

C1	13/01/14	Seconda emissione	AS	DB	GZ
C0	30/08/13	Prima emissione	AS	DB	GZ
REVISIONE			DESCRIZIONE		
			EL.	CON.	APP.

MINISTERO DELLE INFRASTRUTTURE E DEI TRASPORTI
MAGISTRATO ALLE ACQUE

**NUOVI INTERVENTI PER LA SALVAGUARDIA
DI VENEZIA**

LEGGE N.798 DEL 29-11-1984

CONVENZIONE REP. 7191 DEL 04-10-1991

ATTO ATTUATIVO A VALERE SU X ASSEGNAZIONE CIPE PER IL SISTEMA MOSE (10B)

**INTERVENTI ALLE BOCCHE LAGUNARI PER
LA REGOLAZIONE DEI FLUSSI DI MAREA**

CUP: D51B02000050AD1

PROGETTO ESECUTIVO

(estratto Perizia di variante LN.L1.50.PE.04 favorevolmente esaminata dal CTM del 27/01/11 con voto n. 9 ed aggiornamento dei progetti esecutivi di WBS MA.L1.50 e CH.L1.50, favorevolmente esaminati rispettivamente dal CTM del 21/04/10 con voto n. 66 e del 18/09/09 con voto n. 158)

WBS: LN.L1.50 - MA.L1.50 - CH.L1.50

WBE: LN.L1.50.PE.04F - MA.L1.50.PE.11 - CH.L1.50.PE.11

BOCCHIE DI LIDO – MALAMOCCO – CHIOGGIA

IMPIANTI

IMPIANTI DI CONTROLLO – II FASE



**COMUNICAZIONE ED INTERFACCIAMENTO
SPECIFICA TECNICA**

ELABORATO A. Scarpa	CONTROLLATO D. Bortolotto	APPROVATO G. Zoletto
N. ELABORATO MV100P-PE-GIS-5001-04F	CODICE FILE MV100P-PE- GIS-5001-04F.doc	DATA 13 gennaio 2014

CONSORZIO “VENEZIA NUOVA”

COORDINAMENTO PROGETTAZIONE		PROGETTAZIONE ESECUTIVA
VERIFICATO V. Ardone	CONTROLLATO M. Trossello	
 CONSORZIO VENEZIA NUOVA		   

OPERA PROTETTA AI SENSI DELLA LEGGE 22 APRILE 1941 N° 633 TUTTI I DIRITTI RISERVATI
 QUALSIASI RIPRODUZIONE ED UTILIZZAZIONE NON AUTORIZZATE SARANNO PERSEGUITE A RIGORE DI LEGGE

		Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 2
		Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

MINISTERO DELLE INFRASTRUTTURE E DEI TRASPORTI

MAGISTRATO ALLE ACQUE

NUOVI INTERVENTI PER LA SALVAGUARDIA DI VENEZIA

LEGGE N.798 DEL 29-11-1984

CONVENZIONE REP. 7191 DEL 04-10-1991

ATTO ATTUATIVO A VALERE SU X ASSEGNAZIONE CIPE PER IL SISTEMA MOSE (10B)

CONSORZIO VENEZIA NUOVA

**INTERVENTI ALLE BOCCHE LAGUNARI PER LA REGOLAZIONE DEI FLUS-
SI DI MAREA**



- PROGETTO ESECUTIVO -

BOCCHES DI LIDO – MALAMOCCO – CHIOGGIA

IMPIANTI



IMPIANTI DI CONTROLLO II FASE

**COMUNICAZIONE ED INTERFACCIAMENTO
SPECIFICA TECNICA**

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 3
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

INDICE

1.	SCOPO	4
2.	NORME E LEGGI	5
3.	ACRONIMI	6
4.	DATI DI PROGETTO E RIFERIMENTI	8
4.1.	Documentazione di riferimento	8
5.	ARCHITETTURA DEL SISTEMA DI CONTROLLO	9
5.1.	Premesse sulla Topologia Connettiva	9
5.2.	Topologia Connettiva e Protocolli di Interfacciamento	11
5.3.	Comunicazioni Geografiche Private	12
5.4.	Comunicazioni Extranet.....	14
5.5.	Comunicazioni Geografiche Pubbliche (Esterne).....	14
5.6.	Monitoraggio delle comunicazioni	14
5.7.	Schema Connettivo Complessivo	14
5.8.	Criteri di Sicurezza ed Integrità	17
5.9.	Sotto-Impianti	21
5.9.1.	Criterio Generale di Integrazione	22
5.9.2.	Distribuzione Elettrica (PMS)	22
5.9.3.	Compressori.....	22
5.9.4.	Generatori di emergenza.....	23
5.9.5.	Videosorveglianza Interfonia.....	23
5.10.	Sale di Controllo.....	24



 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 4
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

1. SCOPO

La presente WBE LN.L1.50.PE.04F - MA.L1.50.PE.11 - CH.L1.50.PE.11 “Impianti di controllo – II fase” si riferisce alle tre bocche di Lido, Malamocco e Chioggia e si pone come obiettivo quello di implementare il relativo sistema di controllo: parte hardware e software completa.

Tra gli impianti ai quali il sistema di controllo del processo (PCS – *Process Control System*) dovrà interfacciarsi, vi è il sistema di gestione della distribuzione elettrica del MOSE (PMS – *Power Management System*), che è di fatto un impianto Standard, nella classificazione posta alla base del presente progetto esecutivo.

