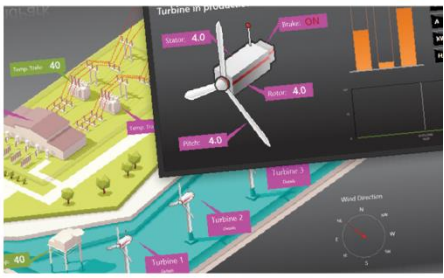
INDUSTRIAL AUTOMATION SOFTWARE
progea

Movicon.next™
Automation Platform.next generation



Movicon NExT

7.0 Ricette

Ver.3.4.268

Sommario

1. Ridondanza (Fault Tolerance)

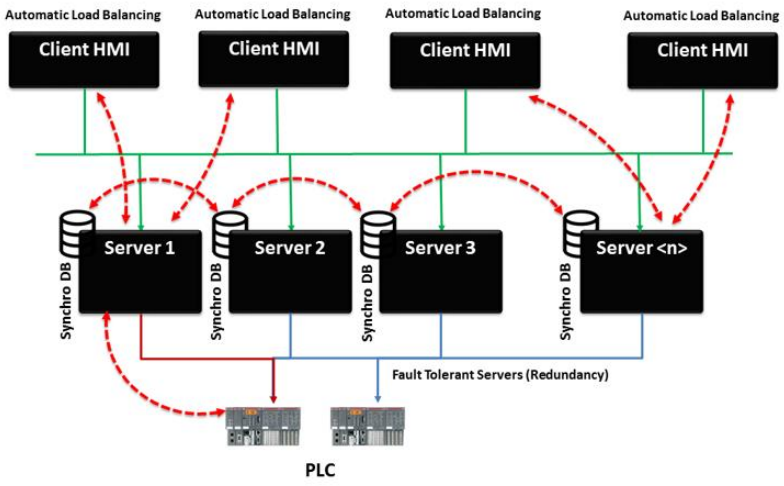
I sistemi di controllo che gestiscono processi di automazione critici, devono avere la possibilità di gestire il massimo criterio di affidabilità e continuità di servizio, in grado di continuare a gestire il processo anche in caso di errore o guasto del sistema di gestione. Per continuità di servizio si intende la piena funzionalità del sistema di gestione e la totale integrità dei dati di processo registrati.

Per garantire la continuità di servizio, è necessario prevedere un sistema di gestione "ridondato" (fault tolerant), composto da due o più sistemi server e due o più sistemi client, in grado di sincronizzarsi tra loro in modo totalmente automatico.

Platform.NExT integra potenti funzioni automatiche per supportare la gestione della ridondanza per stazioni "mission critical" di server e client collegati in rete. Questa funzionalità prevede, in modo completamente automatico e trasparente, la sincronizzazione dei dati tra più stazioni server collegate in rete, sia per la parte di comunicazione che per la parte di gestione storici, in modo tale da disporre sempre di un server attivo in modo "primario" e più server attivi in modo "secondario".

Allo stesso modo, le stazioni Client saranno sempre collegate ad uno dei server attivi, garantendo sempre in modo automatico lo "switch" sulla stazione server opportuna per la garanzia di continuità di funzionamento.

Le funzioni di ridondanza saranno abilitate in runtime solo se sono attive le opzioni Ridondanza e Networking su ogni licenza di ciascuna stazione PC che partecipa al sistema.



Esempio di architettura ridondante per la stazione di supervisione. Possono essere presenti n Server, di cui solo uno sarà quello attivo, ed n Client connessi ai diversi Server.

Livelli di Ridondanza

Il principio di ridondanza nei sistemi di automazione prevede la presa in consegna delle funzionalità del componente in avaria da parte di un componente identico fino al momento inattivo, che entra in funzione e sostituisce automaticamente il componente principale.
Le funzioni di "Ridondanza Calda" o "Hot Backup" prevedono l'entrata in funzione automatica dell'unità secondaria, senza richiedere alcun intervento manuale dell'operatore.
Il concetto di ridondanza può essere applicato sia all'hardware che al software, per determinare la minima perdita di dati o di funzionalità del sistema, durante il trasferimento del controllo dall'unità Primaria a quella secondaria di backup.
Nei sistemi di automazione, il concetto di ridondanza può essere applicato ai seguenti **componenti:**

