

# Development of Remotely Monitoring and Control System for Siemens 840D sl NC Machine Tool Using Snap 7 Codes

Bo Zheng<sup>1</sup>, Junjie Xu<sup>2,3</sup>, Helin Li<sup>2,3</sup>, Junwei Xing<sup>2</sup>, Huadong Zhao<sup>1</sup> and Guoning Liu<sup>1,\*</sup>

<sup>1</sup>School of Mechanical Engineering, Zhengzhou University, P R China

<sup>2</sup>IIoT Institute, Zhengzhou University, P R China

<sup>3</sup>R&D Center, Zhengda Zhineng Company, P R China

\*Corresponding author

**Abstract**—Based on the understanding of the communication methods and the structure and architecture of databases/data blocks of numeric control (NC) system, an open source communication suite designed specifically for Siemens NC system, Snap 7, is used to realize data acquisition from Siemens 840D sl NC system of which the communication interfaces are industrial Ethernet. Furthermore, monitoring system for display and analyses of the production processing state is developed and its reliability is evaluated.

**Keywords-***monitoring; remote control; snap 7; 840D sl; NC system*

## I. INTRODUCTION

To meet the competitive priorities like low cost, good quality, short delivery times, high flexibility, and good service [1], modern manufacturing needs rich information on various factors/parameters related to production like those for product design, materials, and particularly production processing. Modern technologies like NC system and information and communication technology (ICT) make it possible to generate/store/transfer data (information) relevant to the situation and conditions during the manufacturing, e.g., the manufacturing parameters, the state of the machine tools and measurement probes and so on [1-4]. Data (information) can be further analyzed to optimize the manufacturing processes, provide basic information for manufacturing execution system (MES), and set the basis for product life management [1,5]. Clearly, realization of the real time monitoring and control system for manufacturing processes becomes very important today. Mainstream NC systems like those of Siemens and Fanuc are not open systems and data acquisition can be made through their own specifically defined interfaces among the system modulus or by the exchange between the machine data blocks (MDB) [6]. This situation not only limits the advanced system development based on current mainstream NC systems, but also hinders the interoperability since usually more than one NC systems may be used in manufacturing plants. Therefore, the methods for data acquisition other than those provided by the specific NC system itself are preferable for the development of distributed NC system (DNC) which nowadays constitutes the base for smart manufacturing. In this study, aiming at the realization of monitoring system, we choose a

widely adopted NC system in manufacturing industry, SINUMERIK 840D sl, to explore the methods to extract useful data like those concerning the state of manufacturing, the motor and so on.

## II. SINUMERIK 840D SL NC SYSTEM AND THE MODULUS

SINUMERIK 840D sl NC system is capable of high-performance milling and turning and opens up a nearly inexhaustible technology range: from grinding to modern manufacturing technology like the laser machining [6-7]. This system boasts of high flexibility in terms of new manufacturing technology fields. In addition, the SINUMERIK 840D sl also provides excellent modularity of the operator components and has such unique open system architecture that the CNC with this NC system can be optimally adjusted to the machine technology [7]. And the SINUMERIK 840D sl supports various communication protocols and is commutative at all levels. 840D sl mainly consists of human machine interface (HMI), PC unit (PCU), numeric control unit (NCU), drive and motors [7]. The communication architecture is shown as Figure 1.

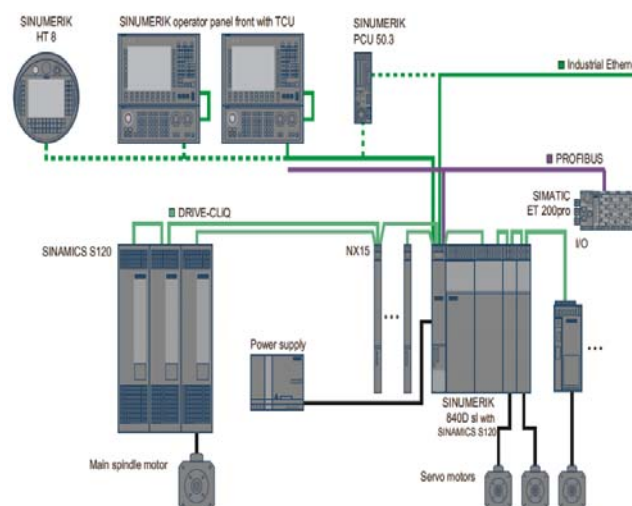


FIGURE I. COMMUNICATION ARCHITECTURE OF 840D SL

The deep green lines, light green lines and purple lines are for the industrial Ethernet communication, drive CLiQ communication and PROFIBUS communication, respectively. Its NCU module, which provides the most important

