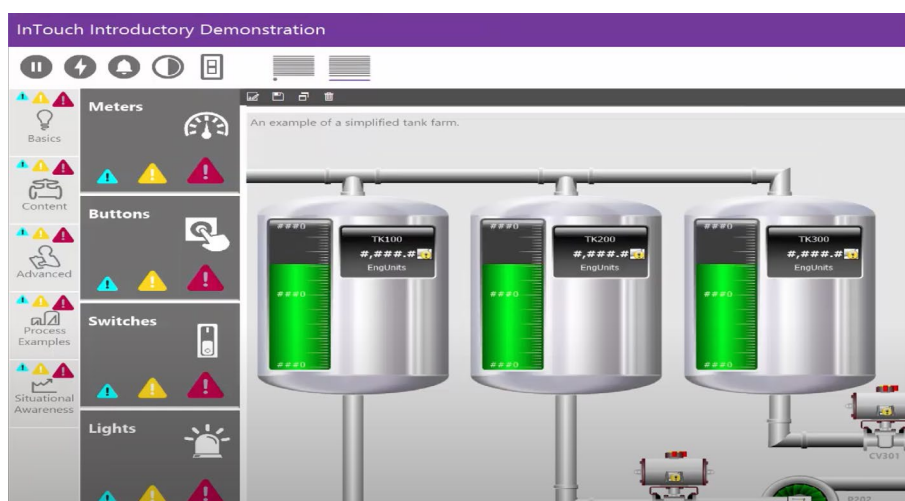
- Security functions that allow their integration with Microsoft Windows, Active Directory, Encryption, Secure Sockets Layer (SSL) and Firewall services;
- Compatibility with architectures involving the use of a DMZ.



**Fig. 8:** Graphical representation of how to secure remote access (Aveva InTouch HMI)  
<https://www.aveva.com/en/solutions/operations/operations-control-hmi/>

**e. Ease of animating the production process** – HMI software should facilitate animation. Animation of machine motions and manufacturing processes can improve comprehension and provide operators with a visual representation of the desired

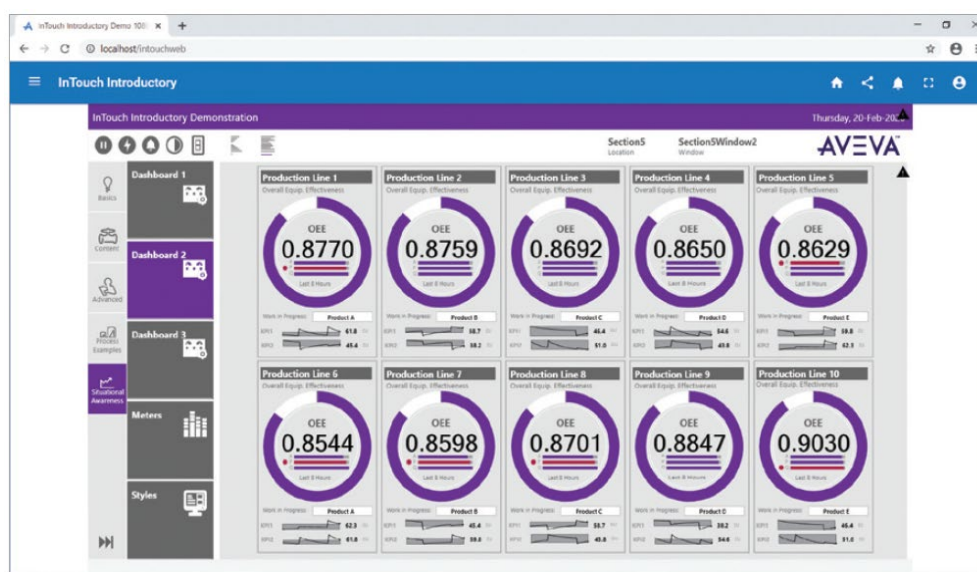
movement of products and machines on the screen. In the event of a breakdown, operators can quickly see the relationship between the position of the product or machine and the sensors or breakdown areas.



