Integrating Your Controller and Consumables with the CPC IdentiQuik™ RFID Interrogator and Tags

Version: 4.3
Date: September 12, 2018

Colder Products Company
1001 Westgate Drive
Saint Paul, Minnesota 55114
USA
Phone: 651-645-0091
Fax: 651-645-5404
www.colder.com
Follow us:
YouTube | Twitter | Facebook | LinkedIn

Smart fluid handling to take you forward, faster.

Integration

CPC's IdentiQuik Radio Frequency Identification (RFID) products provide your consumable with data, tracking and brand integrity within your system. By following a straight forward plan, application of Colder's RFID technology realizes these goals

Basics

Your system's controller, via a USB or serial cable, communicates with a CPC IdentiQuik RFID Interrogator. The Interrogator in turn communicates through the air with your nearby consumable which has an attached RFID tag housed in a CPC Smart coupling, cap, insert or label. Thus your system's controller (a PC, PLC, etc.) may send and receive information with your consumable.

The **system architect** tasks are:

1) Define the RFID tag data content and use to meet your application goals.
2) Decide tracking information.
3) Decide level of additional Brand Integrity to employ.

The **programming** tasks are:

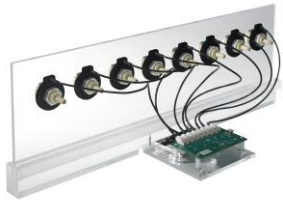
4) Design the RFID tag data layout.
5) Controller / Consumable communication.
    a. Program your factory controller to communicate with the IdentiQuik Interrogator to initialize the tag.[1]
    b. Program your fielded system controller to communicate with the IdentiQuik Interrogator per the data content selected and acting on that data.
6) Implement IdentiQuik Interrogator commands to update the tag in the field.
7) Implement Brand Integrity (security) programming as needed.

The **electronic** tasks are:

8) Interface selection and connection.
9) Power supply.

CPC is available to assist you with every step.

Sample Interrogators (aka RFID Readers) with Various Interfaces





Sample Tags (CPC Smart Couplings with RFID: Cap and Insert)



[1] Initializing of RFID tags with custom data may be done at Colder. See Jeff Anderson Jeff.Anderson@colder.com for details.

System Architect: Define the RFID Tag Data

Your consumable has unique data needs. Sample types of data include: date/time, part ID, text, volume, price and color. Aside from the tag's unique serial number, what is written and updated in an RFID tag is entirely up to you. Any type of data is recordable.

RFID tags have 3 main functional features: a supplied unique serial number, re-writable memory and the ability to make irrevocably *read-only* select portions of memory. Use this RFID memory to store product data, current status/history and authentication codes.

Your Colder Interrogator is attached to your system's controller using a USB or serial interface. Your product (let's call it the "Elixir of Life") has an attached Colder Smart Cap containing the RFID tag. You want to record in the RFID tag various fixed product information.

1) Part Identification
2) Date of Manufacture
3) Use by Date
4) Lot Identification
5) Product Size

Additionally your system wants to keep track of the amount of remaining product.

6) Product Remaining.

Production:

At your factory, as the consumable is made, the initial set of data is written to the consumable's RFID tag.

1)	Part Identification:	Elixir101
2)	Date of Manufacture	Jan. 6, 2020
3)	Use by Date	July 6, 2020
4)	Lot Identification	123456789AB
5)	Product Size	1000 mL
6)	Product Remaining.	1000 mL

Customer Site:

On your deployed system, with the customer's first use of this consumable, the system's controller checks the consumable's fixed data to assess the correctness ("Part ID", "Product Size") and freshness ("Use by Date").

As your customer uses the product, your system checks the "Product Remaining". Your system notes the usage of product and updates the tag's "Product Remaining" as needed. Even if the product was removed and brought back later to the same or another system, the amount remaining would be remembered. Eventually the "Elixir" is used up and the "Product Remaining" field is set to 0 mLs. Thus your system knows to no longer operate with this container of your consumable.