La realizzazione del sistema PMS non è ricompresa nella presente WBE: scopo del presente documento è definire i criteri di interfacciamento di tale impianto con il sistema PCS, vista l'importanza e strategicità della distribuzione elettrica ai fini del funzionamento delle opere di salvaguardia.

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 5
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

2. NORME E LEGGI



Si fa riferimento alle seguenti Norme Tecniche, per quanto applicabili:

- UNI / ISO
- CEI – IEC
- IEEE 802.x
- CE – ATEX
- IETF – RFC

Tutti i documenti applicabili saranno considerati parte integrante della presente specifica.



Requisiti, limiti e disposizioni non specificatamente menzionati nella presente specifica dovranno essere conformi a detti documenti applicabili.

Laddove vi fossero difformità, la presente specifica avrà priorità sui documenti di riferimento applicabili.



		Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 6
		Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

3. ACRONIMI

- CPU: Unità centrale di elaborazione (*Control Process Unit*)
- CR: Sala di Controllo (*Control Room*)
- CRC: Controllo a ridondanza ciclica (*Cyclic Redundant Check*)
- DCS: Sistema di controllo distribuito (*Distributed Control System*)
- DVR: Videoregistratore digitale (*Digital Video Recorder*)
- ESD: sistema di emergenza (*Emergency Shut Down System*)
- ESDSC: Consolle del sistema di emergenza (*Emergency Shutdown System Consolle*)
- FAT: collaudo in fabbrica (*Factory Acceptance Test*)
- FCS: unità di controllo di campo (*Field Control Station*)
- GPS: sistema di posizionamento globale (*Global Positioning System*)
- HART: protocollo di comunicazione tramite doppino (*Highway Addressable Remote Transducer*)
- HDD: Hard Disk Drive
- HIS: Stazione d'interfaccia umana (*Human Interface Station*)
- HMI: Interfaccia uomo macchina (*Human Machine Interface*)
- HSBY: ridondanza firmware a caldo (*hot standby*)
- HVAC: sistema di climatizzazione (*Heating, Ventilation and Air Conditioning*)
- IDS: sistema di rilevazione delle intrusioni (*Intrusion Detection System*)
- IPS: sistema di prevenzione delle intrusioni (*Intrusion Prevention System*)
- MTTF: Tempo medio di guasto (*Mean Time To Failure*)
- MTTR: Tempo medio di ripristino (*Mean Time To Repair*)
- PC: Personal Computer
- PCS: Sistema di controllo del processo (*Process Control System*)
- PID: Controllore Proporzionale, Integrato e Derivativo (*Proportional-Integral-Derivative*)
- PLC: Controllore logico programmabile (*Programmable Logic Controller*)
- PMS: Sistema di gestione distribuzione elettrica (*Power Management System*)

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 7
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

- QCK: Quadro Controllo Comandi
- RAID: Insieme ridondante di dischi indipendenti (*Redundant Array of Independent Disks*)
- RCE: Registrazione Cronologica degli Eventi
- RFC: Request For Comment
- RIO: Schede Input/Output Remote (*Remote I/O*)
- RN: Nodi di controllo posti in campo (*Remote Node*)
- RTT: Round Trip Time
- SAC: Sala di Automazione e Controllo
- SAT: collaudo in sito (*Site Acceptance Test*)
- SIL: livello di integrità della sicurezza (*Safety Integrity Level*)
- SNMP: Simple Network Management Protocol
- TCP/IP: Transmission Control Protocol – Internet Protocol
- UPS: Gruppo di continuità (*Uninterruptible Power Supply*)
- UML: Linguaggio Unificato per la Modellazione (*Unified Modeling Language*)
- VLAN: Rete locale virtuale (*Virtual Local Area Network*)
- VPN: Percorso di rete virtuale (*Virtual Path Network*)

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 8
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	



4. DATI DI PROGETTO E RIFERIMENTI

Si rimanda ai documenti del progetto esecutivo dell'impianto elettrico, per eventuali dettagli.

4.1. Documentazione di riferimento

La presente specifica comprende, come parte integrante, anche i seguenti elaborati :

- Dati di base della Progettazione MV100P-PE-GZR-0002
- Condizioni generali di Fornitura MV100P-PE-GZS-0005
- Specifica tecnica sistema di controllo MV100P-PE-GIS-0137-04F
- Relazione tecnica processo e Appendice NMV100P-PE-GIR-0004-04F
- Architettura dei sistemi di controllo MV100P-PE-L/M/CIK-3001-04F
- Disposizioni consolle operatore in sala controllo MV100P-PE-L/M/CID6521-04F

		Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 9
		Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

5. ARCHITETTURA DEL SISTEMA DI CONTROLLO

Per ognuna delle bocche è previsto un sistema di controllo funzionalmente indipendente e segregato rispetto agli altri, coordinabile/supervisionabile da una sala di controllo di bocca e da una sala di controllo di opera (“Stazione Centralizzata”).

Per l'automazione di ciascuna delle bocche (Chioggia, Malamocco, Lido - San Nicolò / Treporti) è prevista una organizzazione dell'automazione realizzata mediante “impianti componenti”/”sotto sistemi” raggruppabili in 3 tipologie: principali, standard, package.

La gestione dell'automazione della distribuzione elettrica PMS (*Power Management System*) ha una componente strettamente locale a ciascuna bocca ed una componente di automazione complessiva a livello di opera.