**Fig. 9:** Representation of an animation from a HMI simulator (Software used: Aveva InTouch HMI)  
<https://www.aveva.com/en/solutions/operations/operations-control-hmi/>

AVEVA InTouch HMI offers an additional feature, namely, support for web widgets, which are reusable controllers designed using web technology (HTML5). This feature is called a “carousel widget” and enriches the suite of

features offered by the AVEVA InTouch HMI software, allowing the sequential display of a selected set of graphics by automatically rotating them to a configurable predefined range.



**Fig. 10:** Representation of the Carousel HTML5 Widget feature of the Aveva InTouch HMI software  
<https://www.aveva.com/en/solutions/operations/operations-control-hmi/>

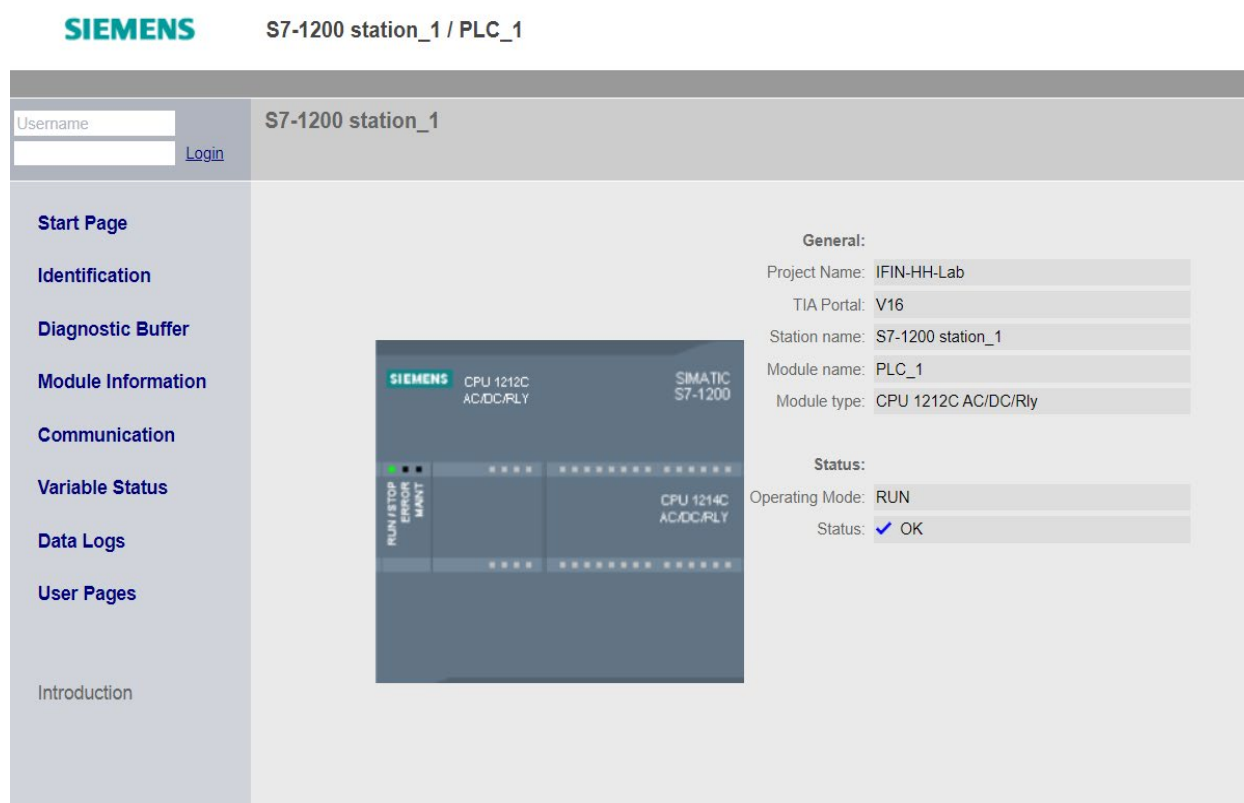
**f. Ease of intuitive use of development tools** – Once an object has been created, it should be possible to give a name to a group of objects or a screen and save them in the HMI software for quick and easy reuse later. It should allow the storage of objects, graphics, sounds and even entire screens.