information on the manufacturing processes, provides with the Ethernet, USB and PROFIBUS DP communication interfaces as illustrated in Figure 2. The manufacturing capacity of the NCU can be further extended by adding NX modules.

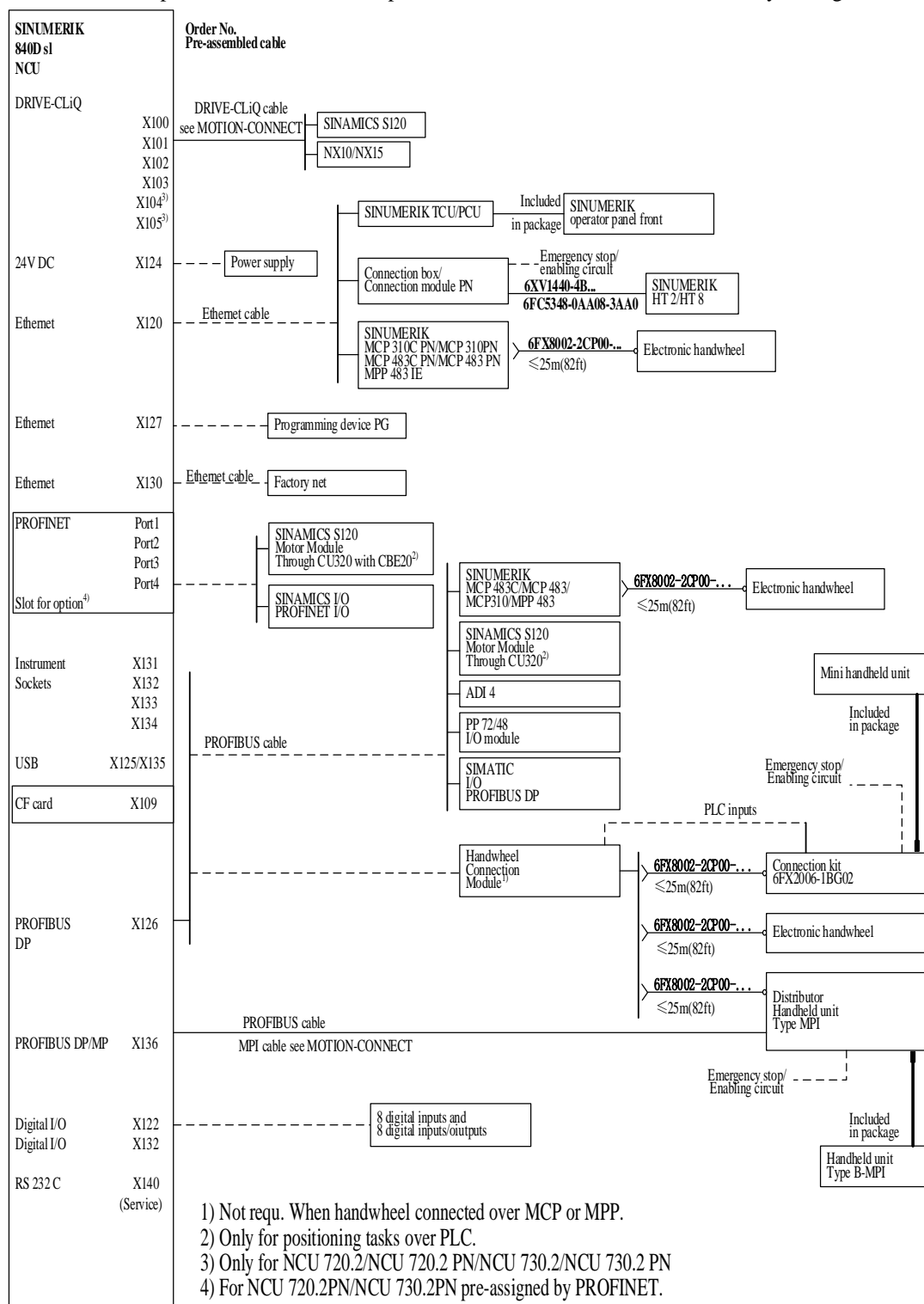


FIGURE II. INTERFACES OF NCU FOR 840D SL

The components of 840D sl are almost same as 840D (now renamed as 840D pl). For 840D pl NC system, the communication interfaces have operator panel interface (OPI), multi-point interface (MPI) and PROFIBUS [6,10]. And its communication architecture may be schematically presented as:

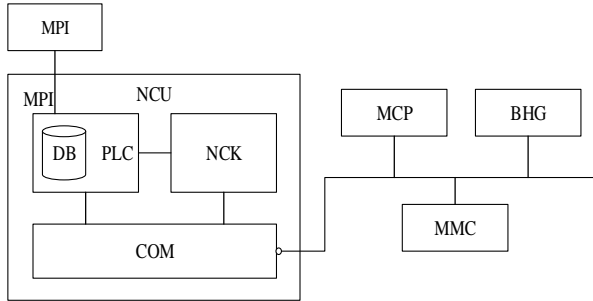


FIGURE III. COMMUNICATION ARCHITECTURE OF 840D SL NC SYSTEM

MCP and MMC in Figure 3 denote the units of machine control panel and man-machine control, respectively. NCK and PLC denote the numeric control kernel and programmable logic control, respectively. The baud rates of MPI and OPI interfaces are 1.5Mbps/s and 187.5Kbits/s, respectively. For 840D sl and 840D pl, besides COM module, the NCU also includes NCK and PLC modules where the data of the machine tool, NC program and processing data and so on are processed or stored. The architecture of NC system in our study is of the NCU+MCP+PCU+OP type, and may be schematically presented as Figure 4.