La distribuzione elettrica di una bocca può avere come fonti di alimentazione energetica la fornitura da parte dell'Ente distributore o può avvenire per mezzo di generatori diesel, per la cui logica di funzionamento e di intervento si rimanda alla MV100P-PE-GIR-0004-04F ed alla relativa appendice N, e comunque al progetto esecutivo della relativa WBE elettrica.

Oltre alla supervisione della gestione del sottosistema PMS relativo alla singola bocca, pertanto, è necessario considerare la presenza di un sistema di automazione/supervisione che gestisca la commutazione delle fonti energetiche a supporto di ciascuna bocca.

5.1. Premesse sulla Topologia Connettiva

La grande quantità di dispositivi (sensori/attuatori) che necessitano per il controllo dell'opera e la loro articolata distribuzione geografica implicano una decomposizione funzionale secondo criteri gerarchici in impianti e sotto impianti e ciò implica la necessità di una articolata struttura connettiva/comunicativa tra le parti componenti il sistema di controllo ed automazione.

La scomposizione funzionale degli impianti che compongono l'opera e la necessità di avere livelli adeguati di ridondanza - sia in ciascun apparato/funzione che nelle

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 10
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

comunicazioni necessarie per ottenere un sistema complessivo integrato - impone di gestire diverse topologie connettive organizzate su più livelli di comunicazione.

A parità di elementi costituenti la struttura di controllo ed automazione dell'intera opera, sono possibili diverse topologie connettive che determinano valori diversi sia di disponibilità dell'opera sia di affidabilità della medesima

La topologia comunicativa è caratterizzata da due elementi aggiuntivi rispetto ai dispositivi (sensori/attuatori) del sistema di controllo che sono:

- collegamenti passivi (mezzi trasmissivi)
- apparati di rete (elementi attivi che implementano i protocolli di rete)



Gli apparati di rete che utilizzano come protocollo di comunicazione “ethernet” hanno una topologia implicita rappresentata dalla modalità “star”, spesso indicata anche come “bus” realizzata da un elemento fisico detto “switch” che funge da interconnessione, e sono caratterizzati da un tempo di accesso al mezzo di trasmissivo non deterministico.

Per innalzare l'affidabilità della comunicazione è necessario operare moltiplicando opportunamente sia gli apparati di rete del singolo dispositivo sia i collegamenti passivi e gli switch di interconnessione, che consentono la formazione del canale di comunicazione tra le parti.

Gli switch (a differenza degli hub) hanno il grande pregio di confinare le collisioni di traffico (dominio di collisione) che rendono non deterministico l'accesso al mezzo trasmissivo.

Per rendere deterministico il tempo di accesso al mezzo trasmissivo senza perdere il vantaggio della grande diffusione del protocollo ethernet devono essere introdotte a livello applicativo (livello 7 della pila ISO/OSI) delle regole di accesso per i diversi dispositivi comunicanti.

L'interconnessione degli switch permette la realizzazione di una topologia a “ring” che consente di avere due percorsi di accesso un dispositivo connesso ad uno qualsiasi degli switch che compongono il ring, con il vantaggio di un cablaggio meno dispendioso.



		Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 11
		Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

L'utilizzo di due ring per raggiungere un dispositivo permette quindi di avere 4 percorsi di accesso al medesimo dispositivo abbassando notevolmente una eventuale indisponibilità del dispositivo causata da problemi di comunicazione.

5.2. Topologia Connettiva e Protocolli di Interfacciamento

L'architettura delle comunicazioni locali private tra i diversi “elementi” dell'opera è organizzata su tre (quattro) diversi livelli:

- un livello (**Layer Device**) destinato alla comunicazione tra gli elementi Remoti o meno adibiti alla conversione analogico/digitale dei segnali I/O (RIO) del sistema di controllo ed i dispositivi (**Device**) componenti il sotto sistema, realizzato in modalità:
 - Analogica
 - Hardwired
 - Digitale
 - Hardwired + HART (utilizzato nei sensori (input analogici) che necessitano di operazioni di taratura senza che vi sia l'accessibilità fisica al device)
 - Profibus DP (utilizzato solo nel caso delle valvole delle linee di controllo pneumatico delle paratoie)
 - Modbus RTU (utilizzato per i device la cui complessità comporta un gran numero di segnali (I/O) da gestire)
- un livello (**Layer Campo**) destinato alla comunicazione tra i PLC e gli apparati remoti di campo (RIO) di ciascun “sotto sistema” basato su una topologia ad anello ridondato. Il riferimento, in tutti i documenti di progetto, allo standard Ethernet per i livelli 1-2 della pila ISO/OSI del Layer campo è da intendersi puramente indicativo e non vincolante, pur rimanendo strettamente necessaria e vincolante la rispondenza ai criteri di ridondanza e disponibilità che sottendono l'intero impianto.