## SIMULATIONS, RESULTS AND CONCLUSIONS - SIMULATION OF HMI AND RELATED SPECIFIC PROTOCOLS (HTTP)

Conpot has a basic profile (default.xml) that can be modified in order to provide a different behavior for the web server so that an attacker does not notice that it is a simulated interface not a real one. There are many useful features of the Conpot honeypot. One of them and the most important is the HTTP protocol. It makes the connection between an attacker and the simulated equipment. Different features of the equipment can be customized in the

HTTP configuration, which results in a very attractive object for the attacker. Certain values can be set in the HTTP configuration that allow an attacker to interact with the device by changing its operating parameters. In this way the equipment becomes more attractive, and the time spent by the attacker on the HMI interface gives us the opportunity to find out useful information about it. The HMI homepage for the simulated Siemens S7-1200 equipment has been modified by entering information about the project name, station name, module name etc. (Take control of communication. SIMATIC S7-1200 controllers by Siemens, 2021)

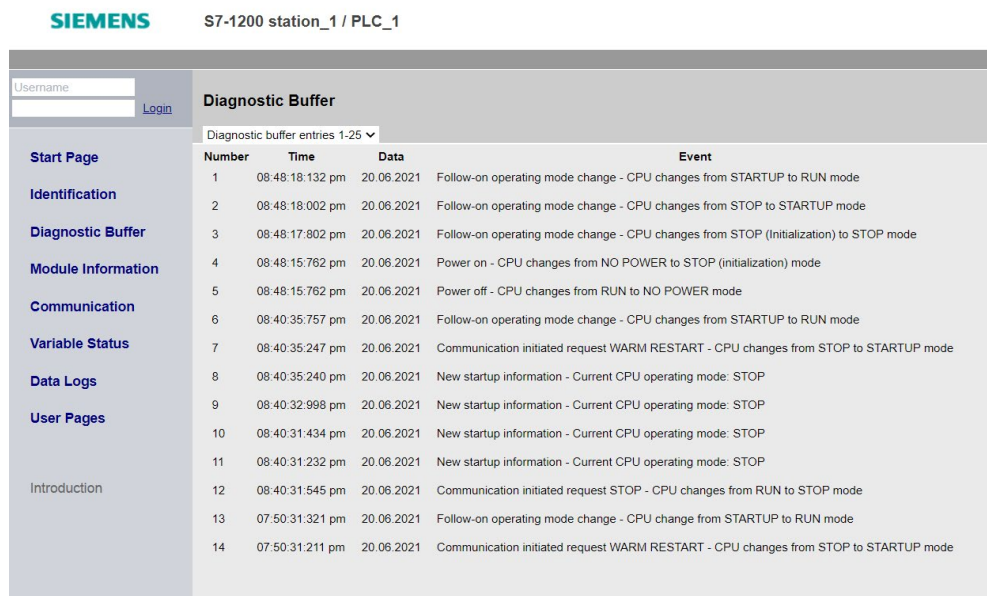
The interface of the module was organized into two frames, identical to the real interface of the simulated equipment. The one on the left contains the menu part of the equipment, and the one on the right, depending on the context, displays logs, offers the possibility to modify the parameters, to download log files, etc.



**Fig. 11:** The HMI homepage for the simulated Siemens S7-1200 equipment  
<https://new.siemens.com/global/en/products/automation/systems/industrial/plc/s7-1200.html>

The Diagnostic Buffer view contains an entry for each diagnostic event of the device. In the image below we have entered 14 diagnostic event entries. Each entry contains the date

and time the event took place, an event category and a short description of the event. Entries are displayed in chronological order with the most recent event at the top.