Campo	**Connessione**	**Supervisione**
PLC, Servo, I/O	Seriale, Fieldbus, Rete Ethernet	Server Scada, HMI (Platform.NExT)

Le funzioni di Ridondanza integrate in Platform.NExT supportano la funzionalità di Fault Tolerance sulle stazioni PC sia lato server che lato client, permettendo il trasferimento delle funzioni di comunicazione, visualizzazione e controllo dalle stazioni attive a quelle non attive in modo completamente automatico, con sincronizzazione automatica dei dati storici.
La particolare tecnologia proprietaria di Movicon permette tempi di sincronizzazione brevissimi, pur in presenza di grandi quantità di dati da sincronizzare. Ciò è dovuto alla sincronizzazione dei dati acquisiti nel periodo di funzionamento in emergenza, trasmettendo dati in formato binario anziché strutture di dati in formato database.

2. Funzionalità della Ridondanza (Fault Tolerant)

La gestione della ridondanza, sia con funzionalità Server che con funzionalità Client, è completamente integrata nella piattaforma Platform.NExT, e garantisce l'intervento automatico di uno dei Server Secondari (non attivi) in modo completamente trasparente per l'utente, in caso di Fault del Server Primario (attivo), rilevabile dopo un tempo di timeout (impostabile).
La piattaforma supporta inoltre la possibilità di definire un "array" di server, in modo da aumentare la garanzia di continuità di funzionamento dell'impianto, anche in caso di ulteriori fault sul server attivo.

Funzionamento

Il principio di funzionamento della Ridondanza di Platform.NExT prevede la definizione di due o più moduli Server connessi ai dispositivi in campo. I Server devono essere collegati tra loro su una rete ethernet, e ciascuno deve essere dotato di apposita configurazione di progetto che prevede la lista dei Server collegati tra loro ed il tempo di timeout per l'intervento.
Ogni server deve essere dotato di una apposita licenza runtime con abilitata la funzione opzionale di ridondanza.

Esercizio Normale

Durante il normale esercizio, il Server primario è collegato ai dispositivi in campo e provvede alla gestione dei dati ed alla registrazione. Gli altri Server secondari sono operativi, dispongono dei dati realtime e registrano esattamente le informazioni perfettamente sincronizzate con il Server primario. Non comunicano direttamente con il campo, anche se sono predisposti a farlo.

Esercizio in condizione di emergenza

In caso di "fault" del Server primario, il Server secondario successivo (in una eventuale lista di server di backup) provvede a comunicare direttamente con i dispositivi in campo, ed a registrare direttamente i dati. Provvede automaticamente a notificare agli eventuali successivi Server secondari che è diventato Server Primario. Tutti gli altri eventuali successivi Server secondari si adeguando di conseguenza.
Nel caso in cui anche il nuovo "Server primario" andasse in fault, il successivo Server Secondario nella lista assumerebbe il ruolo di Server primario, come indicato sopra.

Ripristino Esercizio Normale

Quando un Server primario torna in funzione e viene ripristinato, esegue in modo automatico la sincronizzazione dai dati, sia ripristinando localmente la situazione degli storici, sia acquisendo tutte le informazioni attive. A sincronizzazione avvenuta, il Server primario ripristinato ricomincia a comunicare con i dispositivi in campo, recuperando la sua funzione primaria. Di conseguenza a ciò, il Server che era attivo in quel momento ritorna nella sua condizione "secondaria", operativo ma in conseguenza ai dati forniti dal suo Server primario.

Connessioni Client

Le stazioni Client di visualizzazione dati, connesse ai Server del sistema, sono sempre automaticamente collegate ad uno dei servers attivi, secondo un principio di

bilanciamento ottimale del carico (load balancing). Pertanto, se una stazione Client è connessa ad un Server e questo dovesse andare fuori servizio, il Client automaticamente cercherà la stazione Server successiva, garantendo sempre la continuità di servizio in modo automatico.

Sulla base dei principi di funzionamento sopra indicati, grazie alla funzionalità automatica di ridondanza, il sistema di supervisione Platform.NExT è in grado di garantire una continuità di servizio eccellente, rendendolo particolarmente idoneo ad applicazioni "mission critical" dove il funzionamento deve essere garantito sempre, in qualunque situazione.