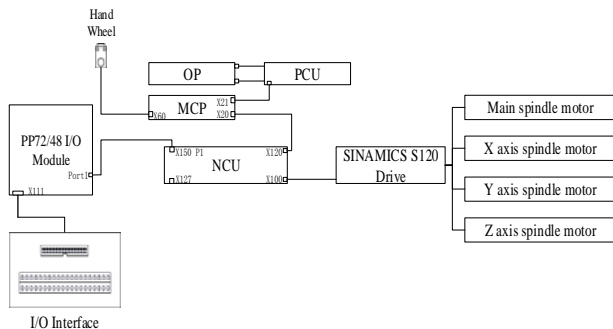


FIGURE IV. ARCHITECTURE OF 840D SL NC SYSTEM

OP is short for operator panel in Figure 4. As indicated in Figure 2, the communication interfaces of 840D sl enable much higher baud rates. Therefore, meaningful real time data acquisition, data analysis and control of machine groups can be realized.

### III. DATA AND DATA BLOCKS (DB) OF THE 840D SL NC SYSTEM

The functions of SINUMERIK 840D sl NC system are realized via the machine data (MD) and data communication. The data/programs can be used for drive control, axis/axes channel setting, machining process and the setting of auxiliary system [10].

#### A. Machine Data Type

Machine data can be categorized by their functions as:

- 1) *General machine data*: for the basic settings of NC system, the drive setting and memory setting et al;
- 2) *Channel data*: for the management of specific channels, for example, the allocation of the channel for axis/axes;
- 3) *Axis/Axes data*: for the settings of spindles, for example, the spindle position and the maximum speed and the manufacturing area;
- 4) *Tool data and magazine data*: for example, tool type, tool name, tool offset and tool characteristics et al;
- 5) *Drive data*: for the setting of motor, for example, the maximum electric current et al.

