IMPLEMENTING THE NEW MCM TECHNOLOGY
(Multi-Chip Module) IN PAYMENT TERMINALS

Miodrag Stankovic, Trintech Technologies Dublin

Abstract – This paper describes advantages and difficulties in implementing the new MCM technology in electronic payment terminals (machines). Compared to various competitive technologies, the MCM offers significant improvement in manufacturing reliability, reduced size, decreased unit cost and extended security. The application described in this paper is first implementation of the MCM technology in payment terminals.

1. INTRODUCTION

Trintech Technologies Limited develops, manufactures and markets hardware devices to process credit and debit card payment transactions quickly, securely and cost-effectively. Trintech has been developing their terminal range since 1998, using PCB and microprocessor control technology. Trintech’s competitors are using either PCB or ASIC technology and Trintech will be a first user in applying MCM technology to high security payment terminals (Note: verified by the TTN). Before this application experiment, Trintech had no experience in applying MCM, FPGA or ASIC technologies.

2. MARKET STRUCTURE

There are 50 manufacturers of electronic payment terminals worldwide and Trintech is ranked amongst the top 15. The market is characterised by one large global supplier (Verifone), several mid-sized vendors operating globally, regional players with strong national market position, of which Trintech is the leading player, and finally a group of domestically based companies.

Regarding the number of units sold and the technology used, competitors can be classified into 3 tiers: global competitors (US companies Verifone and Hypercom) with sales of >200K units p.a. using ASIC technology, a middle tier including Trintech with sales of between 15-50K units p.a. and the tier of small competitors with sales <15K p.a. Vendors in tiers 2 and 3 are primarily using PCB technology. Trintech does not have the economies of scale to compete with global player on cost and thus competes on innovation and design, and this MCM Project will give the company the ability to compete in new markets.

There are a number of key technology trends that are being tackled under this program, as listed in Table 1.

3. PRODUCT TO BE IMPROVED

There were two main products: a customer terminal for secure PIN (personal identity number) entry and retailer terminal.

The retailer terminal, a Compact 9000 is a merchant point-of-sale terminal that accepts all major credit and debit cards. It processes a complete range of transactions types. It’s features include smart card and magnetic swipe card reading facilities, and high speed communication for reduced operating cost and faster transaction time. The range of Compact 9000 terminals includes portable devices. For any secure PIN entry transactions, however, the Compact 9000 terminal has to be accompanied by the customer terminal, described below.

The customer terminal, PINpad 950, is a high security anti-tamper terminal for customer to enter their PIN number. Encryption keys are stored within the unit memory and are used to encrypt the PIN so it may be forwarded to an authori-
station centre for validation. These keys are highly security sensitive and must be protected. The PINPad 930 is inserted in epoxy to achieve a physical security barrier. Any attempt to tamper with the PINPad 950 terminal will activate an alarm. The alarm circuit will detect attempts to drill through the secure area, as well as chemical attacks, heating and cooling, attempt to open the unit, to disconnect battery, etc. Once the alarm has been activated it will wipe the contents of the memory.

The PINPad 950 plugs in to the Compact 900 range, but can also be used as a plug in to an Electronic Cash Register (ECR).

For Tritech to keep ahead of our competitors and to follow the market trends the PINPad 950 must be improved to provide:

- Reduced terminal size
- Decreased unit cost
- High security
- Improved manufacturing reliability

The PINPad 950 production process includes the enclosure of all the sensitive electronics inside wire mesh. This is followed by the potting of the whole assembly in epoxy. This process is expensive, labour-intensive and slow, and any failure detected after potting (up to 10% of the units) result the entire unit been discarded. Tritech performed a feasibility study of the available technologies and identified MCM (Multi-Chip Module) technology as the best method for achieving size reduction, reduced cost and improve manufacturing reliability while maintaining the existing high security.

The PINPad 950 motherboard includes RS-232 communications to its microcontroller. The RAM is divided into 3 secure memory areas where an application can be loaded after the unit is mounted. There are software and hardware firewalls between the applications to prevent loading of rogue application to interrogate a legitimate one.

Tritech did not have any experience on MCM before the start of this project. To move from PCB to MCM was a very large technology step. Tritech considered the possibility of improving the electronic design of the PINPad (another microcontroller, more functionality, etc.) and/or redesign of the PINPad enclosure. However it was felt this would be too risky. Therefore it was decided to transfer the existing design to the MCM as a first step. The second step of the programme will be the integration of the retailer terminal (Compact 9000) and the customer terminal (PINPad) into a combined portable unit using MCM.

As mentioned above, the existing product used conventional PCB technology. This needed to be ported an MCM device in order to meet increasing demand for small handheld units with increased functionality and high security. In order to be considered handheld, the unit should be less than 3 cm high at the center and 10 cm or less in width or length whichever is shortest.

The MCM will be used firstly to improve PINPad 950.