Definizioni e Concetti

- Server Attivo: è la stazione che in condizioni di funzionamento normale provvede a gestire l'impianto, comunicare con esso, acquisire i dati e provvedere al controllo. L'eventuale anomalia di questa stazione determina l'entrata in funzione di una delle stazioni non attive
- Server Non Attivi: sono le stazioni (una o più di una) che in condizioni di funzionamento normale permettono la gestione dell'impianto in modo ridondato, ovvero attraverso la condivisione delle aree di memoria delle variabili. Le stazioni possono consentire di agire sull'impianto in maniera indipendente e dispongono della situazione archivi assolutamente identici a quelli della stazione attiva. In presenza di anomalia dell'unità Attiva, una delle stazioni non attive diventerà Attiva e provvederà a gestire automaticamente l'impianto avviando le funzioni di comunicazione dei driver ed i motori di registrazione, acquisendo i dati e provvedendo al controllo
- I Driver dei Server Non Attivi sono posti in Stand-by e non comunicano direttamente. L'operatività di tali server è gestita mediante la notifica del valore delle variabili da parte del Server Attivo verso gli altri Server e vice-versa. Il tutto avviene in modo automatico e trasparente. Ne consegue che un comando verso il campo può essere impartito indifferentemente da uno qualsiasi dei Server, mentre un operazione di cambio pagina è da considerarsi locale, in quanto ogni unità elabora localmente le proprie funzionalità grafiche
- Gli storici dei Server Non Attivi (Historian, Data Logger, Ricette e Log Storico) non operano direttamente, per garantire l'assoluta identicità dei dati registrati. Le apposite funzioni di ridondanza del sistema provvedono a far si che i dati acquisiti e registrati dal Server Attivo siano archiviati in modo identico e trasparente anche sugli altri Server. Il meccanismo di sincronizzazione garantisce sempre l'integrità dei dati e la loro precisione temporale
- Lo stato degli allarmi del Server Attivo viene ridondato su tutti gli altri Server. Eventuali comandi di Riconoscimento e Reset eseguiti su un Server qualsiasi verranno trasmessi al Server Attivo che ne eseguirà la funzione.
- La lista Eventi e gli Eventi su Variabile degli script non verranno eseguiti sui Server non attivi

Funzioni Supportate

Le funzioni di Fault Tolerance integrate in Platform.NExT prevedono la gestione ridondata dei seguenti moduli funzionali

- Gestione Driver di Comunicazione
- Gestione Historian e Data Logger
- Gestione Log Storico
- Gestione Allarmi

Funzioni Non Supportate

Al momento non sono supportate le Ricette (in preparazione).
Di seguito le ulteriori funzionalità non gestite, dove per "non gestite" si intende che la funzionalità sotto indicata viene eseguita autonomamente e singolarmente dal relativo server, senza sincronizzazione automatica.

- Oggetti Evento
- Alarm Dispatcher
- Schedulatori

Logiche e Variabili

E' disponibile una variabile di sistema sul Server che permette di gestire, ad esempio per eventuali logiche locali, l'informazione se il Server di Ridondanza è "attivo" o "non attivo".

Lista dei Server

Sebbene la funzione di ridondanza di Platform.NExT possa supportare fino a 64 server, Progea al momento **ne garantisce la funzionalità fino a 4.**

Tramite l'impostazione "Redundancy Server" si dovrà inserire il nome dei server (Host Name della macchina) che verranno utilizzati dal progetto. L'ordine in cui i server vengono inseriti nella lista è molto importante perché definisce la priorità con la quale verrà identificato quale sarà il Server Attivo.
Durante il funzionamento in condizioni di esercizio "normali", tutti i Server della lista sono avviati e operativi sull'impianto secondo funzionalità distinte.
Il Server Attivo sarà il primo della Lista definita e sarà quindi quello destinato a gestire la comunicazione dei driver ed a gestire la storicizzazione dei dati su Data Base, secondo appunto il normale funzionamento di ogni progetto. Gli altri Server della lista sono disponibili e operativi per svolgere in modo indipendente le stesse funzionalità del Server Attivo, secondo quanto definito.

Sincronizzazione Orario

E' importante tenere conto della sincronizzazione dell'orario di sistema dei Server ridondati, per una maggiore congruità dei dati storici sincronizzati. Ogni PC viene automaticamente sincronizzato con l'orario di un server centrale di Microsoft Windows, secondo la funzionalità automatica del sistema operativo.
E' possibile comunque sincronizzare l'orario di ogni Server con un Time Server diverso da quello di default di Windows, eseguendo le opportune impostazioni nei comandi "Orario Internet" del menu Impostazioni del Sistema operativo.