#### B. Machine Data Exchange/Communication

The NC system of 840D sl consists of NCK unit, PLC unit and COM interface unit. The variables are set in specific areas of NCK unit in the modular features. NC system specifies the areas, the data modules, the data types and data classes/struts. The data exchange between the PLC unit and NCK unit is through data blocks (DB) exchange via specific interfaces. Basic DBs have been set and defined by NC system. The DBs corresponding to the PLC unit are given in Figure 5. The interfaces include those of MMC, NC, COM, NC channels, tool/magazine management, spindles and so on. Interface protocols, which can not be modified or changed by users, should be followed in the processes of reading/writing data. The signals/data exchange in NCU unit is directional. For example, signals from NCK to PLC can be transferred after PLC unit makes requests in NC system and are only for reading. In response to PLC's requests, NCK unit performs relevant functions after "interpreting" the signals from PLC. The functions could be about the control methods, feed rate, coordination axis selection, et al. User DB is the interface between user's programs and basic program.

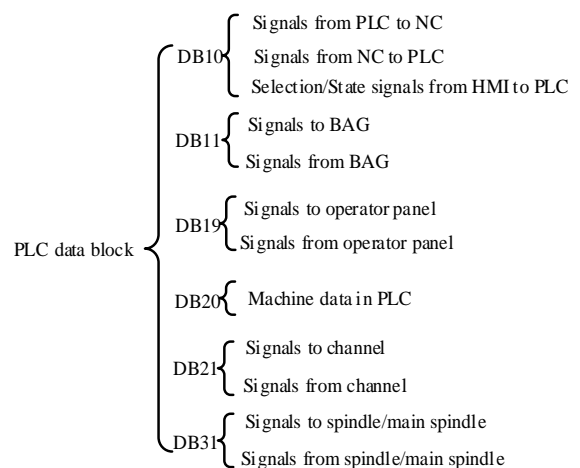


FIGURE V. TYPICAL DBS FOR PLC UNIT

Through variables data exchange can be made between other NC units shown in Figure 1, e.g., data exchange between PLC and MMC. The state data of NCK unit concerning the situations of manufacturing processes can be accessed by PLC unit. Accordingly, by acquisition data from PLC unit, the state data of machine tool can be temporally stored, accessed, extracted, loaded and transferred.

#### IV. METHODOLOGY FOR DATA ACQUISITION AND MONITORING SYSTEM DEVELOPMENT

##### A. Open Resource Snap 7

PLC of 840D sl NC system is S7-300. It supports MPI, PROFIBUS and industrial Ethernet (TCP/IP) communications. X127 connection of its NCU is for the industrial Ethernet communication. As mentioned previously, the systems specifically for one NC system, e.g., WINCC and OPC of Siemens NC system, have many shortcomings and limit the data/information exchange across different NC systems. And these systems routinely cost customers a lot for various authorization fees. Fortunately, many open resources provide with ways or functions to realize data acquisition from PLC unit without the help of the specific systems like WINCC or Siemens' DNC interfaces. And Snap 7 is a powerful tool today to manage this approach [8-9].

Snap7 is an open source, 32/64 bit, multi-platform Ethernet communication suite for interfacing natively with Siemens S7 PLCs, i.e., from S7-200 to S7-1500 [9]. And it is free. Snap 7 can be downloaded from the website [snap7.sourceforge.net](http://snap7.sourceforge.net). The documentation of Snap 7 is somewhat better than that of other open resources. High level object oriented wrappers are provided in Snap7, including .Net [8], so the PLC driver can be written in C# language, users don't need to handle any interoperability with native code [9]. It has the capabilities of connecting and disconnecting with the PLC using sockets, reading and writing bytes from a single area of memory if a starting address and the number of bytes are given. In addition, it can directly map DBs to classes and structs. What's more, Snap 7 supports various operating systems like Windows, Linux, Mac OS and Oracle Solaris.

##### B. Monitoring System Development

Information concerning the state of machine tool includes machine start/stop, manufacturing processes, measurement, tool/magazine situation, alarms, et al. The information can be acquired by accessing the DBs of PLC via Snap 7 codes/functions. IP address and configuration can be automatically made via the X127 connection of NCU. And NCU switch and PLC protection switch should be set as zero. In our research, the IP address is: 192.168.214.1. The platform and softwares for system development here are Windows 7, Visual Studio and C#. Snap 7 supports DLL of Windows platform.