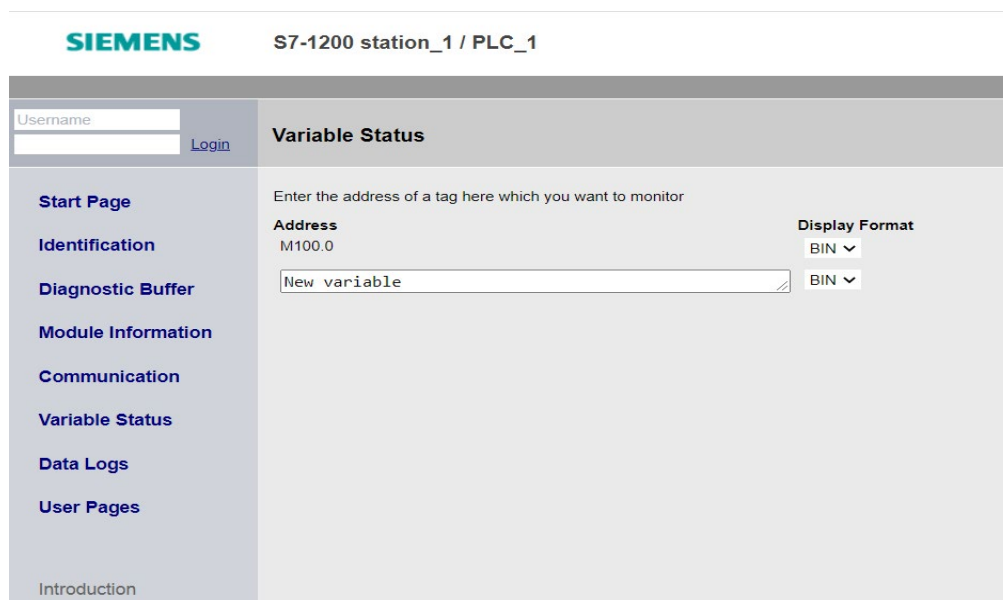
Number	Time	Date	Event
1	08:48:18:132 pm	20.06.2021	Follow-on operating mode change - CPU changes from STARTUP to RUN mode
2	08:48:18:002 pm	20.06.2021	Follow-on operating mode change - CPU changes from STOP to STARTUP mode
3	08:48:17:802 pm	20.06.2021	Follow-on operating mode change - CPU changes from STOP (Initialization) to STOP mode
4	08:48:15:762 pm	20.06.2021	Power on - CPU changes from NO POWER to STOP (initialization) mode
5	08:48:15:762 pm	20.06.2021	Power off - CPU changes from RUN to NO POWER mode
6	08:40:35:757 pm	20.06.2021	Follow-on operating mode change - CPU changes from STARTUP to RUN mode
7	08:40:35:247 pm	20.06.2021	Communication initiated request WARM RESTART - CPU changes from STOP to STARTUP mode
8	08:40:35:240 pm	20.06.2021	New startup information - Current CPU operating mode: STOP
9	08:40:32:998 pm	20.06.2021	New startup information - Current CPU operating mode: STOP
10	08:40:31:434 pm	20.06.2021	New startup information - Current CPU operating mode: STOP
11	08:40:31:232 pm	20.06.2021	New startup information - Current CPU operating mode: STOP
12	08:40:31:545 pm	20.06.2021	Communication initiated request STOP - CPU changes from RUN to STOP mode
13	07:50:31:321 pm	20.06.2021	Follow-on operating mode change - CPU change from STARTUP to RUN mode
14	07:50:31:211 pm	20.06.2021	Communication initiated request WARM RESTART - CPU changes from STOP to STARTUP mode

**Fig. 12:** The Diagnostic Buffer view

<https://new.siemens.com/global/en/products/automation/systems/industrial/plc/s7-1200.html>

In the Variable Status view we allow the attacker to view and modify any of the input / output or memory data of the equipment.

To display data from a memory address, the attacker must enter that address in the „Address” field.