5)	Product Size	1000 mL
6)	Product Remaining.	0 mL

Figure 1: Elixir of Life Example

System Architect: Decide Tracking Information

RFID tags provide the ability to be updated in the field. The consumable's usage and history may be recorded on its RFID tag. Re-use is detectable. Important process steps are recordable - all this without a connection back to a central database as with barcodes. These updates and others, after your product has been created, are called tracking. Two popular aspects of tracking of your consumable include single use and event logging.

Single Use

Consumables may use RFID to insure a single use. Your system, in the field, has the ability to irrevocably mark RFID data as read-only. Thus once a product is used up, data describing the amount remaining may be marked permanently as zero. Note: mid-level thresholds may also be irreversible flagged. Contact CPC for details.

Production:

At your factory, your product is filled. Shaded values are read-only.

1) Product Type — Probe T1
2) Uses Remaining — 1

Customer Site:

Your customer begins to use the consumable.

1) Product Type — Probe T1
2) Uses Remaining — 0

Figure 2: Single Use Example

Event Logging

Your product may need to record its stages of life like: Production, Qualification, and Use. At each stage, your system controller writes data on the RFID tag indicating the event. Should a stage be prohibited from occurring twice, the data could be made read-only, preventing re-use.

Production:

At your factory, 3 date stamps are set-up as part of your RFID data. Shaded dates are read-only.

1) Production: — Jan 6, 2020
2) Qualification — None
3) Use — None

Qualification:

Later the product is qualified.

1) Production: — Jan 6, 2020
2) Qualification — Jan 7, 2020
3) Use — None

Customer Site:

Next month, the product is used by the customer.

1) Production: — Jan 6, 2020
2) Qualification — Jan 7, 2020
3) Use — Feb 14, 2020

Figure 3: Event Logging Example

System Architect: Decide the Level of Additional Brand Integrity

Brand integrity uses RFID tags to insure products' genuineness. Simply using an RFID tag provides the first level of Brand Integrity. To provide higher levels of integrity, additional methods are employed.

Brand Integrity:

1) Simple — Detect the presence of an RFID tag.
2) Good — Detect duplicates (and above).
3) Better — Encrypting the consumable's data (and above).
4) Best — Validate the consumable's with a message authentication code (and above).

Detect the presence of an RFID tag.

The presence of your consumable's tag is the simple first step. Counterfeiters would need to procure a tag. The CPC IdentiQuik Interrogator provides this basic functionality.

Detect duplicates.

Although serial numbers on RFID tags are not duplicable, an adversary may create a circuit to emulate an RFID tag. The sure way to detect duplicates is for your controller to record a history, disallowing re-use based on serial numbers.[2]

Data Encryption

The encrypting of data uses well-known and provably secure encryption techniques. Your controller "knows" the secret number used to encrypt/decrypt some or all of the data. Some additional data space is needed on the tag. Typically fixed data and updatable data are encrypted separately. Well encrypted data on your RFID tag appears random – thus also providing data obfuscation.

Message Authentication Code (MAC)

A MAC is information that provides integrity and authenticity assurance of the data. A good MAC generation function prevents an attacker from making data of their choosing and generating a valid MAC. It is computationally infeasible to do so without know a secret key. This key exists at the factory and within the system's controller.

The longer the MAC, the more secure it is. A separate MAC may be used for fixed and dynamic data.

Production:

Using the first example's data: the tag serial number and constant data of "Part identification", …, "Product size" and a factory secret number; a MAC is added. All this is made *read-only*. The "Product Remaining" is written after being encrypted with a 2nd secret number.

Customer Site:

Only authenticated consumables are usable. As they are used, the "Product Remaining" is updated. Each write of the "Product Remaining" is encrypted. Eventually when consumption is complete, the ""Product Remaining" is made read-only.

Figure 4: Brand Integrity Example

[2] Alternative methods exist. Contact Colder for details.

Programmer: Design the RFID Tag Data Layout

The standard CPC RFID tag contains a unique 8-byte serial number; 28 blocks of 4-byte memory and each block having a write protection flag (WPF). Other sizes are available ranging up to 8,192 bytes of data.