Typical functions are:

##### 1) Connection function

```
public int ConnectTo (string Address, int Rack, int Slot);
```

ConnectTo function can connect the IP address of PLC and the parameters of concerned Rack and Slot. For S7-300, Rack and Slot are set as 0 and 2, respectively. Successful access has the return value of zero. Otherwise, codes for error message will be returned.

##### 2) Reading function

```
public int ReadArea (int Area, int DBNumber, int Start, int Amount, int WordLen, byte[] Buffer);
```

This function can extract the data listed in Table 1 by accessing/analyzing the DBs, the input/output signals, memories for counter and timer.

TABLE I. AREA FUNCTION AND THE PARAMETERS

Parameters	Data
0x81	Input
0x82	Output
0x83	Marker
0x84	DBs
0x1C	Counter
0x1D	Timer

The parameters in the bracket are defined as: DBNumber: DB number; Start: Starting address; Size: Bytes length; Wordlen: data type; Buffer: byte group.

##### 3) Writing function

```
public int WriteArea(int Area, int DBNumber, int Start, int Amount, int WordLen, byte[] Buffer);
```

WriteArea function works in the same way as the reading function ReadArea.

Besides the functions above, Snap 7 also provides many other functions like PLC parameter configuration function, et al. The interface of the monitoring/control system developed here is shown in Figure 6. The system can realize various controls like emergency stop, reset, start, stop, clockwise or anti-clockwise rotation, and auxiliary functions like magazine management, lubrication, cooling, lighting, feed rate control, et al. Using routers or adapters, DNC system can be realized to monitor the state of machine groups and to remotely control machine tool as well.

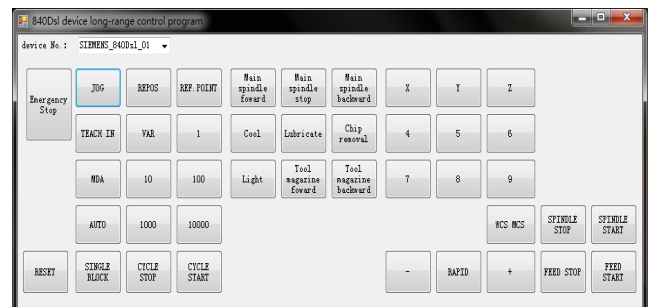


FIGURE VI. INTERFACE OF THE DEVELOPED MONITORING/CONTROL SYSTEM

## V. CONCLUSION

Based on the protocols of communication interfaces of SINUMERIK 840D sl NC system, and utilizing particularly the data exchange rules of PLC unit and NCK unit, the methodology for direct reading/writing of variables in PLC unit is proposed. In this study, monitoring/control system is developed using Snap 7, an open source software, and C# language to extract the data in PLC unit. The system is evaluated and proved reliable to monitor and remotely control the machine tool with 840D sl NC system. The research in this study paves the way for future DNC system development.

## REFERENCES

- [1] Louis B, *International Manufacturing Strategy in a Time of Great Flux*, Springer Switzerland, 2017.
- [2] Ward P T, McCreery J K, et al, Competitive priorities in operations management. *Decis. Sci.* 29(4):1035–1046,1998.
- [3] Boyer M, Lewis M, Competitive priorities: investigating the need for tradeoffs in operations strategy. *Prod. Oper. Manag.* 11(1):9–20, 2002.
- [4] Hallgren M, Olhager J, Schroeder R G, A hybrid model of competitive capabilities. *Oper. Prod. Manag.* 31(5):511–526, 2011.
- [5] Baines T S, Lightfoot H W, et al, The servitization of manufacturing: a review of literature and reflection on future challenges. *J. Manuf. Tech. Manag.* 20(5):547–567, 2009.
- [6] SINUMERIK 840D sl, SINAMICS S120, Machine data and parameters manual, 2013.
- [7] <http://w3.siemens.com/mcms/mc-solutions/de/maschinenbau/handlingsysteme/handling-mit-sinumerik/Seiten/sinumerik-handling.aspx>.
- [8] Nardella D., Snap7 reference manual, 2015.
- [9] <https://www.mesta-automation.com/siemens-s7-plc-c-s7-net-plc-driver/>.
- [10] SINUMERIK 840D sl/840D/810D/840Di lists manual, 2005.