Enter the address of a tag here which you want to monitor

**Address**  
M100.0

**Display Format**  
BIN

New variable

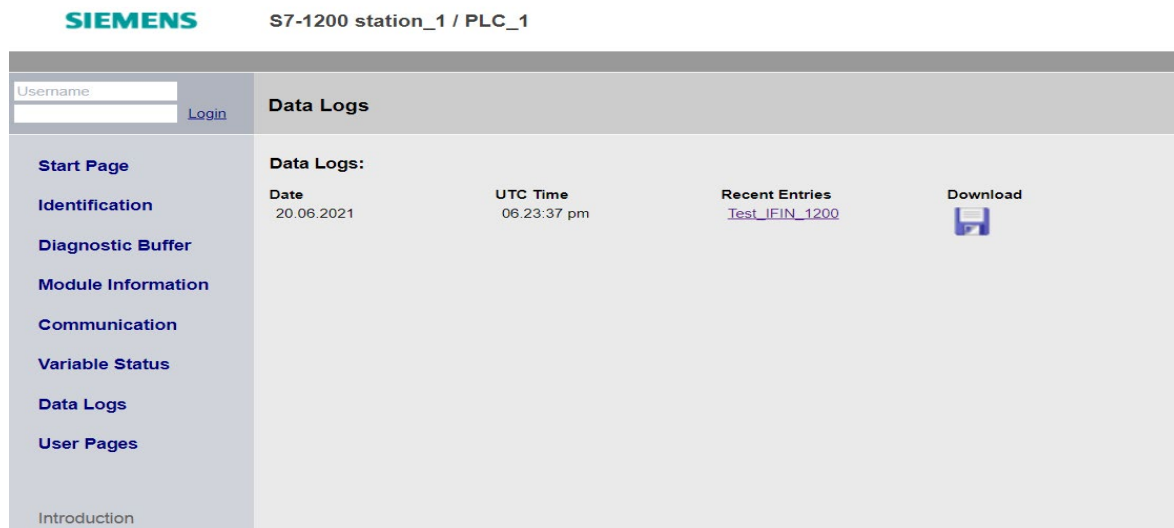
**Fig. 13:** The Variable Status view

<https://new.siemens.com/global/en/products/automation/systems/industrial/plc/s7-1200.html>



The Data Logs view allows the attacker to save the file with the current activity log. In the html page we added an entry containing the date and time when the file was generated, its name and its download link in CSV format.

In practice, the activity log file is persistent in the flash memory of the device. To simulate a real equipment, several entries with real files will be added that will demonstrate the time activity of a real equipment..



**Fig. 14:** The Data Logs view

<https://new.siemens.com/global/en/products/automation/systems/industrial/plc/s7-1200.html>

## ACKNOWLEDGEMENTS

This paper was published in the framework of the project „Center of Excellence for Cyber Security and Critical Infrastructure Resilience (SafePIC)” contract no. 270 / 23.06.2020, ID 120436, financed under the Operational Program Innovations and Competitiveness 2014-2020, Priority Axis 1 - Research, technological development and innovation (RDI) in support of economic competitiveness and business development.

## REFERENCE LIST

- Craig, N. (2018). A new era of HMI. <https://www.oemmagazine.org/technology/automation/article/13274842/a-new-era-of-hmi>, accessed on 26th of September 2021;
- Reiner, E. (2018). Standardizing multi-touch HMI hardware. <https://www.controleng.com/articles/standardizing-multi-touch-hmi-hardware/>, accessed on 23rd of August, 2021;
- Schultz, D. (2021). What is a HMI? International Society of Automation (ISA) Smart Manufacturing & IIoT Division. 2021. <https://blog.isa.org/what-is-an-hmi>, accessed on 15th of September, 2021;
- Take control of communication. SIMATIC S7-1200 controllers by Siemens. <https://new.siemens.com/global/en/products/automation/systems/industrial/plc/s7-1200.html>, accessed on 21st of September 2021.
- Visualize, Control and Optimize Your Operations, 2021. Aveva in Touch. <https://www.aveva.com/en/products/intouch-hmi/>, accessed on 27th of September, 2021.