	Byte 0	Byte 1	Byte 2	Byte 3	WPF[3]
Block 0	'H'	'e'	'l'	'l'	0
Block 1	'o'	' '	'W'	'o'	0
Block 2	'r'	'l '	'd'	0	0
…	…	…	…	…	…
Block 27	0	0	0	0	0

Serial Number	16142028064219747960

Figure 5: 28x4 RFID Tag "Hello World" Example

The initial programming task is to layout the location, size and encoding of the desired data. Various concerns include clarity of representation, space efficiency, obfuscation, relationship to the write protect flag, endian[4] and future growth. Below, Figure 1 data is used as an illustrative example.

Data	Byte Address	Size	Encoding[5]	Sample Value	WPF
Part Identification	0	12	UTF8	Elixir101	1,1,1
Date of Manufacture	12	4	time_t	Jan. 6, 2020 12:34:56	1
Use by Date	16	4	time_t	July 6, 2020 12:34:56	1
Lot identification	20	12	UTF8	123456789AB	1,1,1
Product size	32	4	integer	1000 mL	1
Product remaining	36	4	integer	1000 mL	0
unused	40	72			0,0,…,0

Figure 6: Programming Data Layout Example

	Byte 0	Byte 1	Byte 2	Byte 3	WPF
Block 0	'E'	'l'	'i'	'x'	1
Block 1	'i'	'r'	'1'	'0'	1
Block 2	'1'	0	0	0	1
Block 3	240	9	141	86	1
Block 4	240	250	124	87	1
Block 5	'1'	'2'	'3'	'4'	1
Block 6	'5'	'6'	'7'	'8'	1
Block 7	'9'	'A'	'B'	0	1
Block 8	232	3	0	0	1
Block 9	232	3	0	0	0
…	…	…	…	…	…
Block 27	0	0	0	0	0

Serial Number	16142028064219747960

Figure 7: 28x4 RFID Tag Elixir of Life Example

[3] Write Protect Flag. When the write protect flag is set, the corresponding block is no longer write-able. It is *read-only*. The WPF may not be cleared – it is only settable.
[4] The byte order of data may be either big or little endian. The tag serial number itself is in little endian order.
[5] As needed, contact Colder for recommended encoding formats.

Programmer: Controller / Consumable Communication

The CPC IdentiQuik RFID Interrogator and Tags provide a remote non-volatile memory associated with your system's consumable. Simple commands allow read and write access to the RFID tag's unique serial number, data and data write protection.

The CPC IdentiQuik RFID Interrogator accepts and replies with ASCII commands across a serial or USB (using a virtual serial interface) cable. Various communication rates are available. Your controller (PLC, PC, etc.) opens a stream to a serial interface and transmits commands like "SN" to query the RFID tag's serial number. See *IdentiQuik Smart Coupling Communication Protocol* for details.

At your factory, writes to the RFID tag, via the stream you opened, contain commands and the desired data in byte form. This initializes the consumable's RFID tag. Contact CPC for sample code.

Your system's controller at the customer site also sends various commands to read the RFID data. Thus your controller knows the consumable's product information and serial number. It records the tag's serial number to prevent serial number spoofing. Authentication of the product then occurs as needed – see Brand Integrity section. Your system updates the tag's data, potential irrevocably setting the write protection flags.

Programmer: Updating the Consumable's Data

With your consumable, at the customer's site, updating the consumable's RFID tag is straight forward. Simple re-write the portion of the RFID tag that as needed. Typically, the remaining unset write protect flags are selectively set as your consumable goes through various stages. Contact CPC for sample code.

Programmer: Implement Brand Integrity Programming.

CPC supports and recommends effective Brand Integrity. This needs special attention as it directly affects the authenticity of your consumable. Two optional methods, Digital Signature and Encryption offer strong, yet not difficult to program, solutions. Note: Using a "cycle redundancy check", CRC, as an authentication code is not recommended for it if far too easy to compromise.