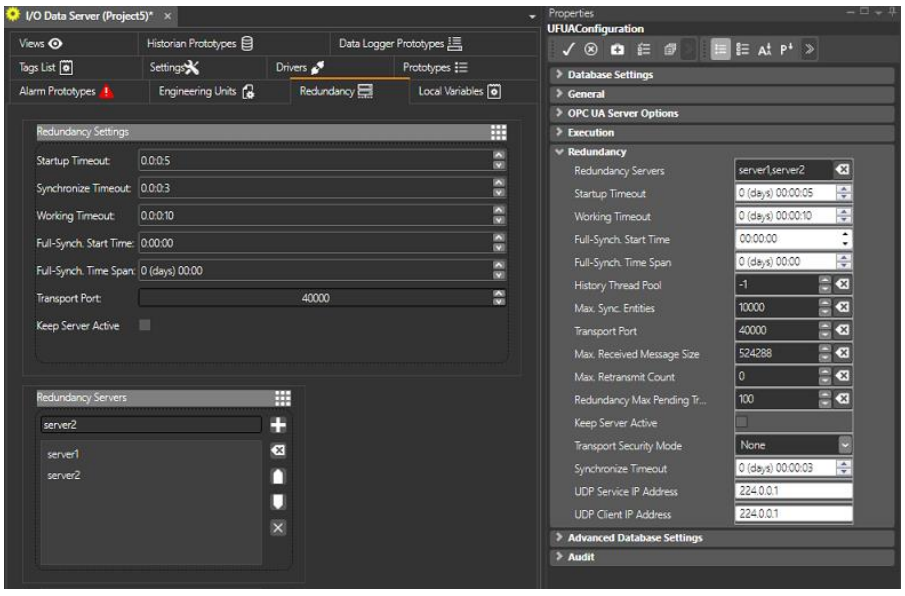
3. Ridondanza Server

Le Impostazioni di Ridondanza si possono configurare tramite la risorsa "Ridondanza" disponibile nel gruppo di impostazioni dell'"I/O Data Server". Alcuni dei parametri di impostazioni avanzate della Ridondanza sono invece disponibili solo nella Finestra delle Proprietà nell'apposito gruppo "Ridondanza".
Per maggiori info. vedi anche il capitolo dedicato alle "Impostazioni Avanzate del Server" .

La funzionalità di Ridondanza del Server si basa sul protocollo UDP Multicast per il quale è necessario impostare l'indirizzo IP del Gateway sulla scheda di rete.
Nel caso in cui il progetto venga eseguito su PC privi di accesso ad internet (dove quindi l'uso del Gateway sarebbe superfluo), è comunque necessario impostare l'indirizzo IP del Gateway sulla scheda di rete utilizzando un qualunque indirizzo IP della stessa "sottorete".

La funzionalità di Ridondanza del Server è supportata solo per i PC che fanno parte della stessa sottorete (ovvero con indirizzi IP della stessa subnet mask).
Non è quindi consentito utilizzare tale funzionalità se i PC sono collegati tra loro tramite un router.

I parametri disponibili sono:



Ridondanza

lista Server di Ridondanza

In questa casella va inserita la lista dei server che parteciperanno alla ridondanza.
Andranno quindi inseriti gli Host Name delle Macchine interessate.
Attenzione: è necessario inserire l'Host Name delle macchine e non il loro indirizzo IP.
Una macchina infatti potrebbe anche avere più indirizzi IP. Per il gestore di Ridondanza quello che fa riferimento è quindi il nome della macchina.

L'ordine di inserimento determina anche la priorità con cui verrà stabilito chi sarà il Server Attivo del sistema.

Partendo dall'inizio della lista il primo dei server avviato e disponibile sarà anche quello Attivo, e avrà il controllo completo del sistema.

Attenzione! Nella lista Server va inserito l'hostname e non l'indirizzo IP.
Nel caso in cui il progetto venga eseguito su PC di una rete dove non è disponibile un DNS Server,
è necessario impostare nel file "Host" di Windows ("C:\Windows\System32\drivers\etc") gli Alias "<Indirizzo_IP> <Nome_PC>" per risolvere i nomi di ogni PC coinvolto nella ridondanza.