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 12
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

- un livello (**Layer Bocca**) destinato alla comunicazione tra i PLC di automazione di ciascuno dei diversi “sotto sistemi” e di comunicazione verso i dispositivi che consentono la supervisione e realizzano le HMI (*Human Machine Interface*) basato a livello 1-2 della pila ISO/OSI sullo standard Ethernet con topologia **BUS** e basato a livello 3-4 della pila ISO/OSI sullo standard TCP/IP ed a livello applicativo preferibilmente su MODBUS/TCP. (**Backbone di Bocca BB**)
- un livello (**Layer PLC**) non sempre presente, destinato alla comunicazione tra i diversi PLC che realizzano l'automazione di uno specifico “sotto sistema” come ad esempio il caso del sistema pneumatico di sollevamento paratoie (PCS - *Process Control System*) o il Sistema di Emergenza (ESD - *Emergency Shut Down*) basato a livello 1-2 della pila ISO/OSI sullo standard Ethernet con topologia RING e basato a livello 3-4 della pila ISO/OSI sullo standard TCP/IP. (**Ring Controllo**)



L'architettura delle comunicazioni geografiche private (**Layer Opera**) tra le diverse Bocche e la Stazione Centralizzata è basato a livello 1-2 della pila ISO/OSI sullo standard Ethernet con topologia **BUS** ed a livello 3-4 della pila ISO/OSI sullo standard TCP/IP. (**Backbone di Opera BO**)

Gli spazi di indirizzamento IPv4 dei livelli sopra descritti prevedono l'utilizzo di subnet private (RFC 1819) distinte per siti geograficamente distinti (Bocca) e prevedono l'utilizzo di subnet private diverse tra ring di campo e ring di controllo/backbone di Bocca.

5.3. Comunicazioni Geografiche Private

I link che collegano gli switch/router, che realizzano i “Backbone di Bocca”, con lo switch/router, che realizza il “Backbone di Opera”, utilizzano le fibre ottiche previste nell’ambito dei seguenti progetti in fase di realizzazione: anello di interconnessione in fibra tra le bocche (WBE: LN.L1.50.PE.12 / MA.L1.50.PE.05 / CH.L1.50.PE.05) e teleguidata Lido – Arsenale (WBE: LN.L1.50.PE.04C).

Il percorso dei cavi che raggiungono ciascuna delle bocche e la numerosità delle fibre in essi contenuti consente svariate configurazioni topologiche e quindi permette di operare in futuro modifiche della topologia di connessione oltre a permettere variazioni nella dislocazione geografica del “Backbone di Opera”.

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 13
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

Il percorso dei cavi e la numerosità delle fibre in essi contenuti permettono notevoli ampliamenti della capacità di banda utilizzabile per interconnettere le località coinvolte e consente la realizzazione di strutture connettive dedicate con capacità di traffico reciprocamente indipendenti.

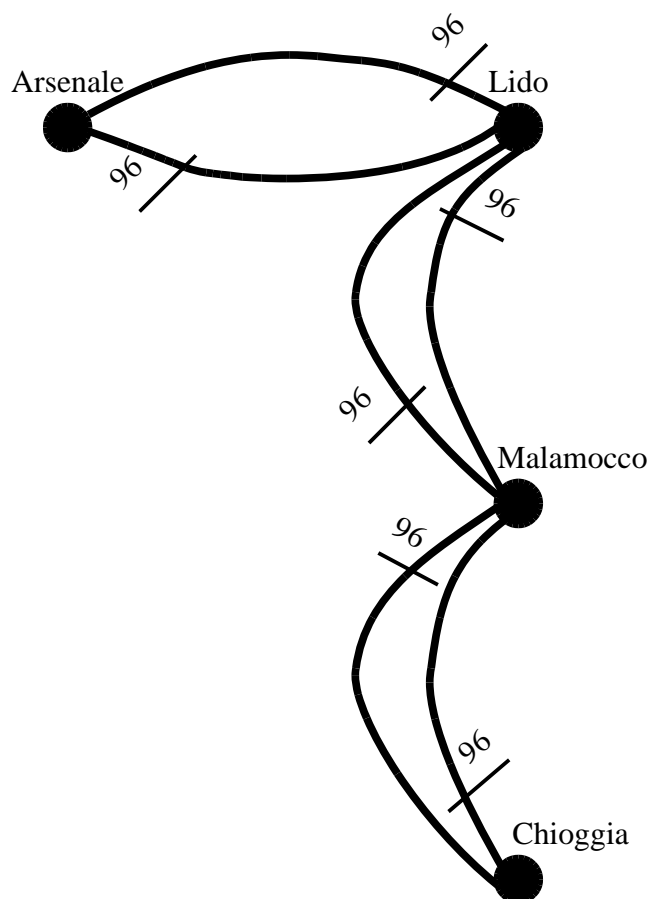




Figura 1 - Topologia cavi di interconnessione delle bocche

Il digramma riportato in figura 1 rappresenta la topologia logica dei cavi che realizzano la struttura comunicativa tra le bocche ed evidenzia che alle bocche di Malamocco e Lido saranno presenti 4 cavi da 96 fibre (96x4 fibre) mentre a Chioggia ed all'Arsenale saranno presenti 2 cavi da 96 (96x2 fibre).

Operando sulla attestazione dei cassette ottici mediante opportune patch sono possibili svariate configurazioni topologiche ridondate (stella/anello) lasciando quindi aperti tutti i potenziali scenari di evoluzione della architettura di comunicazione a supporto dell'automazione.

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 14
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

5.4. Comunicazioni Extranet

L'interfacciamento “Extranet” verso sistemi esterni cooperanti con conseguente trasporto di informazioni su mezzi trasmissivi fuori del controllo fisico del gestore dell'opera richiede che:

- esista uno spazio di indirizzamento locale distinto da quelli sopra descritti
- esso sia concordato con le entità cooperanti partecipanti alla “extranet” coinvolte (deve essere governato/risolto il problema dell'utilizzo della medesima subnet da parte di entità distinte che impedisce il corretto raggiungimento di tutti gli indirizzi IP coinvolti)

5.5. Comunicazioni Geografiche Pubbliche (Esterne)

La connessione dell'intero sistema di controllo di tutte le bocche con eventuali reti esterne all'impianto (comunicazioni geografiche pubbliche), per il solo trasferimento di informazioni selezionate, può avvenire solo presso la stazione centralizzata e per tramite di firewall in configurazione DMZ.