Message authentication code[6]
In an RFID tag, the message authentication code is a large integer that is written on the tag in addition to your data. This integer is derived from a secret integer (private key), your data *and* the tag's unique serial number. Even tags with the same data, but unique serial numbers, will have very different MAC. Your controller uses the same secret integer, your data, the tag's unique serial number and the MAC to determine if the data is authentic. The strength of a MAC depends on its size. A minimum of 32 bytes is recommended. The size need not be a power-of-2. Contact CPC for details.

Encryption[7]
Encryption takes a set of data and scrambles it in a manner that unless one has the secret code (key), it is infeasible to determine how to unscramble it. In addition to the data (plain text) to encrypt, the tag's serial number and a random number are added to the encryption. The resultant encrypted data (cyphered text) looks random. Even a simple change of 1 bit in the plain text will result in about ½ of all bits of the cyphered text changing. Including the RFID tag serial number in the encryption insures that a copy of ciphered text on another tag will fail. Including random integers (~8 bytes) with the encryption insures that even if the same plain text occurs, the ciphered data written to the tag will be different. Contact CPC for sample code.

[6] http://en.wikipedia.org/wiki/Message_authentication_code
[7] Recommend XXTEA. See http://en.wikipedia.org/wiki/XXTEA

Electronics: Interface Connection

CPC provides various options for the system controller to communicate with the CPC IdentiQuik RFID Interrogator. Two popular interfaces available include USB and RS-232.

The USB IdentiQuik comes with a cable terminated with a standard USB A plug.

The RS-232 IdentiQuik comes with a cable terminated with a 9-pin female D-sub organized as a DTE. This interface additionally needs power on pin 4 (DTR). A systems controller's DTR is not expected to sufficiently power the IdentiQuik. An alternate feed of power on pin 4 is recommended.

Pin	Name	Usage
2	TD	Outgoing data
3	RD	Incoming data
4	Pwr	Power input
5	Gnd	Communication and power ground
1,6-9		Not used
Shell	FG	Shell

RS-232 Interface

Electronics: Power

The USB CPC IdentiQuik RFID Interrogator derives its power entirely from the USB interface. Current consumption < 150 mA. When enabled, the IdentiQuik will automatically enter into lower power mode during non-use.

The RS-232 IdentiQuik employs a switching power supply. Power needs are 60mA nominal and 250mA maximum at 8 - 24 Volts DC. When directed, the IdentiQuik will enter into a lower power mode.

FCC Interference

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

Reorient or relocate the receiving antenna.
Increase the separation between the equipment and receiver.
Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
Consult the dealer or an experienced radio/TV technician for help.

FCC Part 15 Clause 15.21

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment

FCC Part 15.19(a)

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

ISED RSS-Gen Notice

This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions:
(1) This device may not cause interference; and
(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
1) l'appareil ne doit pas produire de brouillage;
2) l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

ISED RF Exposure Guidance

In order to comply with FCC/ISED RF Exposure requirements, this device must be installed to provide at least 20 cm separation from the human body at all times.

Afin de se conformer aux exigences d'exposition RF FCC / ISED, cet appareil doit être installé pour fournir au moins 20 cm de séparation du corps humain en tout temps.

Module integration Notes

When incorporating the FCC certified IdentiQuik coupler into your device, the following labeling should be considered for inclusion:

- Device trade name (IdentiQuik)
- Unique device identifier (Model or part number)
- A statement indicating

"Contains Transmitter Module with FCC ID: U9C-IDENTIQUIK and IC ID: 7038A-IDENTIQUIK"

Assuming that your FR-generating device has been tested and certified to FCC standards, the following labeling should be considered for inclusion:

- An FCC logo is allowed, but not required
- The following text should be included, unless the device is too small or if it is impractical to include language on the device "This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation."

If any of the above labeling is not able to be included on the device due to size constraints, it should be included in the manual. Other labeling considerations for the manual include: specific disclosures and warnings about modifications, RF radiation exposure, operation in conjunction with other antennas or transmitters, and limitations or warnings about special accessories.