this is not compulsory. Stored procedures can use RETURN keyword but without any value being passed.

Functions could be used in SELECT statements, provided they don't do any data manipulation. However, procedures cannot be included in SELECT statements. A function can have only IN parameters, while stored procedures may have OUT or INOUT parameters. A stored procedure can return multiple values using the OUT parameter or return no value at all.

```
CREATE FUNCTION MyFunction (@someValue
INTEGER) RETURNS INTEGER
AS
BEGIN
  DECLARE @retval INTEGER

  SELECT localValue
    FROM dbo.localToNationalMapTable
    WHERE nationalValue = @someValue

  RETURN @retval
END
```

VI. Conclusion

In the end we can say that a Stored procedure not only enhancing the possibility of reusing the code and execution plan, but it also increases the performance of the database by reducing the traffic of the network by reducing the amount of information send over the network. Design-time automation makes coding faster and ensures that all the procedures generated use the same naming conventions and structure. In an effort to improve their coding efficiency in a large SQL project, the authors wrote a set of design-time stored procedures that generate run-time stored procedures, and have used them in project after project ever since.

VII. References

[1] C. Anley. Advanced sql injection in sql server applications.
http://www.nextgenss.com/papers/advancedsqlinjection.pdf

[2] C. Anley. (more) advanced sql injection.
http://www.nextgenss.com/papers/more advanced sql injection.pdf, White Paper.

[3] B. M. L. Archive. http://seclists.org/lists/bugtraq/2005/, 2005.

[4] C. Cerrudo. Manipulating Microsoft sql server using sql injection.
http://www.appsecinc.com/presentations/Manipulating SQL Server Using SQL Injection.pdf, White Paper.

[5] S. Friedl. Sql injection attacks by example.
http://www.unixwiz.net/techtips/sql-injection.html.

[6] O. W. A. S. P. (OWASPD). Top ten most critical web application vulnerabilities.
http://www.owasp.org/documentation/topten.html, 2005.

[7] T. R. site exposes Data.
http://www.netsecurity.org/news.php?id=1593, 2002.

[8] K. Spett. Blind sql injection.
http://www.spidynamics.com/whitepapers/Blind SQLInjection.pdf, White Paper.

[9] C. V. N. VU#982109.
http://www.kb.cert.org/vuls/id/982109, 2005.

[10]Dynamically maintain the teaching examples of triggers and stored procedures about the course of database application, Wu Da-sheng; Wu Sheng-yu
Education Technology and Computer (ICETC), 2010 2nd International Conference