Timeout di avvio Ridondanza

Tempo massimo che viene atteso per la ricerca degli altri server sulla rete usando il protocollo udp.
Quando la ridondanza parte fa una ricerca sulla rete degli endpoint che soddisfano i requisiti di ridondanza e il cui hostname fa parte della lista configurata nel progetto in avvio.

Timeout Sincronizzazione Ridondanza

Tempo massimo che viene atteso per i messaggi che un server non attivo scambia con il server attivo per mantenersi sincronizzato.
Questi messaggi viaggiano sul canale tcp e includono la richiesta iniziale del valore dei tag e degli allarmi, così come la lista degli storici da tenere sincronizzati.
Inoltre lo stesso tempo viene usato come intervallo di ping che fa il server non attivo per vedere se il server attivo è ancora vivo.

Timeout Ridondanza

Timeout utilizzato per i messaggi che il server attivo invia agli altri server tramite il canale udp (ad esempio quando cambia un tag o un allarme).
Questo tempo viene utilizzato anche all'avvio della ridondanza come tempo massimo di attesa fra lo start e la notifica che la ridondanza è partita. Se non si inizializza tutto entro questo tempo viene visualizzato un errore.

Ora di Sincronizzazione Completa

Orario di avvio della sincronizzazione completa del database. Durante le fasi di avvio e di arresto dei diversi server si potrebbero creare dei disallineamenti dei dati tra i vari server. La sincronizzazione completa consente di riallineare i database a fronte di queste eventualità. Se il parametro "Full Syncronization Time Span" è diverso da zero allora questa proprietà verrà ignorata e usata solo la "Full Syncronization Time Span".

Intervallo Temporale Sincronizzazione Completo

Questa impostazione consente di definire ogni quanto tempo la sincronizzazione completa del database dovrà essere eseguita.

Num.Max. Thread Storici

Numero di Thread che verranno utilizzati per la gestione della sincronizzazione degli storici. Il valore "-1" significa che verranno creati tanti thread quante sono le CPU o i CPU Core. Aumentando il numero di thread si aumenteranno le prestazioni di sincronizzazione dei dati storici a scapito però delle altre funzionalità, come comunicazione, animazioni, ecc..

Num. Max. Item in Sicronizzazione

Questo parametro riguarda la sincronizzazione degli storici e corrisponde al numero massimo di record che vengono letti dal server attivo per ogni job di sincronizzazione che fanno gli altri server.

Numero Porta Ridondanza

Porta utilizzata per le funzioni di ridondanza dal trasporto.

Dimensione Massima Pacchetti Ricevuti

Dimensione massima del pacchetto che può essere scambiato per la sincronizzazione dei tag.

Numero Massimo Tentativi di Invio

Numero di ritrasmissioni dei pacchetti udp inviati dal server attivo per mandare gli aggiornamenti dei tag e allarmi agli altri server.
L'udp non è un protocollo che controlla se il pacchetto è arrivato a destinazione ed eventualmente lo rispedisce. Questo parametro consente di inviare più volte lo stesso pacchetto per diminuire la probabilità che un pacchetto non venga ricevuto da uno dei destinatari; di contro mettendo il parametro ad un valore diverso da zero, le performances di ridondanza nell'invio delle informazioni decadono.

Max Pending Message

Numero massimo di messaggi pendenti. Se la quantità di messaggi da inviare ai Server Non Attivi supera questo limite, allora quelli in eccedenza verranno persi. Viene usato solo per l'aggiornamento realtime dei tag. Riguarda il numero massimo di cambiamenti gestiti per singola variabile. Se per un tag sono da inviare un numero di cambiamenti superiore a quello impostato in questo parametro, allora vengono rimossi i cambiamenti più vecchi e lasciati gli "enne" più recenti.

Mantieni Attivo il Server Attivo

Questa opzione ha effetto **solo se ci sono due server in lista** e serve a mantenere attivo, in fase di rientro di un server dopo un fault, quello che ha il controllo.

- Se l'opzione è abilitata e ci sono soltanto due Server in lista, allora la priorità della lista non verrà più considerata ma resterà sempre attivo, dopo il rientro di un server, quello attivo al momento. Se ad esempio il primo Server della lista che ha il controllo viene arrestato (fault) si attiverà il secondo server della lista. Quando però il primo Server torna attivo, non dovrà riprendere il controllo ma lasciare il controllo al secondo, fino a che questo non verrà arrestato a sua volta.