5.6. Monitoraggio delle comunicazioni

La presenza di un così elevato numero di apparati di comunicazione, anche a livello di singola bocca, determina la necessità di aver sia a livello di bocca che a livello di opera un sistema di monitoraggio basato su protocollo SNMP (Simple Network Management Protocol) che permetta di verificare:

- raggiungibilità di tutti gli elementi
- volumi di traffico
- pacchetti persi
- RTT (Round Trip Time)

5.7. Schema Connettivo Complessivo

In Figura 2 è riportato lo schema connettivo complessivo privo delle ridondanze riguardanti sia gli apparati attivi che i link passivi, e privo delle molteplicità presenti in

		Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 15
		Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

ciascun livello delle comunicazioni previste per il controllo e l'automazione dell'intera opera.

Con il simbolo “**Server**” riportato sia a livello di “Backbone di Opera” che a livello di “Backbone di Bocca” sono indicate in modo sintetico tutte le diverse tipologie di server (HMI, Configuration/Scenari, Historian, Integration Operation/Maintenance)

Con il simbolo “**Client HMI**” viene rappresentato l’insieme di tutti i client che si vorranno dislocare sul “Backbone di Bocca” e/o sul “Backbone di Opera”

Con il simbolo “**Remote Client HMI**” viene rappresentato l’insieme di tutti i client che si vorranno dislocare in luoghi esterni al perimetro fisico dell’opera. Rientrano in questa categoria ad esempio gli eventuali Client HMI dislocati presso il MAV.

Decomposizione Gerarchica delle Strutture Connettive

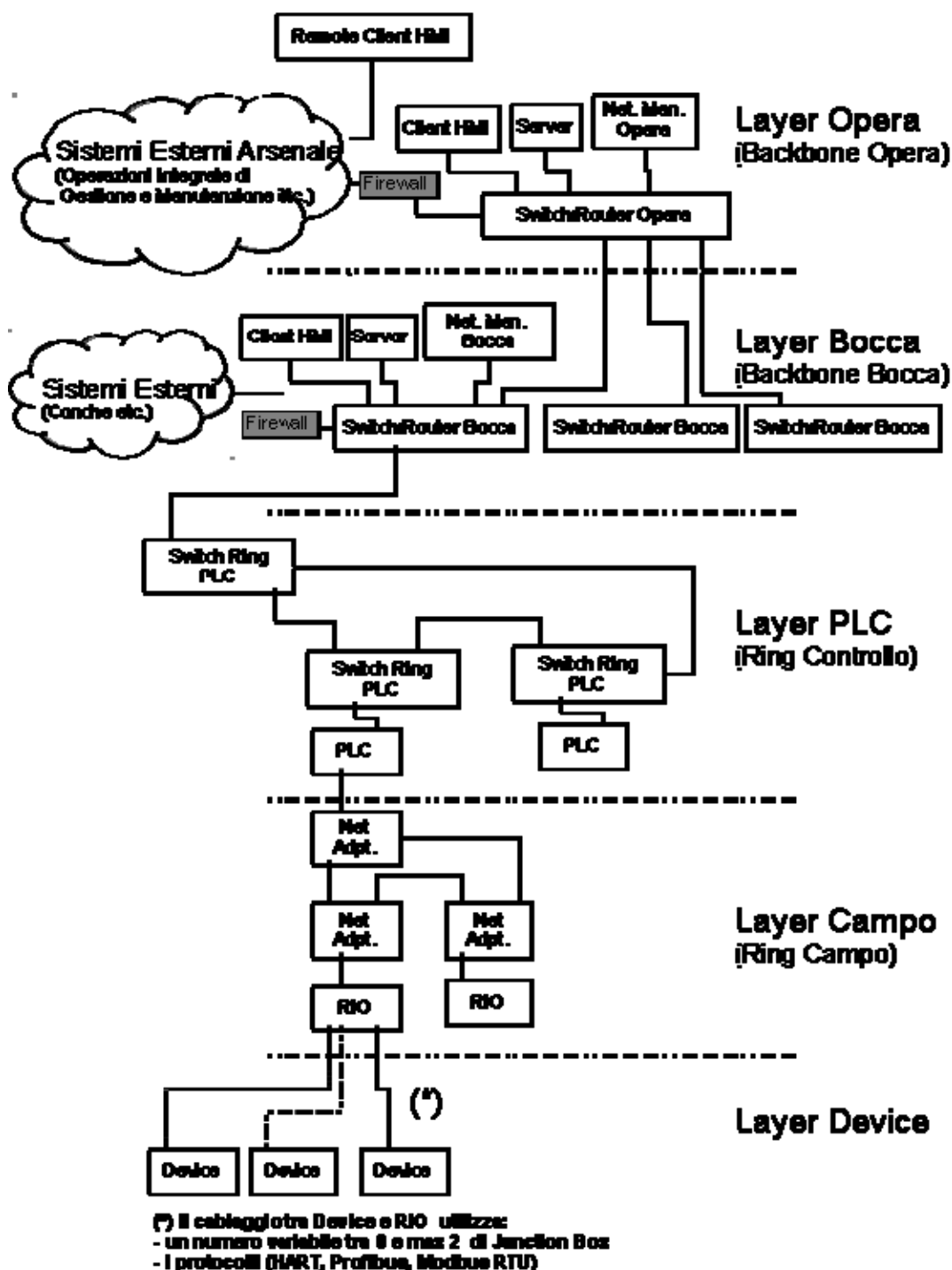




Figura 2 – Schema connettivo complessivo

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 17
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

