

W&T

www.WuT.de

ethernet security data sheet

(complies with the IAONA security data sheet)

Name of Item		Web-IO 12xDigital			
Description		Network device for Input/Output control			
Type	X	a device (any device, active and passive device, switches,...)		a production cell	a network (infrastructure)
Operating System		W&T embedded operating system for Web-IO			
Network Interface		Ethernet 10/100BaseT autosensing			
Backup/Replacement features/procedure		Manually by user or guided replacement with Wutility Tool			
Firmware Update		Manually by TFTP or automatically by Wutility Tool			
External Interface		12 digital industry standard inputs Type 1, current consumption according to IEC 1131-2, 3 groups at 4, isolated, 12 digital outputs in 12V or 24V industrial standard Transistor			
Behavior on power loss		Automatically startup after power on			
Certification		CE conformity			
Implemented Security Features			Network Features		
	Firewall, not configurable		X	Needs/provides DHCP/BootP	
	Firewall,configurable		X	Manageable	
X	Virus detection, protection			MAC-address based authentication	
	Data encryption			IP-address based authentication	
	Intrusion detection				
X	Robustness, stack overflow protection			Service and Maintenance	
	Redundancy possible			Logging	
X	Secure remote maintance		X	Ready for remote maintenance	
X	Access control, user levels			Provides local configuration	
	Local user access possible		X	Provides remote configuration	
	Supports user authentication, manageable				

For more informations: <http://www.wut.de>

Release Date: 09.09.2005

Version: 1.0 beta

Data sheet complies with the rules set in the IAONA Handbook for Network Security (Version 1.0) IAONA Data Sheet v01.00

Used network ports and services

No.	Service	Port(s)	TCP	UDP	Other	Client	Server	Protected	Can be disabled	Needed for operation	Local service / Maintenance	Remote service / Maintenance	Description	Security Rating	Security Classification
1	BootP			X				no	yes	no	no	yes	Protocol for remote IP address configuration	2	2
2	HTTP	0..65535 def. 80	X				X	yes		yes	no	yes	Hypertext Transfer Protocol for Web-based Management	3	4
3	Binary 1	0..65535 def. 49153	X	X			X	yes	yes	*	no	no	Socket Port for binary access, OPC access and Box-to-Box connection. TCP client or server or UDP peer possible	3	4
4	Binary 2	0..65535 def. 49154	X	X			X	yes	yes	*	no	no	Socket Port for binary access, OPC access and Box-to-Box connection. TCP client or server or UDP peer possible	3	4
5	UDP-ASCII	0..65535 def. 42279		X				yes	yes	*	no	no	Socket Port for UDP ASCII Command access	3	3
6	SMTP	25	X			X		yes	yes	*	no	no	Simple Mail Transfer Protocol	3	3
7	SMTP after POP	25,11	X			X		yes	yes	*	no	no	Simple Mail Transfer Protocol with POP3 authentication	4	4
8	TCP Alarm	0..65535	X			X		yes*	yes	*	no	no	Alarm over UDP sockets	5	5
9	UDP Alarm	0..65535		X				yes*	yes	*	no	no	Alarm over TCP sockets	5	5
10	SNMP	161,162		X				yes	yes	*	no	no	Simple Network Management Protocol	3	5

Used network ports and services

No.	Service	Port(s)	TCP	UDP	Other	Client	Server	Protected	Can be disabled	Needed for operation	Local service / Maintenance	Remote service / Maintenance	Description	Security Rating	Security Classification
11	Syslog	0..65535		X				yes*	yes	*	no	no	System Message Logging	5	5
12	Inventory	8513		X				yes*	no	no	no	no		5	5
13	Softreset	8888	X					yes	no	no	no	yes	Remote Software Reset (password protected)	2	3
14	Init Update	8002	X					yes	no	yes	no	yes	Initialize port for secured firmware update	4	5
15	TFTP for Firmware-Update	69		X				yes	no	yes	no	yes	Trivial File Transver Protocol for firmware update	4	5
16	Get Config	8003	X					yes	no	yes	no	yes	Port for reading device configuration	2	3
17	Put Config	8004	X					yes	no	yes	no	yes	Port for writing device configuration	2	3

* = depending on application

yes* = send only service, no data receipt on open port

Legend:	Security Rating: 1 - unsecure mechanisms, unprotected; 2-2minimum security; 3 - common security features, basic protection; 4 - most security features available; 5 - fully protected, state-of-the-art security
	Security Classification: 1 - not recommended to use; 2 - maybe use with caution; 3 - usually advisable; 4 - low risk, advisable to use; 5 - highly recommended
Release Date: 09.09.2005	Version: 1.0 beta
Data sheet complies with the rules set in the IAONA Handbook for Network Security (Version 1.0) IAONA Data Sheet v01.00	