- Se l'opzione è disabilitata, oppure in lista ci sono tre o più server, questa opzione non verrà considerata e si avrà il funzionamento in base alla priorità

della lista dei server. Quando un Server torna attivo, se ha una posizione più alta nella lista dovrà riprendere il controllo.

Nel caso in cui l'opzione "Mantieni Attivo il Server Attivo" è stata abilitata e dono stati definiti solo due Server nella lista, allora sarà possibile anche eseguire uno switch del server attivo tramite il comando "RedundancySwitchActiveServer".

Modalità Sicurezza Ridondanza

Livello di sicurezza da utilizzare per il trasporto. Le possibili selezioni sono:

- None
- Transport
- Message
- TransportWithMessageCredential

Indirizzo IP Servizio UDP

Area "in ascolto" per i pacchetti UDP. Il valore 224.0.0.1 indica il gruppo formato da tutti gli Host della rete LAN.

Indirizzo IP Client UDP

Definisce l'area per l'invio dei pacchetti UDP. Il valore 224.0.0.1 indica il gruppo formato da tutti gli Host della rete LAN.

4. Ridondanza Client

Il modulo Client di Movicon.NExT, sia come visualizzazione locale al Server oppure remoto, può connettersi sempre ed automaticamente ad uno qualsiasi dei Server avviati del sistema di ridondanza. Questa funzionalità è intrinseca ad ogni Client di Platform.NExT, e non richiede abilitazioni o opzioni sulla licenza.

Il Progetto, anche se eseguito solo come Client, prevede la definizione della Lista Server come già descritto.

All'avvio, il Client verificherà la disponibilità di una connessione all'eventuale Server Locale della macchina, se presente, utilizzando il trasporto "net.pipe" se questo è stato abilitato nel progetto. Se non fosse disponibile un Server Locale, il Client verificherà la connessione ad uno dei Server Remoti, utilizzando il trasporto di rete configurato nel progetto (ad esempio il "net.tcp").

La scelta del Server al quale connettersi avviene in base al carico di lavoro (Load Balancing) che viene rilevato al momento della connessione al Server.

Come prima cosa il Client tenterà di connettersi al Server locale alla macchina, se questo è presente, e verrà utilizzato il tasporto "net.pipe" se è stato abilitato nel progetto. Nel momento il cui il Server non sia disponibile localmente allora il Client tenterà di connettersi ad un server remoto, utilizzando un trasporto di rete, ad esempio "net.tcp" che dovrà essere abilitato nel progetto, e la scelta del Server avverrà in base al carico di lavoro che viene rilevato al momento della connessione.

Ogni Client quindi, quando si deve connettere ad un Server, verifica la situazione "ottimale" del carico dei server, e si connette a quello con la situazione migliore, garantendo così una efficace distribuzione del carico di lavoro di ciascun server, soprattutto in presenza di molti Client, contribuendo a migliorare le performances complessive del sistema.
Dopo che il Client si è connesso ad un Server, ne mantiene attiva la connessione fino a che il Server non sarà più disponibile. In questo caso, qualora il Server connesso non sia più disponibile (ad esempio in caso di Fault), il Client automaticamente cercherà di attivare la connessione su uno degli altri Server ridondati disponibili in rete.

La tecnologia di Connessione Automatica e di Load Balancing disponibile in Platform.NExT garantisce una completa continuità di servizio delle stazioni Client, in modo completamente automatico e trasparente per l'utente, al tempo stesso garantendo l'impostazione ottimale del traffico dei dati, contribuendo all'efficacia del sistema ed alle sue performances.

INDUSTRIAL AUTOMATION SOFTWARE

progea

Progea Srl
Via D'Annunzio, 295
I-41123 Modena
info@progea.com
Tel +39 059 451060

Progea International SA
via Sottobisio, 28
6828 Balerna (CH)
international@progea.com
Tel +41 91 96 76 610

Progea Deutschland GmbH
Marie-Curie Str., 12
D-78048 VS Villingen
info@progea.de
Tel +49 (0)7721 99838 0

Progea North America Corp.
2380 State Road 44, Suite C
Oshkosh, WI 54904
info@progea.us
Tel. +1 (888) 305-2999