5.8. Criteri di Sicurezza ed Integrità

Procediamo alla classificazione degli elementi che compongono la intranet di opera:

Sono **elementi interni** alla intranet dell'opera tutti gli apparati che risultino:

1. Collocati fisicamente entro il **perimetro geografico sorvegliato** dell'opera, ad **accesso fisico controllato** e consentito solo a personale dotato degli opportuni profili di sicurezza e gestione sistemistica riservata a personale dotato di opportuni profili di sicurezza
2. Collegati mediante mezzi trasmissivi e apparati di comunicazione fisicamente entro il **perimetro geografico sorvegliato** dell'opera, ad **accesso fisico controllato** e consentito solo a personale dotato degli opportuni profili di sicurezza e gestione sistemistica riservata a personale dotato di opportuni profili di sicurezza.

Sono **elementi di frontiera** della intranet dell'opera gli apparati che presentino una o più porte di comunicazione collegate ad apparati collocati fuori del perimetro geografico sorvegliato e/o ad accesso fisico non controllato.



Sono **elementi extranet** tutti gli apparati che non appartengano alle precedenti due categorie ma che siano elementi di frontiera od interni della intranet di un soggetto qualificato con il quale vi sia la necessità di una interoperabilità.

Sono **elementi esterni** tutti gli apparati che non appartengano a nessuna delle categorie precedenti.

Tutte le comunicazioni verso elementi delle extranet realizzate con soggetti qualificati debbono transitare solo e soltanto attraverso gli elementi di frontiera.

Gli elementi di frontiera debbono essere dotati di funzioni di firewalling, di IDS (Intrusion Detection System) e di IPS (Intrusion Prevention System) e tassativamente sottoposti ai criteri di aggiornamento suggeriti dal fornitore.

Gli elementi di frontiera devono essere fisicamente collocati in aree geografiche sorvegliate e con accesso fisico consentito solo a personale dotato del profilo di massima sicurezza e parimenti la gestione sistemistica dei medesimi deve essere effettuata esclusivamente da personale dotato del profilo di massima sicurezza.

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 18
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

Tutte le operazioni di gestione sugli elementi di frontiera devono essere registrate, abbinate alle credenziali utilizzate per operare le modifiche (log) secondo apposite procedure che garantiscano la non alterabilità dei dati di registrazione e la replicazione di tali registrazioni in apposito sito esterno soggetto a conservazione protetta.

Da quanto sopra ne discende che per i client HMI le funzioni per loro tramite esplicabili devono essere funzione delle/a:

- Credenziali dell'operatore
- Dislocazione fisica del client HMI



In particolare tutti i client dislocati fuori del perimetro fisico di massima sicurezza devono poter esercitare le sole funzioni di consultazione e non quelle di attuazione.

Le regole di firewalling implementate devono garantire in prima battuta che:

- il comportamento di default per qualsiasi elemento interno o di frontiera sia la negazione di qualsiasi comunicazione (Deny All) ad eccezione di quanto sotto elencato
- le comunicazioni verso elementi extranet autorizzati siano iniziate esclusivamente da elementi di frontiera od interni autorizzati
- l'accesso alle subnet locali dell'opera sia protetto con regole di firewall che impediscano per default **tutte** le comunicazioni che non siano strettamente necessarie alle comunicazioni con altre entità.

I livelli di cui al paragrafo 5.2 realizzano una segregazione fisica del traffico e l'utilizzo di subnet distinte garantisce che ove non sia presente un apparato dotato delle funzioni di routing non possano esistere comunicazioni tra elementi appartenenti a layer distinti e dotati di spazi di indirizzamento/subnet distinti.

Quanto sopra va inoltre declinato a cura del progettista costruttivo con le “best practice” specifiche descritte nel documento “*Guide To Industrial Control Systems (ICS)*”

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 19
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

Security”¹ e nel documento “Intrusion Detection and Prevention Systems in the Industrial Automation and Control Systems Environment”².

E' opportuno che tutti gli applicativi che siano coinvolti nelle comunicazioni con “elementi extranet” siano sottoposti a stringenti specifiche di programmazione e test che siano in grado di rilevare “bug” utilizzabili per realizzare attacchi che sfruttano la tecnica del “buffer overflow”, quindi particolare attenzione deve essere riservata alle operazione di “casting” di tutto il contenuto ricevuto mediante comunicazioni verso nodi esterni.

Inoltre tutti gli elementi di elaborazione presenti all'interno dell'opera devono avere una policy di utilizzo delle porte di comunicazione e dei dispositivi di memorizzazione coerente con i livelli sicurezza utilizzati e, quindi, deve essere garantito che essi/e sono disponibili solo a soggetti dotati del massimo livello di sicurezza.

Il sistema IDS deve essere impostato per rilevare e segnalare qualsiasi comunicazione avvenga verso nodi non appartenenti alla lista degli esterni autorizzati.

Il sistema IDS deve inoltre essere configurato per rilevare comunicazioni “anomale/impreviste” tra sistemi afferenti al backbone di bocca.