The MCM will maintain the high security of the device (and even improve it due to small dimension) while reducing its weight and manufacturing costs. The MCM device will also be used to provide high security requirement for the new Barcodes range, which will provide the functionality of the previous two product and will meet the size requirements for portable devices.

The security sensitive electronics have been placed in a single 'secure MCM chip' which includes the tamper detection features. By using a micro via design the sensitive nodes are buried under the IC making it impossible to probe the MCM without destroying it. The inside of the MCM package alone will be secured thus eliminating the requirement to pot the entire functional area, as with the current Tritech terminal range.

4. TECHNICAL IMPROVEMENTS

All the electronics of the existing board have been implemented in the MCM. The size of both PCBs is the same as both fit under the keypads of the PINPad 950. However, while the old board requires the wire mesh and epoxy potting, the new one has a single MCM component which does not require wire mesh or potting.

While the overall size of PINPad units remain the same, the new units offers:

- reduced terminal weight (no epoxy, smaller and less components, etc.)
- decreased unit cost (the new board cost is 16% lower than the existing one)
- high security (improved security due to smaller dimension of the MCM)
- improved manufacturing reliability

The MCM consist of five dies and some passive components:

- Microcontroller- Hitachi 875302 16 bit microcontroller
- SRAM - 128Kx8 low power static RAM
- EPROM - 128Kx8 EPROM
- Microprocessor supervising powerdown and reset for controller.
- PLD-XILINX CPLD device
- The devices include capacitor for charge pump to produce negative voltage, capacitors for decoupling, pull-up and pull-down resistors, resistor for voltage divider, EMI filtering.

The dies have to be attached using a 'flip-chip' process (the die pads are attached from underneath the chip). This process requires the dies to be available as a full wafer. But this was not possible with all the dies components, so wire bonding was also used.

When the dies have been attached and tested, the area inside the cap is filled with hardened gel to provide protection. The mesh, which is printed on the PCB, and the tamper circuitry prevents any attempts to break the MCM module. The size of MCM fears amateur hackers as expensive microcircuit and probes would be required to attempt to gain access to the device. For more sophisticated hackers, a special mesh is printed on the inside of the package of the MCM, to detect drilling or cap removal. The confidential information is contained within the MCM, where any attempt to gain access will result in the alarm being activated and the contents of the memory being erased.
5. CHOICES AND RATIONALE FOR MCM TECHNOLOGY SELECTIONS

The main requirements for the new PINPad product and the Barracuda range were size, cost and ease of manufacture while maintaining the high security of the existing product. The available technologies were analysed and the advantages and disadvantages are listed in Table 2.

Table 2

<table>
<thead>
<tr>
<th>Technology</th>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Competitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCM</td>
<td>Reduced size, Lower manufacturing cost, High security</td>
<td>New technology and not yet approved for high security</td>
<td>None</td>
</tr>
<tr>
<td>PCB</td>
<td>Proven technology</td>
<td>Size, cost, reliability, low functionality</td>
<td>Widely used</td>
</tr>
<tr>
<td>FPGA</td>
<td>Lower unit cost, reduced size</td>
<td>Power consumption too high for portable devices where the battery must power the alarm circuit for 5 years. Low security - would require expensive potting to implement security, as in current PINPad</td>
<td>Competitors use these for non-portable devices with lower security requirement</td>
</tr>
<tr>
<td>ASIC</td>
<td>Lower unit cost, reduced size</td>
<td>Design and manufacturing set up costs too high. Volumes greater than 100k required to justify. Again would not meet security requirements, potting would be needed.</td>
<td>A number of competitors use these, but none have anti-tamper high security features needed for PIN entry</td>
</tr>
</tbody>
</table>

The conclusions of this analysis were as follows:

1. For high security the best option was MCM. Extra components must be added to achieve security with the other devices.
2. To achieve the required size reduction, FPGA, ASIC or MCM would have all been suitable.
3. In terms of individual device cost the best option, for small volumes would be FPGA, while in large volumes it would be ASIC. However these devices do not meet security requirements on their own so the MCM has lower manufacturing costs (no potting, mesh, etc.)
4. For easy manufacturing MCM is best as there is no extra process needed.
5. Furthermore MCM provides increased functionality, improved reliability, and ease of maintenance.

Trintech expects that increased sales will result from:
- Compactness of hardware units arising from miniature MCM technology
- Lower manufacturing costs and improved yield
- Lower device cost.
- Increased functionality of devices
- Expansion of product range to include a portable PoS and PINPad in a single unit (Barracuda)

- Improved graphic displays and other functions as a result of smaller unit

6. CONCLUSION

There is a growing market for the inclusion of anti-tamper high security features in electronic devices across many industry sectors and applications. The payments and banking industry is traditionally very conservative, and there are rigorous approvals to be achieved before products can be launched on the market.

The application described in this paper was the first implementation of MCM technology in high security anti-tamper environment. The new technology significantly improves reliability and security and decreases production costs of payment terminals.

7. LITERATURE