Secondo quanto messo in luce dal caso “*Stuxnet*”³ quanto sopra ha la finalità di:

- “limitare le opportunità”/“impedire l'ingresso” di codice che possa realizzare violazioni della sicurezza
- rilevare sintomi che consentano di rilevare il prima possibile la presenza di codice che possa realizzare violazioni della sicurezza



E' opportuno ricordare che il controllo dell'impianto, almeno per quanto riguarda la dinamica pneumatica che lo caratterizza, non necessita di tempi di ciclo che siano inferiori ai 100ms sono pertanto utilizzabili gli standard di comunicazione basati anche sul protocollo ethernet (IEEE 802.3) supportati dalla organizzazione ODVA (*Open DeviceNet Vendors Association*)⁴

¹ <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>

² http://ics-cert.us-cert.gov/sites/default/files/pcsf-arc/intrusion_detection_prevention_systems-martin.pdf



³ <http://en.wikipedia.org/wiki/Stuxnet>

⁴ <http://www.odva.org/>

		Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 20
		Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

Per quanto riguarda l'alterazione delle comunicazioni derivanti da errori randomici su protocollo IEEE 802.3 è utile ricordare che:

- il mezzo trasmissivo in funzione del rapporto segnale/rumore e della codifica di segnale (livello 1 della pila ISO/OSI) determina un BER (Bit Error Rate) che nel caso di adozione (IEEE 802.3) implica per connessioni fino a 1000BaseT un BER non superiore a 1E-10.
- la specifica IEEE802.3 prevede un meccanismo di CRC che consente al livello superiore di individuare eventuali bit errati
- la specifica TCP/IP (livelli 3-4 della pila ISO/OSI) in modalità “connection oriented” (TCP) consente la ritrasmissione di informazioni che siano state corrotte durante la trasmissione e la certezza della consegna del messaggio.

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 21
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

5.9. Sotto-Impianti

Fermo restando i criteri esposti nel documento MV100P-PE-GIS-0137-04F "Sistema di controllo - Specifica Tecnica" a cui si rimanda, vengono qui di seguito indicati alcuni criteri generali e specifici dei sotto impianti.

Gli apparati destinati all'interfacciamento verso i device di campo (RIO) sono fisicamente dislocati in armadi posizionati in prossimità dei device, parimenti i controllori ridondati sono posizionati in locali in prossimità del sotto sistema da gestire.

Gli armadi per la connessione dei segnali di campo sono stati dislocati rispettando i criteri di segregazione rispettando quindi l'impostazione impiantistica di avere sale tra loro fisicamente isolate, nelle quali sono contenuti armadi relativi ad apparati ridondati in campo.



Il PCS mediante una pluralità di PLC realizza l'automazione direttamente necessaria alla movimentazione pneumatica delle paratoie di una bocca e pertanto gestisce direttamente tutti i sotto impianti catalogati come principali e provvede ad interfacciarsi ai sottoimpianti di tipo package o standard.

Per la movimentazione pneumatica delle paratoie sono stati dedicati due controllori ridondati per ogni cassone, ossia per tre/due paratoie in funzione della tipologia di cassone (i cassoni da due paratoie sono il numero 1 della barriera di San Nicolò ed i numeri 1 e 7 della barriera di Malamocco), ed un controllore ridondato per il coordinamento dei controllori di cassone.

I segnali appartenenti ad ognuna delle 4 linee di processo (ingresso / uscita aria all'interno dei cassoni di soglia) relative ad una paratoia sono mantenuti tra loro segregati e si attestano a gruppi di schede di I/O dedicate (ovverosia schede dedicate per ogni funzione e per ogni linea di processo di ogni cerniera).

Sono inoltre gestiti da PLC dedicati ed indipendenti, tra cui:

- Distribuzione Elettrica (PMS)
- Compressori

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 22
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

- Sistema di Raffreddamento dei compressori
- Generatori di emergenza ed il relativo combustibile
- Sistema Antincendio.

Si dettagliano di seguito i principali impianti e le modalità di integrazione

5.9.1. Criterio Generale di Integrazione

L'integrazione dell'automazione dei vari sotto impianti qualora questi siano realizzati da soggetti diversi dal fornitore del sistema PCS è a cura del medesimo e deve garantire che tutte informazioni/funzioni disponibili sul sotto impianto siano correttamente mappate e disponibili nell'ambito del sistema PCS.



5.9.2. Distribuzione Elettrica (PMS)

Il sotto sistema della distribuzione elettrica è trasversale a tutti gli altri sotto sistemi e prevede una supervisione autonoma comprensiva di specifici client HMI sia a livello di sala consolle per la gestione dei quadri elettrici a 20kV, 6kV e 400V di Bocca sia a livello di sala consolle della Stazione Centralizzata per la gestione delle diverse sorgenti a 20kV che possono alimentare ciascuna bocca.

Tutti i sistemi di controllo che abbiano bisogno di informazioni relative alla “presenza rete” ossia della presenza della distribuzione elettrica sui device controllati possono interrogare il sottosistema destinato alla distribuzione elettrica comunicando con quest'ultimo per mezzo del protocollo MODBUS TCP ed, ove funzionale e consentito dalla presenza di opportuni “contatti puliti” sui quadri di distribuzione elettrica, è tenuto ad accedere direttamente a tali quadri di distribuzione ed a determinare autonomamente la “presenza di rete” sui dispositivi di I/O di sua pertinenza.

5.9.3. Compressori

Per ogni compressore è previsto (in aggiunta al collegamento seriale ridondato MODBUS TCP) un collegamento cablato per i segnali/comandi più importanti tra il quadro di comando di macchina (che gestisce il compressore e ne garantisce la sicurezza) ed il sistema di controllo.

		Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 23
		Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

5.9.4. Generatori di emergenza



Per ogni generatore è previsto (in aggiunta al collegamento seriale ridondato MODBUS RS485) un collegamento cablato per i segnali/comandi più importanti tra il quadro di comando di macchina (che gestisce il generatore e ne garantisce la sicurezza) e il sistema di controllo.

Per quanto riguarda sistemi non critici per il funzionamento delle paratoie, per i quali è possibile intervenire localmente in caso di guasti al sistema di controllo, si è previsto (ove ritenuto funzionale) l'impiego di moduli di I/O ridondanti per le funzioni di comando che non prevedono la ridondanza degli elementi in campo.

5.9.5. Videosorveglianza Interfonia

Il sotto impianto di Videosorveglianza e di Interfonia non oggetto della presente WBE dovrà rispettare quanto previsto al capitolo 5.2 e potrà essere interfacciato al sistema PCS/SCADA sia quale generatore di eventi che possano determinare interferenza con le attività del gestore delle operazioni comandate (intrusioni/presenza in aree a rischio) e sia per consentire al medesimo:

- di ispezionare visivamente aree/apparti che compongono gli impianti
- di comunicare con altri operatori dislocati fuori della sala consolle

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 24
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

5.10. Sale di Controllo

Per ogni bocca è prevista una sala server bocca nell'Edificio di Automazione e Controllo ove in appositi rack sono presenti i server ridonati (e segregati) necessari alla gestione della Bocca (Scada PCS e Scada PMS, Historian, Allarmi) e gli apparati di comunicazione switch/router di backbone. Inoltre in appositi quadri di automazione sono contenuti i PLC di coordinamento dei sottosistemi che abbiano una pluralità di PLC (PCS, ESD, PMS).

Per ogni bocca è prevista una sala consolle/controllo di bocca ove sono presenti i client HMI con superfici di visualizzazione per ciascun posto operatore adeguati alla visualizzazione delle informazioni di supervisione del sistema PCS e del sistema PMS di bocca.

In particolare alle bocche di porto, nell'Edificio di Automazione e Controllo, è prevista una sala/consolle di monitoraggio dedicata ai seguenti sistemi:



- monitoraggio strutturale dei cassoni
- monitoraggio strutturale del componente femmina dei connettori
- monitoraggio dei giunti GINA
- ecc.

Questa sala/consolle, per la barriera di Treporti, è localizzata nell'Edificio di Spalla Ovest e sarà usata come sala di controllo nella fase di pre-collaudato dell'impianto.

La sala server della Bocca di Lido funge anche da sala server di opera e contiene i server necessari alla gestione di opera (PMS di opera, consolidamento dati Historian).

La sala consolle della Bocca di Lido funge anche da sala consolle/controllo di opera (Stazione Centralizzata) per la supervisione e controllo dell'intera opera e quindi di tutte le bocche.

Un'ulteriore sala consolle, detta Stazione Centralizzata Remotizzata situata presso l'Arsenale di Venezia, consente la supervisione degli impianti di tutte le bocche.

 	Rev. C1	Data 13/01/14	MV100P-PE-GIS-5001-04F	Pag. 25
	Rev. C0	Data 30/08/13	COMUNICAZIONE ED INTERFACCIAMENTO SPECIFICA TECNICA	

In futuro la sala dell'Arsenale potrà assumere l'operatività delle tre bocche e non solo funzioni di supervisione.

La sala consolle della stazione centralizzata (remotizzata) prevede la presenza di client HMI in grado di raggiungere mediante la rete di comunicazione i server di supervisione presenti in ciascuna bocca e quelli di opera.

Per ogni sotto sistema un solo client HMI può essere abilitato al comando mentre tutti i client HMI possono essere abilitati al display delle informazioni in funzione delle credenziali possedute dall'operatore (e dalla postazione).

Ogni sala consolle prevede pc, tastiere, mouse, stampanti, video-wall, ecc. necessari alla corretta esecuzione delle operazioni e visualizzazione degli stati del sistema.

Si rimanda alla Relazione MV100P-PE-GIR-0006-04F sull'Architettura, alla Specifica Tecnica MV100P-PE-GIS-0137-04F del presente progetto esecutivo ed alle planimetrie delle sale di controllo proposte per i relativi dettagli (MV100P-PE-L/M/CID6521- 04F), fermo restando l'effettiva realizzazione delle opere civili in sito alla quale necessariamente si rimanda.

I client HMI sono realizzati mediante un sistema multiscreen con elementi da 22" con risoluzione full HD in configurazione 2x1 (circa 4000x1000 pixel) nelle bocche di Chioggia e Malamocco e in configurazione 3x1 (circa 6000x1000 pixel) nella bocca di Lido.

I client HMI della Stazione Centralizzata sono in configurazione 3x2 (circa 6000x2000 pixel).

Anche se non indicate nell'architettura, ogni sistema di controllo è dotato di stazione di ingegneria posizionata presso la sala consolle di bocca (rif. "Disposizioni consolle operatore in sala controllo" MV100P-PE-L/M/CID6521-04F).